protiviti®

Face the Future with Confidence

Unlock Your Guide to AML

U.S. Anti-Money Laundering Requirements

FREQUENTLY ASKED QUESTIONS

Seventh Edition

Internal Audit, Risk, Business & Technology Consulting

PREFACE

"Overall, our goal is to help you help us. And we continue to look for more ways to strengthen that relationship and to identify, with you, better ways that we can accomplish our goals."

FinCEN Deputy Director Jamal El-Hindi

In September 2003, we issued the first edition of Protiviti's *Guide to U.S. Anti-Money Laundering Requirements, Frequently Asked Questions*. We would never have imagined at that time that the 140 questions answered in that edition would expand to the nearly 3,000 questions addressed in this current version, our seventh edition. Our goal for this edition remains the same as that for the first edition: to provide clear and concise responses to the questions we hear regularly from our clients, attorneys, regulators, members of law enforcement, academics and others interested in the requirements and challenges that companies face in anti-money laundering/combatting financial terrorism (AML/CFT) and sanctions compliance. The increase in the number of questions highlights the complexity and dynamic nature of the subject matter. To help you stay current, we are introducing this edition of the Guide in a digital and easily searchable format with regular updates that will be accessible through our website.

The Guide begins by summarising some basic principles of money laundering and terrorist financing, followed by discussions of the U.S. legal and regulatory requirements, practical considerations that companies should address in designing and maintaining effective compliance programs, and insights on the synergies and differences between AML/CFT compliance programs and other overlapping areas of compliance (e.g., fraud, offshore tax evasion, anti-corruption, cybersecurity). The Guide closes with a section on international perspectives and initiatives.

This edition of the Guide includes expanded discussions of recent changes (through June 30, 2017) to AML/CFT and sanctions laws and regulations (e.g., identification and verification of beneficial owners, country-based sanctions programs), suggested reforms to the existing AML/CFT legal and regulatory regime, AML/CFT technology (e.g., incorporation of risk and customer profiles, data analytics, model validation, regtech), and the impact of alternative value transfer systems such as virtual currency providers. It also includes a special supplement on the New York State Department of Financial Services' first of its kind regulation requiring certification of AML/CFT and sanction screening programs.

The responses to the questions have been drawn from myriad regulatory publications, issuances and guidance from other governmental agencies and law enforcement, industry publications, media reports, and Protiviti's own work with a wide range of companies. It is important to note that this Guide is provided for general information only and focuses primarily on federal AML/CFT requirements. The responses and points of view included herein are intended to assist companies with their compliance efforts. However, the information provided is not intended to be legal analysis or advice, nor does it purport to address, except in a few instances, state or international money laundering requirements that may affect U.S. companies. Companies should seek the advice of legal

counsel or other appropriate advisers on specific questions as they relate to their unique circumstances.

We hope the Guide is a useful resource for your AML/CFT and sanctions compliance needs, and we invite you to visit www.protiviti.com/AML to stay current on important developments.

Protiviti
September 2017

Acknowledgments

We are immensely grateful to our former colleague, Karen L. Wilkes, who once again was the primary researcher and drafter of this update. We also offer special thanks to Michael Mancusi of Arnold & Porter Kaye Scholer LLP for his review of the sanctions section of the Guide and to the following Protiviti practice and subject matter experts for their contributions: Shaun Creegan, Shaheen Dil, Vishal Ranjane, Matt Taylor, Chetan Shah, Christine Bucy, Chris Carpenter and Edwin Oloo, and to Kaitlin Lemmo and Scott Solaruckerman, who recently left the firm for industry employment.

CONTENTS AT A GLANCE

TABLE OF CONTENTS

THE FUNDAMENTALS

Key Principles

1. What is money laundering?

Money laundering is the attempt to disguise the proceeds of illegal activity so that they appear to come from legitimate sources or activities.

2. What is the current scale of the money laundering problem?

Measuring the current scale of money laundering is extremely difficult. The World Bank (WB) and International Monetary Fund (IMF) have estimated the volume of money laundering to be between 3 and 5 percent of global gross domestic product (GDP), equivalent to approximately US$2.2 trillion to US$3.7 trillion annually. According to the U.S. Department of the Treasury, more than US$300 billion is laundered in the United States annually.

3. How does money laundering work?

Money laundering can, and does, take many forms; however, it typically occurs in three stages: placement, layering and integration:

- **Placement** is the stage in which funds derived from illegal activities are introduced into the financial system.
- **Layering** involves conducting one or more transactions designed to disguise the audit trail and make it more difficult to identify the initial source of funds.
- **Integration** is the stage in which the funds are disbursed back to the money launderer in what appear to be legitimate transactions.

4. What is terrorism?

18 United States Code (USC) § 2331 defines domestic and international terrorism separately:

- **Domestic terrorism** is defined as activities that:
  - "[I]nvolve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
  - [A]ppear to be intended—
    - [T]o intimidate or coerce a civilian population;
    - [T]o influence the policy of a government by intimidation or coercion; or
    - [T]o affect the conduct of a government by mass destruction, assassination, or kidnapping; and
  - [O]ccur primarily within the territorial jurisdiction of the United States."

- **International terrorism,** sometimes referred to as transnational terrorism, is defined as activities that:
  - "[I]nvolve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
  - [A]ppear to be intended:
    - [T]o intimidate or coerce a civilian population;
    - [T]o influence the policy of a government by intimidation or coercion; or
    - [T]o affect the conduct of a government by mass destruction, assassination, or kidnapping; and
  - [O]ccur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum."

5. What is terrorist financing?

Terrorist financing is a financial crime that uses funds to support the agenda, activities or cause of a terrorist organisation. The funds raised may be from legitimate sources, such as charitable organisations or donations from supporters, as well as from criminal sources, such as the drug trade, weapons smuggling, fraud, kidnapping and extortion for illegal activities.

6. What are some common methods of terrorist financing?

According to the National Terrorist Financing Risk Assessment (2015), major funding sources of terrorist organisations such as ISIL, al-Qaeda and Boko Haram include, but are not limited to, the following:

- Kidnapping for ransom (KFR)
- Private donations, solicited directly or indirectly through charitable organisations;
- Extortion of the population and resources in controlled territory;
- Revenue from legitimate businesses located in controlled territory;
- Illicit revenue from criminal activities (e.g., smuggling, narcotics trafficking); and
- State sponsorship.

7. Is the financing of weapons of mass destruction considered terrorist financing?

If the proliferator is a terrorist, financing weapons of mass destruction (WMDs) could be considered a type of terrorist financing. However, not all proliferators are terrorists; therefore, governments have determined that the development of measures to prevent, suppress and disrupt the proliferation and financing of WMDs, distinct from terrorist financing, is necessary.

Many countries have implemented non-proliferation measures to combat money laundering and terrorist financing. For further guidance, please refer to the Terrorism and Terrorist Financing section.

8. What is the difference between money laundering and terrorist financing?

In contrast to money laundering, which involves the disguising of funds derived from illegal activity so they may be used without detection of the illegal activity, terrorist financing can involve the use of legally derived money to carry out illegal activities. The objective of money laundering is financial gain or the hiding or disguising of illicit proceeds, whereas with terrorist financing, the objective is to hide how raised funds will be deployed (e.g., to promote the agenda or cause of the terrorist organisation). For example, it is widely believed that the terrorist activities of September 11, 2001, were partially financed by legally obtained funds that had been donated to charities.

9. Are the stages of terrorist financing the same as money laundering?

In general, yes, however, in the placement phase, funds could be derived from both legitimate and illegal activities. The methods of layering to disguise the source of funds are the same with money laundering and terrorist financing. In the integration phase, funds are typically disbursed to the terrorist or terrorist organisation, directly or indirectly through a third party to obscure the beneficiary and the ultimate objective of supporting a terrorist act.

10. What types of crimes may give rise to a charge of money laundering?

Although money laundering is often equated with drug trafficking, the proceeds of many crimes can be associated with money laundering. The Financial Action Task Force (FATF), an intergovernmental policy-making body composed of more than 30 countries, whose purpose is to establish and promote international legislative and regulatory standards in the areas of money laundering and terrorist financing, suggests the following "designated categories of offenses for money laundering" as activities that should be considered as predicate crimes to money laundering:

- Participation in an organised criminal group and racketeering
- Terrorism, including terrorist financing
- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Corruption and bribery
- Fraud
- Counterfeiting currency
- Counterfeiting and piracy of products

- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint and hostage-taking
- Robbery and theft
- Smuggling (including in relation to customs and excise duties and taxes)
- Tax crimes (related to direct taxes and indirect taxes)
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation

The United States, as an example, lists hundreds of specified unlawful activities (SUAs) under 18 U.S.C. 1956, including many, though not all, of the crimes listed above, including the following partial listing:

- Racketeering activity (e.g., any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in an obscene matter, or dealing in a controlled substance or listed chemical as defined by the Controlled Substances Act [CSA]), which is chargeable under state law and punishable by imprisonment for more than one year;
- Terrorist financing;
- Counterfeiting (e.g., currency, goods);
- Fraud (e.g., securities fraud, wire fraud);
- Slavery, trafficking in persons and alien smuggling;
- Illegal arms sales (e.g., chemical weapons, nuclear material); and
- Illegal gambling.

11. Is tax evasion considered a predicate crime for money laundering in the United States?

Tax evasion designed to hide illicit funds is considered a predicate crime for money laundering in the United States. If intent to violate federal law can be proven, even tax evasion with legitimate funds is a predicate crime. For further guidance on tax-related disclosures and programs, please refer to the sections Report of Foreign Bank and Financial Accounts and Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act.

12. Is there always a charge of money laundering when a charge is brought for an underlying predicate crime?

No. Money laundering is a separate, autonomous offense, so a charge related to an underlying predicate crime does not have to be accompanied by a charge of money laundering.

A charge of money laundering may be brought if one wilfully aids and abets a money launderer or terrorist, even if the party who aids or abets has not committed a predicate crime.

13. If the predicate crime occurs outside of the United States, can one be charged with money laundering?

In many circumstances, dual criminality, where the illicit activity is considered a predicate offense to money laundering in both countries (e.g., crime occurred in one country, proceeds from the crime detected in another country), may be required to facilitate mutual legal assistance and, ultimately, prosecution for money laundering.

With the globalisation of the world economy, the rise of transnational organised crimes and the focus on foreign corruption, mechanisms to coordinate international cooperation (e.g., information sharing, extradition, asset recovery) to combat money laundering and terrorist financing are more imperative than ever.

14. Is the approach to combating money laundering and terrorist financing the same?

When analysing underlying criminal activities (e.g., drug trafficking), the patterns of activity tend to be different for "laundering" related to terrorism. For example, terrorist financing often involves very small volumes of funds, which may be moved through charities or nontraditional banking systems, whereas laundering the proceeds of narcotics sales typically involves the movement of a large volumes of funds (e.g., bulk cash smuggling). The same infrastructure may be leveraged to combat both money laundering and terrorist financing; however, different risk factors and red flags need to be applied to detect effectively all forms of illicit activity.

15. Have international standards been developed to combat money laundering and terrorist financing?

Yes. In 1990, FATF published 40 legislative and regulatory recommendations for combating money laundering and terrorist financing. These standards, published as the *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation – the FATF Recommendations* and referred to as "FATF Recommendations" or "Recommendations" were revised in 1996, 2001, 2003 and 2012. In 2001, eight additional recommendations, which were ultimately integrated into the 40 Recommendations, were added to address terrorist financing. The Recommendations cover the following:

- **AML/CFT Policies and Coordination (Recommendations 1 and 2)** – Provides guidance on how to assess risks and apply a risk-based approach in developing an AML/CFT framework and how parties (e.g., financial institutions, regulatory authorities, law enforcement) can share information and coordinate efforts with each other, domestically and internationally.

- **Money Laundering and Confiscation (Recommendations 3 and 4)** – Advises countries to criminalise money laundering and consider the widest range of predicate offenses, and provides guidance on legislative measures to enable authorities to freeze, seize or confiscate proceeds and property from money laundering and terrorist financing.
- **Terrorist Financing and Financing of Proliferation (Recommendations 5 – 8)** – Advises countries to criminalise terrorist financing and designate terrorist financing as a money laundering predicate offense; provides guidance on the legislative measures to designate and delist targets and to enable authorities to freeze funds or assets of designated targets subject to sanctions related to terrorism, terrorist financing and proliferation of WMDs; encourages countries to review laws and regulations that relate to nonprofit organisations to evaluate their adequacy in guarding against abuse for the financing of terrorism.
- **Preventive Measures (Recommendations 9 – 23)** – Advises countries to modify secrecy laws to enable implementation of FATF's Recommendations (e.g., to facilitate information sharing between appropriate authorities); and outlines several measures and controls for financial institutions to mitigate risks and prevent money laundering and terrorist financing, including:
    - Risk assessments to identify vulnerabilities and appropriate controls to mitigate the risks associated with new customers, products and business practices, including new delivery mechanisms;
    - Development of an enterprisewide program, including policies on information sharing, consistently applied across foreign branches and subsidiaries, with enhanced measures for those located in high-risk jurisdictions;
    - Risk-based due diligence (e.g., collection of information at account opening and ongoing, verification of identity, reporting of suspicious transactions, obtaining senior management approval) on customers and beneficial owners, with enhanced measures for politically exposed persons (PEPs), correspondent banks, and money or value transfer services (MVTS), also known as money services businesses (MSBs);
    - Ability to stop (e.g., freeze, seize, confiscate) transaction(s)/asset(s) if it involves a designated target subject to sanctions;
    - Reporting of suspicious transactions to financial intelligence units (FIU), with measures to ensure confidentiality and to protect financial institutions from criminal and civil liability (i.e., Safe Harbor);
    - Recordkeeping to permit reconstruction of transaction(s) and, if necessary, to provide evidence for prosecution of criminal activity, including, but not limited to, originator/beneficiary information in wire transfers;
    - Development of policies that outline the conditions under which a financial institution may rely upon a third party to perform due diligence on its behalf; and

  - Due diligence requirements for designated nonfinancial businesses and professions (DNFBPs) (e.g., casinos, real estate agents, dealers in precious metals and stones, attorneys, accountants, trust service providers).

- **Transparency and Beneficial Ownership of Legal Persons and Arrangements (Recommendations 24 – 25)** – Provides guidance on measures to prevent the misuse of legal persons or legal arrangements (e.g., trusts) for money laundering and terrorist financing, including bearer shares or bearer share warrants, by facilitating the collection of and access to beneficial ownership and control information.
- **Powers and Responsibilities of Competent Authorities and Other Institutional Measures (Recommendations 26 – 35)** – Provides guidance on the development of an effective AML/CFT system, including, but not limited to:
  - Designation of competent and empowered authorities to supervise financial institutions and DNFBPs for compliance with AML/CFT laws and regulations with a risk-based approach
  - Establishment of an FIU as the central agency to receive and analyse required reporting (e.g., suspicious transaction reporting, large currency transactions, disclosures of cross-border movement of currency and negotiable instruments) and disseminate guidance, statistics and feedback to relevant authorities in a secure and confidential process
  - Designation of competent and empowered law enforcement authorities with the responsibility for conducting domestic and international money laundering and terrorist financing investigations, and the authority to identify, trace and initiate freezing and seizing of assets
  - Establishment of a large currency transaction reporting requirement above a fixed amount, including both domestic and international transfers
  - Establishment of a declaration or disclosure system to detect cross-border transportation of currency and bearer negotiable instruments (BNI), also referred to as monetary instruments
  - Establishment of sanctions (e.g., civil, criminal, administrative penalties) for noncompliance with AML/CFT laws and regulations for financial institutions, DNFBPs and senior management
- **International Cooperation (Recommendations 36 – 40)** – Countries are encouraged to ratify international conventions/treaties and develop a legal basis (e.g., sign treaties, enter a memorandum of understanding [MOU]) to provide mutual legal assistance (e.g., information sharing, freezing of assets, extraditions) to other countries (e.g., financial institutions, FIUs, supervisors, law enforcement) in relation to money laundering and terrorist financing proceedings. Suggested treaties include:

- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention, 1988);
- The International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention, 1999);
- United Nations Convention Against Transnational Organised Crime (Palermo Convention, 2000);
- The United Nations Convention Against Corruption (2003); and
- Other relevant treaties where applicable.

For further guidance on international AML/CFT standards, please refer to the International Perspectives and Initiatives and Financial Action Task Force sections.

16. Does FATF prescribe a "one-size-fits-all" solution to developing an AML/CFT framework?

No. FATF suggests countries assess their money laundering and terrorist financing risks and develop risk-based AML/CFT frameworks based on their findings.

17. Why has cash historically been used in the majority of criminal dealings?

The inability to trace the origin or owner heightens the money laundering and terrorist financing risk of currency transactions. Currency transactions are typically used during the placement phase of money laundering. Although cash remains the primary form of laundering, criminals have used other payment mechanisms, including, but not limited to, wire transfers, monetary instruments, prepaid access, virtual currency, and precious metals and stones.

18. With the rise of alternative value transfer systems (e.g., virtual currency), is cash still the primary instrument used in money laundering?

Using 2016 as the frame of reference, of the 1.98 million Suspicious Activity Report (SARs) filed from January 1, 2016, through December 31, 2016, reports involved the following instruments:

- Cash/currency totalled more than 744,000 (38 percent)
- Funds transfers totalled nearly 736,000 (37 percent)
- Monetary instruments totalled nearly 315,000 (16 percent)
- Other instruments totalled more than 62,000 (3 percent)
- Foreign currency totalled nearly 54,000 (3 percent)
- Gaming instruments totalled more than 26,000 (1 percent)

Cash and funds transfers are the most commonly reported instruments. While virtual currency transactions may be included under "other instruments," virtual currency is not a common instrument for money laundering as reported on SARs. For further guidance on virtual currency, please refer to the Virtual Currency Systems and Participants section.

19. How did the United States approach developing its AML/CFT legislative and regulatory framework?

The United States developed its AML/CFT legislative and regulatory framework gradually, focusing on large cash transactions, domestic and international funds transfers and other recordkeeping requirements in the 1970s, and, influenced by the FATF Recommendations and international treaties and U.N. resolutions to combat money laundering and terrorist financing, expanding to other types of activities.

The United States developed a risk-based approach by, over time, designating more than 20 different types of businesses as "financial institutions" and subjecting them to comprehensive AML/CFT laws and regulations. The U.S. definition of financial institutions includes entities defined by FATF as "financial institutions" and "designated nonfinancial businesses and professions" (DNFBPs), including, but not limited to: depository institutions, broker-dealers, MSBs, mutual funds, housing government-sponsored enterprises (GSEs), insurance companies, trust companies and dealers in precious metals, precious stones or jewels.

AML/CFT measures include, but are not limited to, the following:

- Freezing transactions and assets
- Maintaining records and reporting high-risk transactions and suspicious activities
- Self-disclosures of cross-border movement of high-risk products (e.g., currency, monetary instruments) and financial accounts held in foreign jurisdictions
- Collection and verification of information of customers and beneficial owners
- Sharing information with other financial institutions, regulatory authorities and law enforcement

Additional AML/CFT measures have been issued for the following high-risk customer, product and transaction types:

- Correspondent banks (e.g., payable-through accounts [PTAs], shell banks)
- Private banking
- PEPs
- Designated targets subject to sanctions
- Cash (e.g., large cash transactions over US$10,000, cross-border movement of cash)
- Funds transfers (e.g., wire transfers)
- Monetary instruments (e.g., bank checks, cashier's checks, money orders, traveller's checks)
- Prepaid access devices

20. Are banks the only types of businesses vulnerable to abuse by money launderers and terrorists?

No. Money launderers and terrorists also launder funds through nontraditional, underground and nonbanking business types, including, but not limited to, the following:

- MSBs (e.g., check cashers, money transmitters)
- Informal value transfer systems (IVTS) (e.g., hawala, Black Market Peso Exchange [BMPE])
- Broker-dealers in securities
- Casinos and card clubs
- Insurance companies
- Real estate businesses (e.g., lenders, persons involved in real estate settlements and closings)
- Exporters/importers (e.g., trade-based money laundering [TBML])
- Retailers (e.g., stores that offer luxury items such as precious metals and stones and works of art)

Despite implementing AML/CFT measures, criminals can continue to gain access to financial systems through third-party proxies (e.g., professional service providers, such as attorneys and accountants), hence the focus of recent AML/CFT laws on the identification of beneficial owners beyond nominal customers.

For further guidance on nonbank financial institutions (NBFIs), please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section. For further guidance on beneficial owners, please refer to the Beneficial Owners section.

21. What is trade-based money laundering (TBML)?

Trade-based money laundering (TBML) refers to the process of disguising the proceeds of illegal activity and moving value through the use of trade transactions so that they appear to come from legitimate sources or activities. One example of a TBML is the Black Market Peso Exchange (BMPE). For further guidance, please refer to the Trade Finance Activities and Alternative Value Transfer Systems sections.

22. What is insider abuse as it relates to AML/CFT laws?

Insider abuse generally refers to violations or attempted violations of laws, regulations or internal policies by employees (e.g., directors, officers) for personal gain. Insiders may have the knowledge and ability to evade internal controls designed to prevent money laundering and terrorist financing.

23. What are some challenges in combating money laundering and terrorist financing?

Some challenges include, but are not limited to, the following:

- Emerging risks (e.g., new payment systems and delivery mechanisms)

- Development of AML/CFT measures to guard against abuse from criminals without excluding vulnerable members of society who may be denied access to financial systems due to these measures
- Capacity for developing nations to establish comprehensive AML/CFT frameworks
- Effective international cooperation (e.g., legal framework, privacy issues, security and confidentiality issues)
- Efficient information sharing/collaboration domestically (e.g., within institutions, across an industry, with regulators, law enforcement, federal/state/local) and internationally

Overview of U.S. AML/CFT Laws

24. What are the key U.S. AML/CFT laws?

The key U.S. AML/CFT law is the Bank Secrecy Act (BSA) (also known as the Financial Recordkeeping of Currency and Foreign Transactions Act of 1970), which was significantly amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

The BSA was the first major money laundering legislation in the United States. It was designed to deter the use of secret foreign bank accounts and provide an audit trail for law enforcement by establishing regulatory reporting and recordkeeping requirements to help identify the source, volume and movement of currency and monetary instruments into or out of the United States or deposited in financial institutions.

Following the terrorist activity of September 11, 2001, the USA PATRIOT Act was signed into law by President George W. Bush on October 26, 2001, was reauthorised and amended by the USA PATRIOT Improvement and Reauthorisation Act of 2005, and was reauthorised by President Barack Obama. Title III, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, deals with money laundering and terrorist financing. Title III made significant changes to money laundering regulations, imposed enhanced requirements for AML Programs, and significantly expanded the scope of coverage to NBFIs. It requires financial institutions to establish AML Programs that include policies, procedures and controls; designation of a compliance officer; training; independent testing; and ongoing risk-based monitoring of customer activity and information with updates as necessary. It also requires, among other things, that certain financial institutions establish customer identification procedures for new accounts, as well as enhanced due diligence (EDD) for correspondent, private banking accounts maintained by non-U.S. persons and senior foreign political figures also referred to as PEPs.

The BSA's implementing regulations are detailed under 31 C.F.R. Chapter X (Parts 1000 et seq.): Financial Crimes Enforcement Network, Department of the Treasury.

For additional guidance on the specific requirements of U.S. AML/CFT laws and regulations, please refer to the Bank Secrecy Act and USA PATRIOT Act sections.

25. What other federal AML/CFT laws have been enacted in the United States?

In addition to the BSA and Title III of the USA PATRIOT Act, other AML/CFT laws include, but are not limited to, the following:

- The Money Laundering Control Act of 1986 (MLCA), (18 U.S. C. §§ 1956 and 1957)
- The Anti-Drug Abuse Act of 1988 (Pub. L. 100-690, 102 Stat. 4181, codified as amended in scattered sections of the U.S.C. (2012))
- The Annunzio-Wylie Anti-Money Laundering Act of 1992 (Pub. L. 102-550, 106 Stat. 4044 (codified as amended in scattered sections of the U.S.C. (2012)))
- The Money Laundering Suppression Act of 1994 (MLSA) (31 U.S.C. §§ 5301, note 5330 (2012))
- The Money Laundering and Financial Crimes Strategy Act of 1998 (31 U.S.C. §§ 5301, 5340-5342, 5351-5355 (2012))
- Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA), (18 U.S. C. Pub. L. 104-132, 114 Stat. 1214 (codified as amended in scattered sections of the U.S.C. (2012)))
- The Intelligence Reform and Terrorism Prevention of 2004 (Pub. L. 108-458, 118 Stat. 3638 (codified as amended in scattered sections of the U.S.C. (2012)))

The MLCA established two criminal statutes that, for the first time, made money laundering a criminal offense, with penalties of up to 20 years and fines of up to US$500,000 for each count. Additionally, the MLCA prohibits the structuring of currency transactions to avoid filing requirements and requires financial institutions to develop AML Programs.

The primary purpose of the Anti-Drug Abuse Act of 1988 was to provide funding and technical assistance to state and local units of government to combat crime and drug abuse. This Act increased the civil and criminal penalties for money laundering and other BSA violations to include forfeiture of any property or asset involved in an illegal transaction related to money laundering. It introduced the "sting" provision, which enables law enforcement to represent the source of funds involved in a transaction as the proceeds of unlawful activity. This Act also required the identification and recording of purchases of monetary instruments, including bank checks or drafts, foreign drafts, cashier's checks, money orders or traveller's checks in amounts between US$3,000 and US$10,000 inclusive. This legislation, in conjunction with the Office of National Drug Control Policy (ONDCP) Reauthorisation Act of 1998, authorised the director of the ONDCP to designate areas within the United States that exhibit serious drug trafficking problems and harmfully impact other areas of the country as High Intensity Drug Trafficking Areas (HIDTAs). The HIDTA program aims to improve the effectiveness and efficiency of drug control efforts among local, state and federal law enforcement agencies. This Act also authorised the issuance of Geographic Targeting Orders (GTOs) that require a financial institution or a group of financial institutions (or businesses) in a geographic area to file additional reports or maintain additional records above and beyond the ordinary reporting requirements (e.g., less than US$10,000 for large currency transactions). GTOs are used to collect information on individuals/entities suspected of conducting transactions under reportable thresholds.

The Annunzio-Wylie Anti-Money Laundering Act of 1992 gave protection from civil liability to any financial institution, or director, officer or employee thereof, who/that makes a Suspicious Activity Report (SAR) under any local, state or federal law, a Safe Harbor provision, which was further clarified by Section 351 of the USA PATRIOT Act. The Annunzio-Wylie Act made it illegal to disclose when a SAR is filed. It also made it illegal to operate a money transmitting business without a license where such a license is required under state law, and required all financial institutions to maintain records of domestic and international funds transfers. In addition, this Act introduced the "death penalty," mandating that bank regulators consider taking action to revoke the charter of any banking organisation that is found guilty or pleads guilty to a charge of money laundering.

MLSA specifically addressed MSBs, requiring each MSB to register and maintain a list of its agents. In addition to making it a federal crime to operate an unregistered MSB, the MLSA encouraged states to adopt uniform laws applicable to MSBs. It also established procedures that allowed banks to exempt certain customers from Currency Transaction Report (CTR) filing.

Continuing with the trend of developing a national strategy to combat money laundering, the Money Laundering and Financial Crimes Strategy Act of 1998 called for the designation of areas at high risk for money laundering and related financial crimes by geography, industry, sector or institution. Some of these areas were later designated as High Intensity Financial Crime Areas (HIFCAs). The HIFCA program was created to coordinate the efforts of local, state and federal law enforcement agencies in the fight against money laundering.

The Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) criminalised activities dealing with terrorism and terrorist financing, including providing material support or resources to designated terrorists or terrorist organisations, providing or collecting terrorist funds, concealing or disguising material support or funds to terrorists, and receiving military-type training from terrorist organisations. The AEDPA also required U.S. financial institutions to block funds of designated terrorists and terrorist organisations.

The Intelligence Reform and Terrorism Prevention Act of 2004 amended the BSA to require the U.S. Treasury Secretary to prescribe regulations requiring certain financial institutions to report cross-border electronic transmittals of funds, if the Secretary determines such reporting is "reasonably necessary" to aid in the fight against money laundering and terrorist financing.

26. What significant legislation has been proposed or passed to strengthen existing AML/CFT laws to address gaps and emerging risks such as digital currencies?

In May 2017, the U.S. Senate introduced Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017 to strengthen existing AML/CFT laws by addressing gaps and emerging risks such as virtual currencies. Key sections include, but are not limited to, the following:

- **Section 2 – Transportation or transshipment of blank checks in bearer form** – Monetary instruments with blank dollar amounts are to be valued at US$10,000 to trigger existing regulatory reporting requirements for Report of International Transportation of Currency or Monetary Instruments (CMIRs).

- **Section 3 – Increasing penalties for bulk cash smuggling** – Increases maximum term of imprisonment from five years to 10 years and adds a criminal fine provision.
- **Section 4 – Section 1957 violations involving commingled funds and aggregated transactions** – Clarifies that the "withdrawal of funds in excess of US$10,000 from an account containing more than US$10,000 in criminal proceeds commingled with other funds" is a transaction involving more than US$10,000 in criminally derived property and thus subject to 18 USC 1957 relating to the transfer of criminal proceeds.
- **Section 5 – Charging money laundering as a course of conduct** – Gives the U.S. government the option to file a single count of money laundering if a defendant has committed multiple money laundering offenses (as opposed to filing a separate offense with each transaction); conspiracies to violate the prohibition of unlicensed money transmitters would be included under money laundering conspiracies.
- **Section 6 – Illegal money services businesses** – Clarifies that specific knowledge of the licensing requirement is unnecessary to be charged with operating an illegal money services business; increases penalties and fines for violations.
- **Section 7 – Concealment money laundering** – Clarifies that couriers (or mules) are not required to know that the transportation of cash or drugs is designed to conceal or disguise a specified unlawful activity (SUA) nor are couriers required to know that the cash are proceeds from a specific SUA (as opposed to some form of SUA) in order to be prosecuted under AML/CFT laws and regulations.
- **Section 8 – Freezing bank accounts of persons arrested for offenses involving the movement of money across international borders** – To address the issue of the transfer of criminal proceeds from defendants' accounts, Section 8 grants the U.S. government the authority to obtain a 30-day order freezing accounts held by a person arrested for offenses involving the movement of funds in or out of the United States.
- **Section 9 – Prohibiting money laundering through hawalas, other informal value transfer systems, and closely related transactions** – To address whether parallel transactions meet the "proceeds of a criminal offense" element when conducted through hawalas or informal value transfer systems (IVTSs), Section 9 extends the clarification issued in 2006 that "a financial transaction includes proceeds of a specified unlawful activity if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement" to hawalas and IVTSs.
- **Section 10 – Technical amendment to restore wiretap authority for certain money laundering and counterfeiting offenses** – Restores U.S. government's ability to obtain wiretap authority for currency reporting, bulk cash smuggling, illegal money services businesses and counterfeiting offenses.
- **Section 11 – Making the international money laundering statute apply to tax evasion** – Transferring funds into or out of the United States with the intent to violate U.S. income tax laws will become a money laundering violation.

- **Section 12 – Conduct in aid of counterfeiting** – Adds materials (e.g., anything similar to security features, bleached paper that removes images of lower denominations allowing for printing of higher denominations), tools, machinery, in addition to existing list of prohibited items (e.g., cover plates, stones) that may be used to counterfeit U.S. or foreign currency.
- **Section 13 – Prepaid access devices, digital currencies, or other similar instruments** – Amends existing AML/CFT regulations to include funds stored in a digital format (e.g., prepaid access devices, digital currencies) within the definition of monetary instrument.
- **Section 14 – Administrative subpoenas for money laundering cases** – Expands the availability of administrative subpoenas for criminal investigations involving money laundering activities, activities of illegal money services businesses and activities aimed at avoiding certain currency transaction reporting requirements; authorises administrative subpoenas for investigations that would constitute a money laundering offense against a foreign nation; adds additional scenarios for issuing a nondisclosure order for an administrative subpoena.
- **Section 15 – Obtaining foreign bank records from banks with United States correspondent accounts** – Requires foreign banks to produce certified records to be used as evidence, prohibits foreign banks from disclosing the existence of the subpoena, authorises the U.S. government to seek contempt for noncompliance with the subpoena and allows the U.S. government to seek civil penalties against a U.S. financial institution if it does not terminate its correspondent relationship with a foreign bank if the foreign bank does not comply with or successfully challenge the subpoena, pursuant to Section 319 of the USA PATRIOT Act.
- **Section 17 – Clarification of Secret Service authority to investigate money laundering** – Clarifies that the Secret Service has the jurisdiction to pursue money laundering investigations.
- **Section 18 – Prohibition on concealment of ownership of account** – Makes it an offense for an "individual to knowingly conceal, falsify or misrepresent, from or to a financial institution, a fact concerning the ownership or control of an account or assets held in an account."
- **Section 19 – Prohibition on concealment of the source of assets in monetary transactions –** Enables U.S. government to pursue individuals (and their assets) who conceal, falsify or misrepresent the involvement of a Special Measures entity identified as a "primary money laundering concern" or a foreign PEP.

Whether this bill will ever be passed into law is unclear; however, the ML/TF risks identified by these gaps should be considered by financial institutions.

27. Are AML/CFT laws issued only at the federal level?

No. Many states have also implemented their own AML/CFT laws, consistent with federal AML/CFT laws, including, but not limited to, the following:

- Criminalisation of money laundering and terrorist financing
- Predicate crimes (e.g., racketeering laws, cocaine, heroin and marijuana laws)
- Supervision of NBFIs (e.g., MSBs, insurance companies, vehicle sales and leasing)

- Civil and criminal forfeiture
- Divestment from sanctioned countries or entities

For example, New York's money laundering statute, New York Penal Law Article 470, criminalises money laundering, including laundering in support of terrorism. In 2015, New York finalised regulations for virtual currency businesses, under the BitLicense Regulatory Framework for Virtual Currency Firms, the first of all states and ahead of the federal government. In 2016, New York implemented Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certification, imposing requirements, including annual certifications, for transaction monitoring and sanctions filtering programs.

Colorado regulates its MSBs under state law Title 12, Article 52 – Money Transmitters. Also, under Amendments 20 and 64, Colorado legalised medicinal and recreational use of marijuana, creating a stalemate between the marijuana industry and financial institutions, as federal law still prohibits the growth, sale and possession of marijuana.

If regulated on a state level, a strong coordination between state and federal authorities is required when enforcing AML/CFT laws and regulations.

For further guidance on businesses engaged in marijuana-related activities, please refer to the Marijuana-Related Businesses section. For further guidance on virtual currencies, please refer to the Virtual Currency Systems and Participants section.

28. What is the role of the Office of Foreign Assets Control (OFAC) and how does it fit into AML/CFT laws and regulations?

The purpose of OFAC is to promulgate, administer and enforce economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. Sanctions programs target, for example, terrorists and terrorist nations, drug traffickers and those engaged in the proliferation of WMDs.

Sanctions programs administered by OFAC include, but are not limited to, the following:

- Counter Terrorism Sanctions Program
- Counter Narcotics Trafficking Sanctions Program
- Transnational Criminal Organisations Sanctions Program
- Cyber-Related Sanctions Program
- Non-Proliferation Sanctions Program
- Rough Diamond Trade Controls Sanctions Program
- Country- and Regime-Based Sanctions Program (e.g., Cuba, Iran, Iraq, Libya, North Korea, Russia, Syria, South Sudan)

In addition to the objectives of OFAC to combat terrorism, narcotics trafficking, the proliferation of WMDs, and transnational criminal organisations, the primary objectives of the U.S. government with respect to the Country- and Regime-Based Sanctions Program vary but overall, aim for the following:

- Reduce/eliminate political corruption;
- Reduce/eliminate misappropriation of public assets and natural resources;
- Politically stabilise regions;
- Protect sovereignty and territorial integrity;
- Reduce/eliminate human rights violations with an emphasis on acts of violence against women, children and refugees;
- Reduce/eliminate the use and recruitment of child soldiers;
- Protect internationally accepted human rights (e.g., freedom of expression, religion, right to assemble)
- Protect channels delivering humanitarian assistance; and
- Protect international peacekeeping missions.

For further guidance, please refer to the Country- and Regime-Based Sanctions Programs section.

Since OFAC Sanctions Listings include alleged narcotics traffickers, terrorists and proliferators of WMDs, institutions often consider the OFAC Sanctions Compliance Program to be a subset of their overall AML/CFT Compliance Program. For additional guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

29. What key international principles influenced or shaped U.S. AML/CFT laws?

The FATF Recommendations have influenced U.S. AML/CFT laws. As have the following treaties that have been ratified by the United States:

- **United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances** (Vienna Convention, 1988)
- Organisation for Economic Co-operation and Development (OECD) **1997 Convention on Combating Bribery of Foreign Public Officials in International Business Transactions** (OECD Bribery Convention)
- **United Nations Convention Against Transnational Organised Crime** (Palermo Convention, 2000)
- **The United Nations Convention Against Corruption** (2003)
- **The International Convention for the Suppression of the Financing of Terrorism** (the Terrorist Financing Convention, 1999) (plus an additional 11 U.N. conventions relating to terrorism [e.g., unlawful seizure of aircrafts, violence at airports, hostage-taking, maritime navigation, nuclear terrorism])

- **Arms Trade Treaty** (ATT) (2013), a multilateral treaty that regulates international trade in conventional arms (e.g., tanks, armoured combat vehicles, artillery systems, military aircraft, small arms, light weapons, combat support equipment)

The U.N. Security Council has adopted multiple resolutions to maintain international peace and security since the 1940s. These resolutions are formal expressions of the U.N. Security Council and generally include a description of the issue(s) and any action(s) to be taken to address the issue (e.g., freezing funds, travel bans, arms embargo). Key resolutions relating to the prevention and suppression of terrorism and terrorist financing include, but are not limited to, the following:

- **Al-Qaida Sanctions Lists** – Resolutions 1267 (1999), 1333 (2000), 1526 (2004), 1989 (2011) and its successor resolutions;
- **Taliban Sanction Lists** – Resolutions 1267 (1999), 1526 (2004), 1988 (2011) and its successor resolutions;
- **Islamic State of Levant/Sham** (ISIL/ISIS/Da'esh)-Sanctions Lists – Resolutions 2249 (2015), 2253 (2015), and its successor resolutions;
- **Resolution 1373** (2001) was passed shortly after the September 11, 2001, attacks in New York City, Washington, D.C. and Pennsylvania. The resolution reaffirmed past resolutions related to combating terrorism (e.g., Resolution 1269 [1999], Resolution 1368 [2001]) and called on all members to fully implement relevant international conventions relating to terrorism. Resolution 1373 provided a mechanism for identifying targets for designation on a national or supranational level; and
- **Resolutions related to the proliferation of WMDs** – Resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), 1929 (2010) and its successor resolutions.

30. Who are the members of the U.N. Security Council?

The U.N. Security Council has five permanent members and 10 nonpermanent elected members who serve two-year terms. The five permanent members include China, France, Russia, the United Kingdom and the United States.

Members of the United Nations that are not members of the U.N. Security Council may participate in discussions, but may not vote on actions taken by the Council. Out of approximately 200 U.N. members, nearly 70 have never been elected to the U.N. Security Council.

31. Do U.S. financial privacy laws inhibit financial institutions from sharing with law enforcement key information related to money laundering investigations?

While there are a number of U.S. laws in place to protect consumers, in particular, law enforcement is not inhibited in its ability to investigate and prosecute money laundering offenses. Multiple information sharing mechanisms have been implemented that enable financial institutions to provide law enforcement with critical information, including, but not limited to, reports and records of potentially suspicious activities, large currency transactions, and responses to inquiries about specific customers.

32. What is the value to law enforcement of the various reporting and recordkeeping requirements imposed by the BSA?

In general, BSA-required reports have become extremely useful to law enforcement in the identification, investigation and prosecution of money laundering and other criminal activity, especially those generating large amounts of cash. Data contained in these reports also are used to identify and trace the disposition of proceeds from illegal activity for possible seizure and forfeiture. In addition, agencies can analyse reports on a strategic level to obtain trends and assess the threat(s) in particular areas.

33. How can one measure the effectiveness of an AML/CFT regime?

A number of factors can be considered when assessing the effectiveness of an AML/CFT regime, including the number of money laundering/terrorist financing investigations, prosecutions and convictions, number and amount of frozen/seized assets, identification of deficiencies in financial institutions in examinations by regulatory authorities, and quality of coordination among financial institutions, regulatory and law enforcement authorities. For additional guidance on tools and techniques used to assess the effectiveness of AML/CFT systems, please refer to the Financial Action Task Force section.

34. Has the United States conducted a self-assessment of its money laundering and terrorist financing risks?

Yes. The most recent National Money Laundering Risk Assessment (NMLRA) was published in 2015 by the U.S. Treasury with input from multiple federal agencies and offices (e.g., Federal Bureau of Investigation [FBI], the Internal Revenue Service (IRS), the Drug Enforcement Administration [DEA], the Office of Foreign Assets Control [OFAC], Financial Crimes Enforcement Network [FinCEN], Immigration and Customs Enforcement [ICE], United States Secret Service [USSS]) as an update to the U.S. Money Laundering Threat Assessment (MLTA), published in 2005. The NMLRA contains detailed analyses of money laundering vulnerabilities, similar to those identified in the MLTA (2005) across banking, insurance, casinos and MSBs including, but not limited to, the following:

- Use of currency and monetary instruments (e.g., bank notes, cashier's check, money order, traveller's check) in transactions structured under regulatory recordkeeping and reporting thresholds (e.g., US$10,000 for currency transactions, US$3,000 for monetary instruments), commingled with licit funds, used in bulk cash smuggling activities and in trade-based money laundering (TBML) (e.g., Black Market Peso Exchange [BMPE]);
- Establishment of bank and brokerage accounts using nominees (i.e., agent acting by or on behalf of a third party) to disguise the identities of the individuals who control the accounts;
- Creation of legal entities (e.g., shell companies, shelf companies) without accurate information about the identity of the beneficial owner;
- Misuse of products and services (e.g., correspondent banking services, funnel accounts, omnibus accounts, remote deposit capture [RDC], prepaid access cards, virtual currency) resulting from deficient compliance with AML/CFT obligations; and

- Complicit merchants (e.g., wholesalers), third-party payment processors (TPPPs), MSBs (e.g., foreign exchange dealers, money transmitters) and other financial institutions (e.g., banks, broker-dealers, casinos) with deficient compliance with AML/CFT obligations, and in some cases, wittingly facilitating illicit activity.

The National Terrorist Financing Risk Assessment (NTFRA) was also published in 2015 by the U.S. Treasury, with input from many of the same federal agencies and offices that collaborated on the NMLRA, as well as Customs and Border Protection (CBP), the Bureau of Counterterrorism, the Bureau of International Narcotics and Law Enforcement and the National Counterterrorism Center (NCTC). The NTFRA contains detailed analyses of terrorist financing vulnerabilities, including, but not limited to, the following:

- Global terrorism and terrorist financing threats
    - Terrorist threats to the United States (e.g., al-Qaeda, Al-Nusrah Front [ANF], Islamic State of Iraq and the Levant [ISIL], Hizballah, Hamas, Taliban, Haqqani Network, foreign terrorist fighters)
    - Terrorist financing sources (e.g., kidnapping for ransom [KFR], extortion, drug trafficking, private donations through charitable organisations, state sponsorship, cybercrime, identity theft) and vulnerabilities (e.g., charitable organisations, licensed and unlicensed MSBs, foreign correspondent banking, cash smuggling, virtual currency)
- Counterterrorism and CFT efforts
    - Law enforcement efforts (e.g., reorientation, interagency coordination and cooperation, information sharing)
    - Financial/regulatory efforts (e.g., Office of Foreign Assets Control [OFAC] sanctions)
    - International efforts (e.g., United Nations [UN], Financial Action Task Force [FATF])

FATF recommends that each country continues to conduct self-assessments to evaluate and ultimately mitigate money laundering and terrorist financing risks on a national level. For further guidance, please refer to the Risk Assessments section.

35. How do U.S. regulations compare to international AML/CFT regulations?

The United States' role as a leader in the fight against money laundering and terrorist financing dates back nearly 50 years to the passage of the Bank Secrecy Act (BSA) in 1970. Through the ensuing decades and especially following the terrorist activities of September 11, 2001, the United States has reinforced its commitment through the passage of a number of additional money laundering and terrorist financing-related laws, issuance of extensive regulatory guidance (e.g., United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [USA PATRIOT Act] of 2001), and aggressive enforcement.

That said, the United States, as with many other major jurisdictions, is not in full compliance with the FATF Recommendations. In the past decade, FATF has conducted two mutual evaluations of the

United States AML/CFT system, a 2006 assessment based on the Forty Plus Nine FATF Recommendations and a 2016 assessment based on the consolidated FATF Recommendations (updated in 2012 with an updated methodology in 2013). The 2006 mutual evaluation identified several areas in need of improvement, including, but not limited to, the following:

- Customer due diligence relating to beneficial owners;
- Authorised signers, legal persons and trusts;
- Ongoing due diligence; and
- General AML/CFT requirements for designated nonfinancial businesses and professions (DNFBPs) (e.g., accountants, attorneys, dealers in precious metals and stones, real estate agents).

The 2016 mutual evaluation for the United States identified significant gaps in the U.S. framework:

- Poor efforts to prevent criminals from using legal entities to facilitate illicit schemes. This low rating was driven by the inadequate and untimely access to comprehensive and accurate beneficial ownership information in the United States.
- Continued lack of coverage of DNFBPs (e.g., lawyers, accountants, real estate agents, and trust and company service providers), particularly related to customer due diligence (CDD), recordkeeping, suspicious transaction reporting and internal controls.

In July 2016, the United States finalised the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule), which addressed due diligence for beneficial owners and made the ongoing due diligence obligation an explicit requirement of U.S. AML/CFT laws and regulations. While some DNFBPs, such as casinos and dealers in precious metals and stones, are required to establish AML Programs, many are also required to file certain AML/CFT reports, including, but not limited to, the following:

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)

In addition to filing reports, DNFBPs are required to comply with sanctions administered by the Office of Foreign Assets Control (OFAC), and in some instances, required to participate in information sharing as outlined by Section 314 of the USA PATRIOT Act.

Despite these controls, it appears that the United States continues to remain deficient in this area according to FATF, particularly as it relates to investment advisers, real estate agents and professional service providers (e.g., attorneys, accountants).

For additional guidance, please refer to the sections: Financial Action Task Force, Mutual Evaluations: Methodology and Reports, BSA Reporting Requirements, Beneficial Owners, Nonbank Financial Institutions and Nonfinancial Businesses and Professional Service Providers.

36. How has the United States responded to the AML/CFT deficiencies identified within its regulatory framework?

The National Money Laundering Strategy (NMLS) was written by the U.S. Departments of Homeland Security, Justice, Treasury, and State, as well as by the Federal Reserve, the OCC, and the FDIC. The most recent NMLS was published in 2007 in direct response to the Money Laundering Threat Assessment (MLTA). Nine key goals were outlined:

- Continuing to safeguard the banking system
- Enhancing financial transparency in MSBs
- Stemming the flow of illicit bulk cash out of the United States
- Attacking trade-based money laundering (TBML) at home and abroad
- Promoting transparency in the ownership of legal entities
- Examining anti-money laundering regulatory oversight and enforcement at casinos
- Implementing and enforcing anti-money laundering regulations for the insurance industry
- Supporting global anti-money laundering capacity building and enforcement efforts
- Improving how to measure progress

Since then, the United States has published advisories, guidance or proposed or enacted regulations to address these and other noted vulnerabilities within its AML/CFT system. These include, but are not limited to, the following:

- To address the lack of commitment to compliance efforts and accountability:
  - Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (FinCEN's Advisory issued in August 2014)
  - Individual Accountability for Corporate Wrongdoing (Yates Memo) (Department of Justice (DOJ) Memorandum issued in September 2015)
- To address vulnerabilities related to beneficial owners of legal entities and ongoing due diligence requirements:
  - Customer Due Diligence Requirements for Financial Institutions ([Beneficial Ownership Rule], FinCEN's final rule issued in July 2016)
- To address vulnerabilities in financial institutions not subject to AML/CFT Program and Customer Identification Program (CIP) requirements:
  - Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks lacking a Federal Functional Regulator (FinCEN's Notice of Proposed Rulemaking [NPRM] issued in August 2016)
- To address wholesale "de-risking:"

  - Risk Management Guidance on Foreign Correspondent Banking (Office of the Comptroller of the Currency [OCC] in October 2016)
  - Financial Institution Letters: Statement on Providing Banking Services (Federal Deposit Insurance Corporation [FDIC] in January 2015)

- To address vulnerabilities in the real estate industry:
  - Geographic Targeting Orders (GTOs) requiring title insurance companies to collect and report purchases of residential real property over a specified amount (e.g., US$500,000 to US$3 million) in specified cities and counties of California, Florida, New York and Texas, made without external financing (e.g., bank loan) that partially used currency or monetary instruments (e.g., cashier's check, traveller's check, money order) (issued in July 2016, renewed in February 2017)
  - Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Housing Government-Sponsored Enterprises (GSEs) (FinCEN's Final Rule issued in February 2014)
  - Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators (FinCEN's Final Rule issued in April 2012)
- To address vulnerabilities with cyber-related attacks:
  - Cyber-Related Sanctions Program (Implemented by the Office of Foreign Assets Control [OFAC] in December 2015)
- To address vulnerabilities in nonbank financial systems such as MSBs and emerging value transfer systems (e.g., prepaid access, virtual currency):
  - Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017 (a bill introduced by the U.S. Senate in May 2017; Section 13 proposed amending the definition of monetary instrument to include funds stored in a digital format [(e.g., prepaid access devices, virtual currency]).
  - Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies (FinCEN's Guidance published in March 2013)
  - Bank Secrecy Act Regulations: Definition of "Monetary Instrument" (FinCEN's Proposed Rule issued in October 2011; proposed amending the definition of monetary instrument to include select tangible prepaid access devices for purposes of the Report of International Transportation of Currency or Monetary Instruments [CMIR] requirements)
  - Definitions and Other Regulations Relating to Prepaid Access (FinCEN's Final Rule issued in July 2011)
- To address vulnerabilities related to bulk cash smuggling and trade-based money laundering (TBML) schemes:

  - Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML (FinCEN's Advisory issued in August 2014; also related to the following preceding advisories:
    - Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency (FinCEN Advisory issued in June 2010)
    - Information on Narcotics and Bulk Currency Corridors (FinCEN's Advisory issued in April 2011)
    - Update on U.S. Currency Restrictions in Mexico (FinCEN's Advisory issued in July 2012)
    - Supplement on U.S. Currency Restrictions on Banks in Mexico (FinCEN's Advisory issued in September 2013)
  - CMIR Guidance for Common Carriers of Currency, Including Armored Car Services (FinCEN's Guidance issued in August 2014)
- To address vulnerabilities in cross-border funds transfers:
  - Cross-Border Electronic Transmittals of Funds (CBETF) (FinCEN Proposed Rule issued in September 2010)
- To improve how to measure progress:
  - Reformatted SAR Stats (formerly The SAR Activity Review By the Numbers), a compilation of numerical data gathered from the FinCEN Suspicious Activity Reports (SARs) with downloadable data made available for further analysis
- To address financial inclusion:
  - Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers (Request for Information issued by the Consumer Financial Protection Bureau [CFPB] in June 2014)

In some instances, states are ahead of the federal government in proposing and implementing AML/CFT laws and regulations that address emerging risks and other regulatory areas. Examples from New York State include, but are not limited to, the following:

- BitLicense Regulatory Framework for Virtual Currency Firms (Department of Financial Services (DFS) State Regulation proposed in July 2014 and finalised in June 2015)
- Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certification (DFS finalised in 2016)
- Part 500 – Cybersecurity Requirements for Financial Services Companies (DFS regulation finalised in 2017)

For further guidance on Part 504, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications section.

37. Has the United States rescinded any proposed or final AML/CFT regulations or orders?

Yes. The AML/CFT framework is complex and continually evolving. The following are examples of regulations and orders the United States has rescinded:

- AML Program Requirements for Investment Advisers and Unregistered Investment Companies (rules were proposed in 2002/2003, withdrawn in 2008 and reissued in 2015)
- Special Measures Orders (e.g., Asia Wealth Bank, Naura, Ukraine)

Some regulations have been proposed but not yet finalised, including, but not limited to the cross-border electronic transmittals of funds (CBETF) rule proposed in 2010.

38. What are the consequences of not complying with AML/CFT laws and regulations?

The consequences of noncompliance with AML/CFT laws and regulations may include:

- Regulatory enforcement actions;
- Civil and criminal penalties;
- Seizure and forfeiture of funds; and
- Incarceration for the individuals involved.

Depository institutions also may be subject to restrictions on growth and expansion and, in the extreme, may have their charters/licenses revoked, a consequence known as the "death penalty."

For additional guidance, please refer to the Enforcement Actions section.

39. What factors are considered by law enforcement when it assesses whether an institution or its personnel are guilty of aiding and abetting money laundering or terrorist financing?

When assessing whether an institution or its personnel are guilty of aiding and abetting money laundering or terrorist financing, the authorities consider, among other factors, the following "standards of knowledge":

- **Reckless Disregard** – Careless disregard for legal or regulatory requirements and sound business practices
- **Wilful Blindness** – Deliberate ignorance and failure to follow up in the face of information that suggests probable money laundering or illicit activity
- **Collective Knowledge** – Aggregates/attributes the knowledge of employees to the employing company

It is important to remember that under U.S. law, a company may, in general, be held liable for the actions of its employees, regardless of the number or level of employees involved in the wrongdoing.

40. What can financial institutions do to minimise penalties for deficient AML/CFT or sanctions programs?

Voluntary self-disclosures (VSDs) and cooperation with regulatory authorities may help to minimise penalties for deficient AML/CFT or sanctions programs.

The Department of Justice (DOJ) issued Guidance Regarding Voluntary Self-Disclosures, Cooperation and Remediation in Export Control and Sanctions Investigations Involving Business Organisations in 2016. While the guidance explicitly stated that it did not apply to financial institutions, only corporate entities engaged in export activity and their employees, some of the guidance could be applied to financial institutions, in both the sanctions and AML/CFT environment. The guidance discussed how the following activity could impact the "credit" of the VSD:

- Timing and accuracy [e.g., full disclosure of relevant facts] of initial VSD;
- Subsequent cooperation with investigations (e.g. proactive versus reactive); and
- Remediation efforts of flawed sanctions/export control programs (e.g., timeliness, disciplinary actions of responsible employees).

The guidance discussed the following aggravating factors:

- Exports involving nuclear non-proliferation or missile technology to a proliferator country;
- Exports involving items to be used in weapons of mass destruction (WMDs);
- Exports to a terrorist organisation;
- Exports of military items to a hostile foreign power;
- History of repeated sanctions violations;
- Degree of knowledge of involvement of senior management in the sanctions violation(s); and
- Amount of profits earned from sanctions violations, intended or realised.

The guidance also discussed the following types of impact on benefits or "credits" for the self-disclosing entity:

- Reduced fine and/or forfeiture;
- Non-prosecution agreement (NPA) as opposed to a deferred prosecution agreement (DPA);
- Reduced period of supervised compliance; and
- No requirement for a monitor.

Whether self-disclosing for sanctions violations, tax evasion or other laws, it is advisable that institutions seek legal counsel's advice before self-disclosing. For guidance on developing a comprehensive sanctions compliance program, please refer to the OFAC Basics section.

41. Who can be held liable for deficient AML/CFT Compliance Programs?

There is a movement toward making compliance officers and other management personally and criminally liable for their compliance programs. Outside of the AML/CFT space, there's a shift toward individual accountability for corporate misconduct and wrongdoing (e.g., Department of Justice [DOJ] Memorandum on "Individual Accountability for Corporate Wrongdoing" issued by former Deputy Attorney General Sally Quillian Yates [Yates Memo]). On a state level, in 2015, the New York Department of Financial Services (DFS) finalised regulations requiring senior officers or the board of directors to certify annually that their suspicious activity monitoring and sanctions filtering programs are in compliance, thus making these individuals personally liable if they knowingly submit a "false or incorrect" certification.

42. What is an example of an enforcement action emphasising individual accountability?

To date, the largest public civil AML enforcement action against an individual was a US$250,000 fine and a three-year injunction barring compliance employment with any money transmitter against former chief compliance officer (CCO) of MoneyGram International Inc. (MoneyGram), Thomas E. Haider, commonly referred to as "The Haider Settlement" (May 2017).

In December 2012, MoneyGram entered into a Deferred Prosecution Agreement (DPA) with the DOJ with a forfeiture of US$100 million for aiding and abetting wire fraud and failing to maintain an effective AML Program. Initially, Haider faced a personal fine up to US$5 million for his "wilful inaction." According to FinCEN's press release, Haider ultimately settled for a lower amount after admitting, acknowledging and accepting responsibility for the following:

- "[F]ailing to terminate specific MoneyGram outlets after being presented with information that strongly indicated that the outlets were complicit in consumer fraud schemes;
- [F]ailing to implement a policy for terminating outlets that posed a high risk of fraud; and
- [S]tructuring MoneyGram's anti-money laundering (AML) program such that information that MoneyGram's Fraud Department had aggregated about outlets, including the number of reports of consumer fraud that particular outlets had accumulated over specific time periods, was not generally provided to the MoneyGram analysts who were responsible for filing suspicious activity reports with FinCEN."

For further details on MoneyGram's enforcement action, please refer to the Key U.S. Enforcement Actions and Settlements section.

43. What protections do financial institutions have when complying with AML/CFT laws and regulations?

The Annunzio-Wylie Anti-Money Laundering Act of 1992 gives protection from civil liability to any covered financial institution that, or director, officer or employee who, makes a suspicious transaction report under any federal, state or local law. Section 351 of the USA PATRIOT Act further clarifies the terms of the Safe Harbor from civil liability when filing SARs. This protection does not apply if an action against an institution is brought by a government entity.

It is important to note that the Safe Harbor is applicable if a SAR is filed in good faith by a covered financial institution, regardless of whether such reports are filed pursuant to the SAR instructions. The Safe Harbor does not apply to SARs filed maliciously.

44. Does the Safe Harbor provision apply to methods of reporting suspicious activity other than actually filing a SAR?

Yes. Certain other forms of reporting, whether written or verbal, are covered by the Safe Harbor provision, so long as the other forms of suspicious activity reporting are through methods considered to be in accordance with the regulations of the applicable agency and applicable law.

For further guidance, please refer to the Safe Harbor section.

Overview of the U.S. Regulatory Framework

Key U.S. Regulatory Authorities and Law Enforcement Agencies

45. Who has the authority to assess penalties for violations of AML/CFT laws and regulations?

Authority to assess civil penalties rests with the Secretary of the U.S. Treasury and is delegated to the Financial Crimes Enforcement Network (FinCEN) and the primary federal regulators or Self-Regulatory Organisations (SROs) (e.g., Financial Industry Regulatory Authority [FINRA]). Some state regulatory agencies have their own authority to assess civil penalties, as well. Criminal penalties are determined through legal proceedings at state or federal levels. The Department of Justice (DOJ) can bring criminal and civil actions, as well as forfeiture actions.

46. Who are the primary federal banking regulators, and what are their responsibilities?

The five federal banking regulators are:

- The **Board of Governors of the Federal Reserve System (FRB)** oversees state-chartered banks and trust companies that belong to the Federal Reserve System, financial holding companies, bank holding companies (BHCs) and thrift holding companies.
- The **Federal Deposit Insurance Corporation (FDIC)** regulates federally chartered banks (e.g., state-chartered banks that do not belong to the Federal Reserve System) as well as state-chartered thrifts.
- The **Office of the Comptroller of the Currency (OCC)** regulates federally chartered banks (e.g., banks that have the word "National" in or the letters "N.A." after their names, as well as federal thrifts).
- The **National Credit Union Administration (NCUA)** regulates federally chartered credit unions.

- **Consumer Financial Protection Bureau (CFPB):** Established by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank), the CFPB is a federal regulator charged with regulating consumer protection for financial products and services.

47. What is the Federal Financial Institutions Examination Council (FFIEC)?

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards and report forms, and to make recommendations to promote uniformity in the supervision of financial institutions. Council members include the five federal regulators: CFPB, FRB, FDIC, OCC, NCUA, and the State Liaison Committee (SLC). The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

48. Which are the key nonbanking regulatory agencies and SROs?

Nonbanking regulatory agencies and SROs include, but are not limited to:

- **U.S. Securities and Exchange Commission (SEC):** The SEC is the federal regulator of the securities markets and administers the federal securities laws (including the Securities Act of 1933, the Securities Exchange Act of 1934, the Investment Company Act of 1940, the Investment Advisers Act of 1940 and the Trust Indenture Act of 1939), with direct regulatory and oversight responsibilities of securities exchanges, securities brokers and dealers, investment advisers and investment companies, and self-regulatory organisations (SROs).
- **Commodity Futures Trading Commission (CFTC):** The CFTC is the federal regulator of U.S. commodity futures and options markets in the United States. It administers and enforces the federal futures and options laws as set forth in the Commodity Exchange Act (CEA) and the accompanying regulations.
- **Financial Industry Regulatory Authority (FINRA):** Formerly known as the National Association of Securities Dealers (NASD), FINRA is an SRO for broker-dealers.
- **Federal Housing Finance Agency (FHFA):** Established by the Federal Housing Finance Regulatory Reform Act of 2008 as an independent agency of the federal government as the regulatory authority over housing government-sponsored enterprises (GSEs), Federal National Mortgage Association (Fannie Mae), Federal Home Loan Mortgage Corporation (Freddie Mac) and Federal Home Loan Banks (FHL Banks).
- **National Futures Association (NFA):** The NFA is the SRO for the futures market.
- **New York Stock Exchange (NYSE):** The NYSE is the SRO for exchange member organisations (i.e., a registered broker-dealer organised as a corporation, a partnership or an LLC that holds an NYSE trading license or opts for NYSE regulation).
- **National Indian Gaming Commission (NIGC):** The NIGC is an independent federal regulatory agency whose primary mission is to regulate gaming activities on Indian lands.

- **IRS Tax Exempt and Government Entities Division (IRS-TEGE):** The IRS-TEGE provides federal oversight to all nonprofit organisations in the United States, including reviews to determine if nonprofit organisations are facilitating terrorist financing.
- **IRS Small Business and Self-Employed Division (IRS-SBSE):** The IRS-SBSE has been delegated examination authority over all financial institutions that do not have a federal functional regulator as defined in the BSA, including MSBs, insurance companies, credit card companies, non-federally insured credit unions, casinos (tribal and nontribal), and dealers in precious metals, stones and jewels. The IRS-SBSE also has responsibility for auditing compliance with currency transaction reporting requirements that apply to any trade or business (Form 8300).

For further guidance on the AML/CFT responsibilities of broker-dealers, MSBs and other nonbank entities, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

49. Are financial institutions that do not have a federal functional regulator required to comply with AML/CFT laws and regulations?

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM), "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator," which will expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations
- State-chartered non-depository trust companies
- International banking entities

50. What are examples of agencies with responsibilities to combat money laundering, terrorist financing and proliferation of WMDs?

Key agencies with responsibilities to establish policies and strategies and coordinate efforts to combat money laundering, terrorist financing and the proliferation of WMDs include, but are not limited to, the following:

- U.S. Department of the Treasury
  - Financial Crimes Enforcement Network (FinCEN)
  - Office of Foreign Assets Control (OFAC)
  - Office of Terrorism and Financial Intelligence (TFI)
  - Office of Terrorist Financing and Financial Crimes (TFFC)

  - Office of Intelligence and Analysis (OIA)
  - Treasury Executive Office for Asset Forfeiture (TEOAF)
- U.S. Department of Justice (DOJ)
  - Federal Bureau of Investigation (FBI)
  - Drug Enforcement Administration (DEA)
  - Internal Revenue Service Criminal Investigation (IRS-CI)
  - Organised Crime Drug Enforcement Task Forces (OCDETF)
  - Asset Forfeiture and Money Laundering Section, Criminal Division (AFMLS)
  - Counterterrorism Section, Criminal Division (CTS)
  - Office of International Affairs, Criminal Division (OIA)
- U.S. State Department
  - Arms Control and International Security
    - Bureau of International Security and Nonproliferation (ISN)
    - Office of Cooperative Threat Reduction (ISN/CTR)
    - Office of Export Control Cooperation (ISN/ECC)
    - Export Control and Related Border Security Program (EXBS)
    - Office of Weapons of Mass Destruction Terrorism (ISN/WMDT)
    - Nuclear Smuggling Outreach Initiative (NSOI)
    - Global Initiative to Combat Nuclear Terrorism (GICNT)
    - Office of Nonproliferation and Disarmament Fund (ISN/NDF)
    - Bureau of Arms Control, Verification and Compliance (AVC)
    - Directorate of Defense Trade Controls (DDTC)
- Public Diplomacy and Public Affairs
  - Center for Strategic Counterterrorism Communications (CSCC)
- Economic Growth, Energy and Environment
  - Office of Threat Finance Countermeasures
  - Office of Terrorism Finance and Economic Sanctions Policy
- Civilian Security, Democracy and Human Rights
  - Bureau of Counterterrorism (CT)
  - Office of the Coordinator for Counterterrorism (S/CT)

  - Bureau of International Narcotics and Law Enforcement Affairs (INL)
  - Office to Monitor and Combat Trafficking in Persons (TIP)
- U.S. Office of the Director of National Intelligence (ODNI)
  - Central Intelligence Agency (CIA)
  - National Counterterrorism Center (NCTC)
  - National Counterproliferation Center (NCPC)
- U.S. Department of Homeland Security (DHS)
  - Immigration and Customs Enforcement (ICE)
  - Customs and Border Protection (CBP)
  - Domestic Nuclear Detection Office (DNDO)
- U.S. Department of Commerce
  - Bureau of Industry and Security (BIS) (formerly Bureau of Export Administration [BXA])
- U.S. Department of Defense (DOD)
  - Defense Threat Reduction Agency (DTRA)
- U.S. Department of Energy (DOE)
  - National Nuclear Security Administration (NNSA)
- U.S. Postal Service (USPS)
  - U.S. Postal Inspection Service (USPIS)

51. What AML/CFT publications and resources have been provided to the public by U.S. regulatory and/or law enforcement authorities?

Examples of AML/CFT publications and resources include, but are not limited to, the following:

- **FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Handbook** – Provides guidance to examiners for carrying out AML/CFT and OFAC examinations for depository institutions. The manual contains an overview of AML Program requirements, AML/CFT risks (e.g., products, services, transactions and customer types of heightened risk), risk management expectations, industry sound practices and examination procedures. To ensure consistency in the application of AML/CFT requirements, the development of this manual was a collaborative effort of the Federal Reserve, the OCC, the NCUA, the FDIC, FinCEN and the OTS (which has since been dissolved and replaced on the FFIEC by the CFPB).
- **Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses** – Provides guidance to examiners for carrying out AML/CFT and OFAC examinations for MSBs. The manual contains an overview of AML Program requirements, risk

management expectations, industry sound practices, examination procedures, overviews of the different types of MSBs (e.g., check cashers, currency dealers or exchangers, issuers of travellers checks and money orders, money transmitters), overview of the relationship between principals and agents, and additional guidance on MSB registration requirements, foreign agent or foreign counterparty due diligence, and recordkeeping and retention requirements for all types of MSBs. The development of this manual was a collaborative effort by the IRS, state agencies responsible for MSB regulations, the Money Transmitter Regulators Association (MTRA), the Conference of State Bank Supervisors (CSBS), and FinCEN.

- **Bank Secrecy Act Exam Resources** – Developed by the NCUA, this resource provides guidance to examiners for carrying out AML/CFT and OFAC examinations for credit unions, including, but not limited to, the following:
  - ***NCUA Compliance Self-Assessment Guide*** – Developed by the NCUA, this guide is intended for use by a credit union's board of directors and management, compliance officers, and others having responsibility for compliance as part of their duties. While the guide covers most federal consumer protection laws and regulations that affect credit unions, it does not address all federal laws or any state laws.
  - ***NCUA Examiner's Guide*** – Provides guidance (e.g., risk-focused approaches) to examiners to assist with determining scope and execution of examinations.
  - **AIRES Exam Questionnaires** – Automated Integrated Regulatory Examination System (AIRES) questionnaires, including, but not limited to, BSA, IT and Payment of Overdraft.
- **FFIEC Information Technology (IT) Examination Handbook** – Developed through a collaborative effort by the Federal Reserve, the OCC, the NCUA, the CFPB and the FDIC, the IT Examination Handbook covers key technology topics as they relate to financial services in separate booklets, including:
  - Audit
  - Business continuity planning
  - Development and acquisition
  - E-banking supervision of technology service providers
  - Information security
  - Management
  - Operations
  - Outsourcing technology services
  - Retail payment systems
  - Wholesale payment systems

The IT Examination Handbook provides guidance on topics such as risks and suggested controls on third-party payment processors (e.g., Automated Clearing House [ACH] providers, remote deposit capture [RDC] providers) and electronic payments (e.g., electronic banking, automated teller machine [ATM]).

- **Anti-Money Laundering Source Tool for Broker-Dealers** – Developed by the SEC to assist broker-dealers with fulfilling their responsibilities to establish an AML Program, as required by AML/CFT laws and regulations.
- **Anti-Money Laundering Template for Small Firms** – This template, available on FINRA's website, is designed to assist small firms in fulfilling their responsibilities to establish an AML Program, as required by the BSA and its implementing regulations and FINRA Rule 3310, by providing text examples, instructions, relevant rules, websites and other resources.
- **Anti-Money Laundering E-Learning Courses** – FINRA offers several e-learning courses and interactive scenarios on AML/CFT-related topics, ranging from customer identification procedures to recognising red flags.
- **U.S. Money Laundering Threat Assessment (MLTA)** – Published in 2005, the MLTA was written by several agencies, bureaus and offices, including, but not limited to, FinCEN, OFAC, FBI, DEA and the IRS. It contains detailed analyses of money laundering vulnerabilities across banking, insurance, casinos and MSBs.
- **National Money Laundering Risk Assessment (NMLRA)** – Published in 2015 as an update to the MLTA from 2005 by several federal agencies and offices, covering ML risks.
- **National Terrorist Financing Risk Assessment (NTFRA)** –Published in 2015 by many of the same federal agencies and offices that published the NMLRA, covering global terrorism and terrorist financing threats and counter-terrorism and CFT efforts.
- **National Money Laundering Strategy (NMLS)** – Written by the U.S. Departments of Homeland Security, Justice, Treasury, and State, as well as by the Federal Reserve, the OCC and the FDIC. The most recent NMLS was published in 2007 in direct response to the MLTA.
- **International Narcotics Control Strategy Report (INCSR)** – An annual report issued by the U.S. Department of State that describes the efforts to attack, country by country, all aspects of the international drug trade, as well as chemical control, money laundering and financial crimes.
- **Country Reports on Terrorism** – An annual report, previously known as Patterns of Global Terrorism, issued by the U.S. Department of State that provides overviews of terrorist activity in countries where acts of terrorism occurred, countries that are state sponsors of terrorism, and countries determined by the secretary of the U.S. State Department to be of particular interest in the global war on terror. The Country Reports on Terrorism also cover major terrorism-related events involving Americans; information on terrorist groups; terrorist sanctuaries; terrorist attempts to acquire WMDs; statistical information provided by the National Counterterrorism Center (NCTC) on individuals killed, injured or kidnapped by terrorist groups; and bilateral and multilateral counterterrorism cooperation.

- **Key OFAC Resources** – Multiple resources on OFAC Sanctions Programs, OFAC Sanctions Listings (e.g., Specially Designated Nationals and Blocked Persons List [SDN List]) and the development of a risk-based OFAC Sanctions Compliance Program. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

For additional guidance issued by key international groups, please refer to the International Perspectives and Initiatives section. For details on guidance specific to a particular topic (e.g., Suspicious Activity Reports [SARs], correspondent banking, politically exposed persons [PEPs], trade finance), please refer to the respective sections throughout this publication.

Financial Crimes Enforcement Network

52. What is the Financial Crimes Enforcement Network, and what is its role in AML/CFT regulation?

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Treasury Department, was established in 1990 by Treasury Order 105-08. Its mission is to safeguard the financial system from abuses of financial crime. It is the Financial Intelligence Unit (FIU) of the United States, formed to support law enforcement and the financial community in the fight against money laundering, terrorist financing and other financial crimes through the collection, analysis and sharing of BSA information. FinCEN seeks to provide adequate financial intelligence to law enforcement without overburdening the financial community or compromising the privacy of individuals.

While FinCEN relies primarily on federal functional regulators to examine financial institutions and enforce AML/CFT compliance, the regulators look to FinCEN for guidance in the implementation of the BSA and USA PATRIOT Act. FinCEN has issued regulations, in concert with federal functional regulators and the Internal Revenue Service (IRS), related to BSA compliance. FinCEN may issue enforcement actions for violations of the BSA and USA PATRIOT Act through its Enforcement Division jointly with other regulatory bodies or unilaterally. The Office of Enforcement evaluates enforcement matters, including the assessment of civil money penalties.

53. In what types of initiatives does FinCEN engage?

In 1992, under the authority of the Annunzio-Wylie Anti-Money Laundering Act, FinCEN formed the Bank Secrecy Act Advisory Group (BSAAG), a task force established to coordinate and inform the financial community about BSA-related matters. The BSAAG includes senior representatives from financial institutions, federal law enforcement agencies, regulatory agencies, and others from the public and private sectors. In 2009, the Financial Fraud Enforcement Task Force (FFETF) was established as a multiagency task force with federal, state and local partners to improve efforts to investigate and prosecute significant financial crimes, recover proceeds for victims, and address financial discrimination in the lending and financial markets.

FinCEN also has created several communication systems to facilitate the sharing of information among both domestic and international entities. The BSA E-Filing System allows financial institutions to file electronic BSA forms, such as CTRs and SARs, quickly and securely.

FinCEN Query is a web-based application for authorised users to access FinCEN data. Authorised users can apply filters, narrow search results, and import lists of data (e.g., names, addresses). FinCEN Query replaced the Web Based Currency and Banking Retrieval System (WebCBRS).

On behalf of the Egmont Group, FinCEN also developed the Egmont Secure Web (ESW), which is a private network that allows connected FIUs to interface with FinCEN and each other to access information related to money laundering trends, analytical tools and technological developments.

The many partnerships of FinCEN are not limited to the United States, but expand internationally to law enforcement, financial institutions and regulatory authorities in foreign countries, as well. FinCEN collaborates with other FIUs globally to exchange information supporting AML/CFT initiatives worldwide, and assists other countries with developing their FIUs. For additional guidance on FIUs, please refer to the Egmont Group of Financial Intelligence Units section.

54. What resources has FinCEN provided to the public?

Among the issuances and resources provided by FinCEN are the following:

- **Statutes and Regulations** – Resource that contains links to the following:
  - **Bank Secrecy Act (BSA)** statutes, including a BSA timeline, pending rulemakings and past comments on regulatory proposals.
  - **USA PATRIOT Act** statutes and related reports, including but not limited to 314(a) and 314(b) fact sheets.
  - **Chapter X** – Codified regulations by financial institution type.
  - **Federal Register Notices** – Links to final regulations issued after the date of codification as well as Notices of Proposed Rulemaking (NPRs) in the Federal Register by year and financial institution type.
  - **Guidance** – Clarification of issues or responses to questions related to FinCEN regulations (e.g., completion and filing of Suspicious Activity Reports [SARs]; applicability of the definition of a MSB to a particular business activity; applicability of the Safe Harbor provision when sharing SARs under certain circumstances).
  - **Administrative Rulings** – Rulings that provide a new interpretation of the BSA or any other statute granting FinCEN authority, express an opinion about a new regulatory issue, and/or outline the effect of the various releases on covered financial institutions.
  - **Advisories/Bulletins/Rulings/Fact Sheets** – An archive of advisories, advisory withdrawals, bulletins, rulings and fact sheets dating back to 1996.
- **Filing Information** – Resource that contains links to the following:
  - **BSA Forms** – Guidance for the filing of BSA Reports by financial institution type (e.g., depository institutions, casinos, MSBs, insurance industry, securities and

futures, precious metals/jewellery industry, mortgage companies and brokers, housing GSEs).

  - **E-Filing** – Guidance including frequently asked questions related to mandatory e-filings of BSA Forms, advisories and system updates.

- **Financial Institutions** – All of the above resources provided by financial institution type (e.g., depository institutions, casinos, MSBs, insurance industry, securities and futures, precious metals/jewellery industry, mortgage companies and brokers, housing GSEs).
- **Law Enforcement** – A summary of support services for law enforcement with links to resources for law enforcement agencies, including analytical support, strategic support, 314(a) requests, reference manuals and networking bulletins, direct access to BSA data, access to global network of financial intelligence units (FIUs), and case examples that have been assisted by information reported under BSA regulations.
- **International Programs** – Links to international resources, including but not limited to the Egmont Group of FIUs, FATF and Transnational Organised Crime.
- **News Room –** Links to the following resources:
  - **News Releases** – An archive of important FinCEN news releases dating back to 1994.
  - **Speeches, Testimony and Other** – An archive of speeches and testimony given by the director of FinCEN dating back to 2004.
  - **Reports and Publications** – Reports published periodically on key regulatory issues and strategies to address these issues, including, but not limited to, the following:
    - ***The SAR Activity Review: Trends, Tips & Issues*** – A publication produced periodically by FinCEN in cooperation with many regulatory, law enforcement and industry partners. The publication gives the public information and insight concerning the preparation, use and value of SARs filed by institutions.
    - **SAR Stats** (replaced *The SAR Activity Review: By the Numbers*) – A publication that provides numerical data on SAR filings (e.g., by type of financial institution, suspicious activity characterisations, product types, geography). Users can generate custom SAR Stat reports via FinCEN's website as well.
    - **Financial Institutions Outreach Initiative** – Reports sharing information gathered through various outreach initiatives with representatives in the financial services industry (e.g., large depository institutions, MSBs, prepaid access industry).

        - **Strategic Analytical Reports and Other Publications** – Publications addressing other trends and issues, such as mortgage loan fraud, suspicious activity in the gaming industry and identity theft.
        - **Annual Report** – Provides an overview of FinCEN's current state and details the strategies and outcomes of the year's operations.
        - **Reports to Congress** – An archive of reports made to Congress by the U.S. Secretary of the Treasury dating back to 2002, including the required annual 361(b) report.
        - **The Strategic Plan** – Published periodically, the Strategic Plan details how FinCEN intends to achieve its current goals in the near future.
    - **Enforcement Actions** – Links to enforcement actions dating back to 1999.
    - **Advisories/Bulletins/Fact Sheets**
- **Frequently Asked Questions (FAQ) Guides** – Answers to FAQs that include but are not limited to the following:
    - **Answers to Frequently Asked Bank Secrecy Act (BSA) Questions** – A list of basic questions and answers about BSA and USA PATRIOT Act laws and regulations.
    - **Frequently Asked Questions Regarding the FinCEN Currency Transaction Report (CTR)**
    - **Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (SAR)**
    - **Mandatory E-Filing FAQs**
    - **FinCEN's IT Modernization Efforts FAQs**
    - **Frequently Asked Questions: Final Rule: Definitions and Other Regulations Relating to Prepaid Access**
    - **Frequently Asked Questions: Casino Recordkeeping, Reporting, and Compliance Program Requirements**
- **Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses (2008)** – Guidance on the examination process of MSBs, in English and Spanish.

National and International Cooperation

55. How does FinCEN interact with other U.S. regulators?

In 2004, FinCEN entered into a Memorandum of Understanding (MOU) with the then existing federal banking regulators. The MOU sets forth procedures for the administration of the BSA, information relating to the primary federal regulators' policies and procedures for examination of BSA compliance; significant BSA compliance issues at banking organisations supervised by the regulators; and analytical data based on or derived from information provided by the regulators. The MOU also gives

FinCEN authority to issue its own enforcement actions, even when regulators may not think it is necessary. On April 26, 2005, FinCEN and the New York State Banking Department entered into a similar MOU; shortly thereafter, a number of other states followed suit.

In late 2006, the SEC and FinCEN entered into an MOU under which the SEC provides FinCEN with detailed information on a quarterly basis regarding the AML/CFT examination and enforcement activities of the SEC and the Self-Regulatory Organisations (SROs). In return, FinCEN provides assistance and analytical reports to the SEC.

In June 2011, FinCEN entered into an MOU with the CFPB, which provides the CFPB direct electronic access to BSA information and analytical materials (e.g., analytical tools, BSA information reviews) as required and appropriate for the exercise of the CFPB's regulatory authority. In return, the CFPB, upon request, will provide reports on the results of its investigations or examinations and statistical information related to any inquiries to assist FinCEN in understanding and analysing the value of BSA information.

Beginning in 2012, FinCEN entered into MOUs with multiple state insurance regulators, including California, Kansas, Louisiana, Nebraska, and Wisconsin as well as with Washington, D.C., with other states expected to follow.

56. What mechanisms are in place to facilitate international cooperation in combating money laundering and terrorist financing?

To facilitate international cooperation among FIUs, law enforcement authorities and regulatory authorities in relation to money laundering and terrorist financing, the United States has implemented the following:

- Ratification of international treaties (e.g., Vienna Convention, 1988; the Palermo Convention, 2000; the United Nations Convention against Corruption, 2003; the Terrorist Financing Convention, 1999)
- Establishment of FinCEN to facilitate information requests, communications and training with other FIUs
- Establishment of a legal framework to provide mutual legal assistance to international authorities, including, but not limited to, extradition requests and the freezing and confiscation of property related to money laundering and terrorist financing

In 2013, FinCEN entered into the first-ever MOU with Mexican authorities to enhance coordination on a variety of AML/CFT initiatives to combat transnational organised crime. In 2015, FinCEN entered into an MOU with the China Anti-Money Laundering and Analysis Center (CAMLMAC).

For additional guidance on international cooperation, please refer to the International Perspectives and Initiatives section. For additional guidance on asset forfeiture, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

57. What is the primary authority responsible for managing requests for mutual legal assistance (MLA)?

The DOJ's Office of International Affairs, Criminal Division (OIA) is the primary authority to manage MLA requests to and from the United States.

58. Can foreign financial institutions without a U.S. presence be impacted by U.S. AML/CFT laws beyond requests for international cooperation?

Even though the specific requirements of U.S. AML/CFT laws are not applicable to foreign financial institutions (FFI) that operate exclusively outside of the United States, U.S. AML/CFT laws, nonetheless, have a significant impact on financial institutions across the globe.

Specifically, several provisions of the USA PATRIOT Act can have significant effects on non-U.S. financial institutions. In summary, these requirements could result in the following:

- Additional information requests about the financial institution itself and its customers if their transactions are processed through a U.S. financial institution
- Seizures of a financial institution's funds maintained in an account in the United States
- Sanctions against either the financial institution itself or the country from which it operates

These measures are far-reaching; global financial institutions must be aware of their potentially significant impact. For further guidance, please refer to the USA PATRIOT Act section.

Enforcement Actions

59. What types of enforcement actions are available to regulators for addressing AML Program deficiencies and violations?

Regulators have a range of enforcement tools available to address AML Program deficiencies and violations of AML/CFT laws and regulations.

While enforcement actions against nonbanks have increased in recent years, the number of enforcement actions issued by bank regulators continues to outnumber those of other agencies, at least in the United States. Examples of enforcement actions available to U.S. bank regulators in order of severity are:

- **Commitment Letter**: A Commitment Letter is an agreement between a bank's board of directors and a bank regulator in which the board, on behalf of a bank, agrees to take certain actions to address issues or concerns surfaced by the regulator. A Commitment Letter is not legally binding, but the failure of a bank to live up to the terms of the Commitment Letter may subject the bank to more formal regulatory action.
- **Memorandum of Understanding (MOU)**: An MOU is an agreement between a bank's board of directors and one or more regulatory agencies. The content of an MOU may be similar or identical to more formal enforcement actions, but MOUs are non-public documents and, similar to Commitment Letters, not legally binding.

- **Formal Agreements**: A Formal Agreement is an agreement between a bank's board of directors and one or more regulatory agencies. While the contents of a Formal Agreement may mirror those of an MOU, violations of a Formal Agreement can provide the legal basis for assessing civil money penalties (CMPs) against directors, officers and other institution-affiliated parties.
- **Consent Order or Order to Cease and Desist (C & D)**: Consent Orders and Orders to Cease and Desist are agreements between a bank's board of directors and one or more regulatory agencies. Violations of a Formal Agreement can provide the legal basis for assessing civil money penalties (CMPs) against directors, officers and other institution-affiliated parties. The regulator's decision to issue a Consent Order or Order to Cease and Desist rather than a formal agreement is based on its assessment of the severity of the bank's problems.
- **Civil Money Penalties (CMPs)**: CMPs are financial penalties that may be imposed by a regulator against a bank or an individual(s) for a violation of a law or regulation or noncompliance with a formal enforcement action.
- **"Death Penalty"**: Under the Annunzio-Wiley Act of 1992, bank regulators are obligated to consider whether the license/charter of a depository institution that is found guilty or pleads guilty to money laundering charges should be revoked. The revocation of a license/charter is known as the "Death Penalty."

Unlike the formal enforcement actions issued by bank regulators, which are usually very prescriptive as to the actions that must be taken to address the identified deficiencies, the enforcement actions taken by securities and futures/commodities regulators generally report findings that detail the nature of the deficiency, but do not prescribe specific corrective action (and accompanying fines have been modest compared to those levied against banks).

60. Beyond the actions and penalties that may be imposed by regulators, are U.S. companies subject to any other potential actions?

Yes. Other actions, such as Deferred Prosecution Agreements (DPA), may result from legal actions.

61. What is a Deferred Prosecution Agreement?

A DPA is an agreement entered into between a prosecutor and a defendant in a criminal case whereby in exchange for successful completion of agreed-upon commitments, the criminal charges against the defendant will be dismissed in their entirety by the prosecutor.

62. How are violations of law characterised by the regulators?

Some common themes have been:

- **Program Violations:** Overall failures supported by "pillar" violations (i.e., the failure of an institution to address adequately its obligation to designate a qualified AML compliance officer; develop and implement appropriate policies, procedures and controls; provide adequate training; and perform periodic independent testing of its AML Program).
- **Systemic and Recurring Violations**: Pervasive control breakdowns.

- **Isolated and Technical Violations:** Limited instances of noncompliance that do not threaten overall program effectiveness.

63. What are some common deficiencies that have been identified in recent enforcement actions and settlements?

The following areas are some of the common deficiencies in AML/CFT compliance programs that have been identified in recent enforcement actions:

- Inadequate and inconsistent AML/CFT policies and procedures
- Deficient AML/CFT risk assessments and risk management program:
  - Lack of understanding of AML/CFT risks and risk assessment methodology
  - Lack of understanding of financial institution's overall risk appetite
  - Lack of coverage of all customers, products/services and geographies
  - Inadequate application across enterprise (e.g., lines of business, support units, legal entities)
  - Outdated risk assessments
- Deficient KYC/CDD/EDD programs
  - Failure to address CDD and EDD for high-risk customers and products/services (e.g., beneficial owners, PEPs, MSBs, foreign correspondents, remote deposit capture services [RDCS])
- Inadequate suspicious activity monitoring program and suspicious activity report (SAR) filing program, including, but not limited to, the following deficiencies:
  - Lack of alignment with the AML/CFT risks of the financial institution
  - Lack of coverage of high-risk customers/transactions leading to the failure of filing SARs on potentially suspicious activities (e.g., high-volume trading)
  - Incomplete data feeds into transaction monitoring system
  - Errors in transaction monitoring rules
  - Lack of periodic reviews and validation of transaction monitoring rules
  - Failure to investigate alerts triggered in automated transaction monitoring systems
  - Unsustainable monitoring procedures leading to backlogs of aging alerts
  - Lack of or inadequate escalation procedures to senior management for significant investigations
  - Poor documentation of clearing alerts (e.g., not entered into case management system)
  - Failure to file timely SARs

  - Filing of SARs with poor narratives

- Inadequate structuring, resources and training of AML/CFT compliance officer and staff
  - Inadequately defined roles between compliance and operations staff leading to a conflict of responsibilities
  - Insufficient number of staff to evaluate suspicious activity monitoring alert in a timely manner
  - Inadequate skill level of compliance personnel to evaluate suspicious activity monitoring alerts and investigations properly
  - Poor communication or wilful miscommunication between compliance personnel and senior management on significant matters
- Insufficient independent testing of AML/CFT compliance programs
- With respect to MSBs, inadequate due diligence of agents
  - Failure to terminate relationships with agents responsible for significant suspicious activity (e.g., elder financial exploitation)

The following areas are some of the common deficiencies in OFAC compliance programs that have been identified in recent OFAC settlements:

- Wilful violations of sanctions programs (e.g., the Iranian Transactions and Sanctions Regulations [ITSR], Cuban Assets Control Regulations)
- Processing of transactions in a nontransparent manner to evade sanctions restrictions
  - Utilisation of third parties to process transactions to circumvent sanctions controls
- Failure to screen high-risk customers and products/services (e.g., import-export letters of credit) against sanctions lists

AML/CFT Compliance Program

64. What are the key elements of an effective AML/CFT governance framework?

Among the keys to establishing and maintaining an effective AML/CFT governance framework are:

- Strong and evident support of the board of directors and executive management for a culture of compliance, which is reinforced, among other ways, through a clearly defined risk appetite statement, appropriate limits, and the institution's performance review and compensation decisioning processes.
- A designated AML compliance officer with the necessary skills, authority and support to manage the AML/CFT Compliance program across the entire organisation.

- An adequate number of dedicated skilled resources, which will be determined by factors such as the size, complexity and geographic reach of the institution as well as the extent to which the compliance effort is enabled by technology.
- Robust policies and procedures that contain clear delineation of roles and responsibilities of the first, second and third lines of defence including obligations for "credible challenge" or "effective challenge."
- Effective, dynamic processes for assessing money laundering/terrorist financing and sanctions risk.
- AML training, which is appropriately customised to different audiences within the institution.
- A strong working relationship among the AML/CFT compliance organisation and other groups within the organisation (such as Legal and Fraud) with which the AML/CFT compliance organisation would be expected to interact.
- Appropriately selected and maintained technology to support, as examples, transaction monitoring and sanction screening.
- Robust management reporting that includes the necessary metrics to measure and monitor risks and performance.
- Ongoing monitoring and periodic independent testing of the effectiveness of the program.

65. How can financial institutions develop risk-based compliance programs?

Financial institutions are expected to develop and maintain risk-based compliance programs. For financial institutions, the development of a risk-based program begins with evaluating the risks of customer types, products/transactions, and geographies within the enterprise and developing appropriate measures to mitigate those identified risks. Financial institutions can utilise risk assessments in the design and application of their compliance programs in many ways, including, but not limited to, the following:

- Development of an AML/CFT strategy (e.g., discontinue or prohibit the provision of products and services of heightened ML/TF risks)
- Allocation of resources (e.g., personnel, technology) to high-risk areas
- Design and application of a Know Your Customer (KYC) program
- Design and application of a suspicious activity monitoring program
- Design and application of sanctions screening program
- Development and provision of targeted training

66. What is a risk assessment?

The Financial Action Task Force (FATF) defines a risk assessment as "a process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand … risks and serves as a first step in addressing them and making judgments" about identified risks.

There are many different types of risk assessments. Risk assessments may be designed to measure the following on a line of business or at an enterprise level:

- Inherent risks;
- Controls or control environment (e.g., strengths/deficiencies in a compliance program); and
- Residual risk

Other risk assessments, such as ones performed to assess product/service risk or geographic, may only measure inherent risk of these factors and may be used as inputs in an organisation's other risk assessments.

67. What is inherent risk?

Inherent risk is the risk to an entity in the absence of any actions management might take (e.g., controls) to alter either the risk's likelihood or impact.

68. What is a control?

A control is a process, designed and/or performed by an entity, to mitigate or reduce the likelihood or impact of a risk. Control processes may be manual, automated, proactive and/or reactive.

In terms of a financial institution's AML/CFT Compliance Program, the following are examples of controls:

- The financial institution sets a policy prohibiting the offering of products/services to a particular type of customer (e.g., money services businesses).
- Supervisors or managers review and approve a documentation checklist, completed by an account officer, prior to account opening, as a control to ensure the necessary customer information is collected according to the financial institution's policies and procedures.
- The financial institution's systems require the input of necessary customer information before the account officer can proceed to the account opening screen as an automated control to ensure the necessary customer information is collected according to the financial institution's policies and procedures.
- The financial institution may require more frequent updating of customer information or the performance of periodic site visits.
- The financial institution utilises an automated monitoring system to detect potentially suspicious activity.

69. What is residual risk?

Residual risk is the risk remaining after all controls have been applied to reduce the likelihood or impact of the risk. An acceptable level of residual risk is determined by the risk appetite or tolerance of the financial institution.

70. Are there customer types, products, services or transactions that pose no risk of money laundering or terrorist financing?

No. Every customer type, product, service or transaction poses some degree of risk of money laundering and terrorist financing; therefore, it is recommended that "zero" not be used when assigning risk to customer types, products, services and transactions. However, some customers, products, services and transactions may pose only a very minimal risk, such as a customer who performs a onetime, low-dollar amount transaction or only has direct deposits of payroll and performs only low-dollar transactions.

71. What types of customers pose a higher money laundering and terrorist financing risk?

Business types and occupations considered to be at high risk for money laundering and terrorist financing include those that are cash-intensive; those that allow for the easy conversion of cash into other types of assets; those that provide the opportunity to abuse authoritative powers and assist in disguising the illegal transfer of funds; those that lack transparency; those that involve international transactions/customers; and those that offer high-risk or high-value products.

72. What products/services/transactions pose a higher money laundering and terrorist financing risk?

Products/services that allow unlimited third-party transactions (e.g., demand deposit accounts), those that operate through channels with limited transparency (e.g., internet banking, telephone banking, pouch activity, prepaid access, ATM, trust), and those that may involve significant international transactions (e.g., correspondent banking) pose the highest risk.

Transactions that are processed quickly and electronically for customer convenience (e.g., wire transfers), are difficult to trace (e.g., cash), and are negotiable (e.g., monetary instruments, drafts, bearer securities, stored-value cards) also are susceptible to money laundering and terrorist financing.

73. What factors affect whether a jurisdiction poses a higher money laundering and terrorist financing risk?

Financial institutions should develop an objective approach to determine which countries should be considered at increased risk of money laundering or terrorist financing. Factors that can be considered include, but are not limited to, the following:

- Strength of AML/CFT system (e.g., legal and regulatory framework)
- Subject to government sanctions
- Degree of corruption

- Designation as a state sponsor of terrorism
- Designation as a tax haven
- Strength of secrecy laws (i.e., favours/encourages secrecy)
- Designation as a drug trafficking region
- Designation as a human trafficking/smuggling region

74. Are high-risk jurisdictions limited to international locations?

No. High-risk geographic locations may include domestic locales, such as financial institutions doing business within, or having customers located within, a U.S. government-designated high-risk geographic location.

75. What is "de-risking"?

De-risking often refers to a financial institution's policy to exit from a high-risk customer group or activity to reduce its inherent risk profile. To avoid risk, as opposed to managing risk, some financial institutions may opt out of offering services to certain categories of high-risk customers (e.g., foreign correspondents, money transmitters, marijuana-related businesses [MRBs]) or customers located in high-risk geographies. While this may reduce risk and simplify the KYC and suspicious activity monitoring programs of individual financial institutions, it may increase overall money laundering risk in the system as money is moved through less transparent or less regulated financial systems (e.g., hawalas, financial institutions in lax AML/CFT jurisdictions).

Many financial institutions have taken steps to de-risk because of perceived regulatory pressures. U.S. and international authorities, however, have released guidance cautioning against wholesale de-risking while attempting to provide further clarification on regulatory expectations on servicing inherently high-risk customers (e.g., Office of the Comptroller of the Currency [OCC] Risk Management Guidance on Foreign Correspondent Banking, Federal Deposit Insurance Corporation [FDIC] Financial Institution Letter: Statement on Providing Banking Services, Financial Action Task Force [FATF] Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking, International Monetary Fund [IMF] The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action).

For further guidance on risk assessments, please refer to the Risk Assessments section.

76. What types of risk assessments can a financial institution conduct to develop a risk-based AML/CFT Compliance Program?

Financial institutions can conduct the following types of risk assessments to develop a risk-based AML/CFT Compliance Program:

- **Enterprisewide risk assessment –** An exercise intended to identify the aggregate money laundering (ML) and terrorist financing (TF) risks facing an organisation that may not be apparent in a risk assessment focused on a line of business, legal entity, or other assessment unit. In other words, it is the big picture view, or profile, of an organisation's ML/TF risks that aggregates the

results of other risk assessment exercises in order to quantify and relate the total risks for the organisation to the established risk appetite and tolerance for the enterprise.

- **Horizontal risk assessment –** An exercise intended to identify systemic ML/TF risks of designated high-risk products/services and/or customers across an organisation regardless of which line of business or legal entity owns these activities or customers.
- **Line of business (LOB)/legal entity (LE) risk assessment –** An exercise intended to identify the level of vulnerability of each line of business (LOB) or legal entity (LE) to ML/TF. This is accomplished by evaluating, for a specific LOB or LE, among other factors, the ML/TF risks of products/services, the customer base (e.g., type, location) and geography (e.g., customers, transactions, operations) and the controls (e.g., policy and procedures, customer acceptance and maintenance standards, transaction monitoring, management oversight, training, personnel) mitigating those risks at the business line or legal entity level.
- **Product/transaction/service risk assessment –** An exercise intended to identify the inherent ML/TF risks of the products, transaction types and services offered by a financial institution.
- **Geographic risk assessment –** An exercise intended to identify the inherent ML/TF risks of the international and domestic jurisdictions in which a financial institution and its customers conduct business.
- **Customer risk assessment –** An exercise intended to identify the level of inherent ML/TF risks in the types of customers (e.g., individual, institutional, financial institution, not for profit) served by a financial institution.
- **OFAC/Sanctions risk assessment –** An exercise intended to identify an organisation's level of vulnerability to noncompliance with economic sanctions administered by OFAC or any sanctions program as required by the financial institution's policy. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types, the geographic origin and destination of transactions, and the strength of the controls mitigating those risks.

77. With which key AML/CFT and sanctions requirements are depository institutions required to comply?

Depository institutions must comply with the following key federal AML/CFT requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, conducts an independent review of the AML Program and conducts ongoing monitoring and updates (Section 352 of the USA PATRIOT Act)
- Establishment of a Customer Identification Program (CIP) (Section 326)
- Establishment of a customer due diligence program that identifies beneficial owners under select circumstances (Section 312, Beneficial Ownership Rule)
- Filing of Suspicious Activity Reports (SARs)

- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- Complying with Special Measures (Section 311)
- Obtaining Foreign Bank Certifications (Section 319(b))
- Establishing an EDD program for foreign correspondent account relationships, private banking relationships and PEPs
- OFAC and other sanctions requirements

For additional guidance on the various AML/CFT requirements for nonbank financial institutions (NBFIs), please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

78. What are key elements of an effective AML Program as required by Section 352 of the USA PATRIOT Act?

At a minimum, Section 352 requires financial institutions to establish AML Programs, which previously included the following "four pillars":

- Development of written internal policies, procedures and controls
- Designation of an AML compliance officer
- Ongoing AML employee-training program
- Independent testing of the AML Program

Since FinCEN issued the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) in July 2016, a fifth pillar has been added to the AML Program:

- Ongoing risk-based monitoring of customer activity and information with updates as necessary

The Beneficial Ownership Rule did not add new AML/CFT requirements for financial institutions; it only served to make existing AML/CFT expectations explicit requirements for the sake of clarity and consistency. The fifth pillar emphasises the importance of current and complete customer due diligence to support the identification of suspicious activity.

Section 352 is implemented for depository institutions under 31 C.F.R. 1020.210 – Anti-Money Laundering Program Requirements for Financial Institutions Regulated Only by a Federal Functional Regulator, Including Banks, Savings Associations and Credit Unions.

79. What are the key components of an AML/CFT Compliance Program?

To distinguish the AML Program with "five pillars" pursuant to Section 352 of the USA PATRIOT Act, this publication will use "AML/CFT Compliance Program" when referencing the expanded program that includes the following components:

- **Board of Director and Senior Management Support and Oversight**, supported and evidenced by adequate investment in the AML/CFT Compliance Program.
- **Designation of an AML Compliance Officer and Well-Defined Roles and Responsibilities** – For further guidance, please refer to the Designation of AML Compliance Officer and the AML/CFT Compliance Organisation section.
- **Risk Assessments** – For further guidance, please refer to the Enterprisewide Risk Assessment, Line of Business/Legal Entity Risk Assessment, Horizontal Risk Assessment, Geographic Risk Assessment, Product/Service Risk Assessment, Customer Risk Assessment and OFAC/Sanctions Risk Assessment sections.
- **Customer Acceptance and Maintenance Program** – For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence, Section 326 – Verification of Identification, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Beneficial Owners sections.
- **Large Currency Monitoring and Currency Transaction Report Filing Program** – For further guidance, please refer to the Currency Transaction Reports section.
- **Monitoring, Investigating and Suspicious Activity Report Filing Program** – For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Reports sections.
- **OFAC Sanctions Compliance Program** – For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs and International Sanctions Program section.
- **Model Governance over Enabling Technologies** – For further guidance, please refer to the AML/CFT Technology section.
- **Information Sharing** – For further guidance, please refer to Section 314(a) – Cooperation Among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities, Section 314(b) – Cooperation Among Financial Institutions and Section 505 – Miscellaneous National Security Authorities (National Security Letters [NSLs]) sections.
- **BSA Recordkeeping and Retention Program** – For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule, Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, Form 8300, Report of Foreign Bank and Financial Accounts and Report of International Transportation of Currency or Monetary Instruments sections.
- **Independent Testing** – For further guidance, please refer to the Independent Testing section.

- **Training** – For further guidance, please refer to the AML Training section.

It is important to note that not all types of financial institutions may be required to have each of the key components listed above. For additional guidance on the AML/CFT requirements of nonbank financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

80. What are the key components of an OFAC Sanctions Compliance Program?

Unlike AML/CFT laws and regulations, OFAC does not dictate specific components of compliance programs; however, financial institution regulators do expect companies to develop compliance programs. An effective OFAC Sanctions Compliance Program should include the following:

- Performing a sanctions risk assessment.
- Developing risk-based internal controls for OFAC compliance, including screenings and reviewing of customers and transactions, as appropriate, against lists of sanctioned entities.
- Blocking/rejecting transactions with designees on OFAC Sanctions Listings
- Reporting blocked or rejected transactions
- Designating an individual to be responsible for OFAC compliance
- Developing and implementing written OFAC policies and procedures
- Conducting an OFAC/sanctions risk assessment
- Conducting comprehensive and ongoing training
- Designing and maintaining effective monitoring, including timely updates to the OFAC filter
- Periodic, independent testing of the program's effectiveness, including validation of enabling technology.

81. What is a culture of compliance?

A culture of compliance is one in which management and staff of an organisation do the right thing because they know it is what is expected and the organisation will support them and where they are not afraid to surface compliance issues for fear of retribution or retaliation.

82. How can financial institutions cultivate a strong culture of compliance?

In August 2014, FinCEN issued an advisory suggesting how financial institutions can cultivate a strong culture of compliance through:

- Efforts to manage and mitigate AML/CFT deficiencies and risks are not compromised by revenue interests;
- Implementation of an effective AML/CFT Compliance Program that is tested by independent and competent parties;
- Adequate human and technological resources dedicated to AML/CFT compliance function;

- Active support and understanding of AML/CFT and sanctions compliance efforts by leadership and employees; and
- Strong information-sharing mechanisms in place between lines of business and AML/CFT compliance with a mutual understanding of how BSA reports and data further AML/CFT efforts.

Some common practices to encourage compliance throughout the financial institution include:

- Ensuring consistency between the practices of the institution and written policies and procedures
- Embedding compliance requirements into business processes
- Ensuring timely communication between the compliance department and senior management on compliance matters
- Establishing roundtables or group forums around compliance matters
- Conducting customised compliance training sessions for lines of business
- Requiring attestation to a code of conduct as a condition of employment
- Communicating and enforcing specific and clear consequences for noncompliance
- Factoring compliance into compensation decisions
- Developing key performance indicators (KPIs) for measuring the effectiveness of the compliance program

The sentiments expressed by FinCEN have since been echoed by other regulators and encouraged by the industry itself.

83. How can technology be used to support a financial institution's AML/CFT Compliance Program?

Technology can be used, for example, to support:

- **Monitoring for Suspicious Transactions and Filing Suspicious Activity Reports**– For further guidance, please see the Monitoring, Investigating and Filing of Suspicious Activity Reports (SARs) section.
- **Large Currency Transaction Monitoring and Filing of Currency Transaction Report**– For further guidance, please see the Large Currency Transaction Monitoring and Filing of Currency Transaction Reports (CTRs) sections.
- **Facilitation of the KYC Process including Verification of Customer Information (e.g., CIP)** – For further guidance, please see the sections Customer and Transaction List Screening and KYC Process.
- **Calculation of Customer Risk Ratings** – For further guidance, please see the Risk Assessment Automation section.

- **Screening Against Special Lists of Prohibited and/or High-Risk Individuals/Entities (e.g., Office of Foreign Assets Control [OFAC], 314(a), Subpoenas, Media Searches, Internal "Deny" Lists, PEPs) for Customers and Transactions** – For further guidance, please see the Customer and Transaction List Screening section.
- **AML Training** – For further guidance, please see the Training Software section.
- **Management Reporting –** For further guidance, please see the Management Reporting section.
- **Data Analytics and the Development of Models –** For further guidance, please refer to the sections Model Validation and Data Analytics.

Additionally, multiple vendors providing regulatory solutions, often referred to as "regtech," are providing agile cloud-based technology solutions for KYC repositories and customer verification across the globe. For further guidance on technology solutions, please refer to the AML/CFT Technology section.

84. What have been the most common deficiencies in AML/CFT Compliance Programs?

Some common problems and issues include, but are not limited to, the following:

- Inadequate board of director and senior management oversight
- AML compliance officer (as well as other employees) lacks sufficient experience and/or knowledge regarding AML/CFT policies, procedures and tools
- Insufficient/inadequate investment in and resources dedicated to AML/CFT compliance
- Lack of specific and customised training of employees with critical functions (e.g., account opening, transaction processing, risk management)
- Failure to conduct adequate risk ratings (e.g., enterprisewide risk assessment, customer risk assessment, OFAC/sanctions risk assessment)
- Failure to incorporate risk assessments into a transaction-monitoring process, customer acceptance standards, audits, testing or training
- Inadequate Know Your Customer (KYC) procedures (e.g., CIP, CDD and EDD at or after account opening, including inadequate controls over required fields, inadequate methods of obtaining and/or maintaining current information, lack of reporting capabilities over missing information, and lack of verification procedures)
- Poor documentation maintained for investigations that did not lead to SAR filings
- Poor follow-up on SAR actions (e.g., close account, monitor)
- Lack of reporting of key SAR information to senior management/board of directors
- Failure to perform adequate due diligence when selecting third party technology vendors to support compliance efforts
- Inadequate customisation of third party transaction monitoring systems

- Inadequate tuning, validation and documentation of automated monitoring systems
- Overreliance on software to identify transactions for which CTRs and/or SARs must be filed without fully understanding how the software is designed and what information it does/does not capture
- Exclusion of certain products from transaction monitoring (e.g., loans, letters of credit, capital markets activities)
- Lack of timeliness when filing CTRs and SARs (e.g., reports are manually filed via certified mail, and the date postmarked is not noted)
- Lack of or inadequate independent testing of the AML Program
- Lack of or untimely corrective actions to prior examination or audit findings

To identify potential gaps in a financial institution's AML/CFT Compliance Program, regulatory enforcement actions for AML/CFT deficiencies against other (similar) financial institutions should be reviewed to identify the specific gaps and violations and related action steps. This enables financial institutions to recognise and correct any potential weaknesses of their own before their next regulatory examination.

85. What are some of the common challenges to maintaining an effective OFAC Sanctions Compliance program?

The following include some of the challenges that companies have experienced in implementing an OFAC Sanctions Compliance Program:

- Updates to OFAC Sanctions Listings (e.g., Specially Designated Nationals and Blocked Persons List [SDN List], Sectoral Sanctions Identification List [SSI List], Foreign Sanctions Evaders List [FSE List]) are not incorporated in a timely manner
- Inadequate OFAC training and/or understanding of the various sanction programs
- Overreliance on third parties to perform the OFAC screening (e.g., correspondent banks, intermediary banks, third-party service providers)
- Inadequate and poor documentation of due diligence in clearing potential OFAC matches
- Poor "white list" management
- Poor record retention
- Existing customers, employees or third-party service providers (e.g., vendors, consultants) are not screened against OFAC Sanctions Listings, and/or updates to the list are performed infrequently, if at all (e.g., safe deposit box customers who do not have deposit accounts, noncustomers or parties involved in letters of credit)
- Certain transactions (e.g., checks, monetary instruments, ACHs, cover payments) are not screened against OFAC Sanctions Listings

- Updates to the OFAC Sanctions Listings are not performed timely
- Lack of screening beyond originator and beneficiary fields (e.g., cover payments often list originator/beneficiary in additional fields that may not be screened in interdiction software), and additional address fields (e.g., physical, mailing, alternate)
- Ineffective use of interdiction software:
  - Utilisation of high confidence levels for matches (e.g., 100 percent), thereby preventing possible hits from generating alerts for further review
  - Implementation of inconsistent matching algorithms/confidence levels across products, transactions, customers and/or departments
  - Ineffective use of exclusion features, thereby suppressing potential hits

86. How can multinational financial conglomerates manage their AML/CFT compliance efforts?

For multinational financial conglomerates subject to different AML/CFT requirements for each of their diverse business areas, as well as each jurisdiction in which they operate, the coordination of AML/CFT compliance efforts can be particularly challenging. Even further, common requirements do not necessarily mean common implementation or enforcement.

Institutions will benefit from AML/CFT compliance efforts being as consistent as possible throughout their global operations by, for example, adopting common standards for customer due diligence and enhanced sue diligence and risk assessments. While full consistency is not desirable (e.g., because one jurisdiction may have far more burdensome requirements) or simply cannot be achieved due to the differing business and jurisdictional requirements, the most efficient AML/CFT Compliance Program can be developed by an institution's headquarters to incorporate as many common characteristics as possible. The program then can be further customised across different businesses and jurisdictions to include the specific requirements of those businesses/countries.

Whenever possible and permissible under governing privacy and data transmission laws, centralisation of key monitoring functions, or at least internal sharing of monitoring results among global compliance departments, allows an institution to take a holistic approach to the AML/CFT Compliance Program.

87. What are some obstacles to establishing a global AML/CFT Compliance Program?

One of the biggest challenges in establishing a global AML/CFT Compliance Program is adopting one global standard that meets the specific requirements of each country's AML/CFT laws and regulations. Although the overarching goal is very similar, the individual requirements are different. Global institutions typically implement a global policy with minimum requirements, often dictated by the location of the head office, and adopt local procedures at international locations. It can be difficult for the other offices to meet minimum standards if they are set too high, especially if local resources lack the requisite experience and knowledge and if their local competitors are not implementing such tight controls.

Multinational institutions also are facing the challenge of implementing transaction-monitoring systems on an enterprise level. Systems may need to apply custom rules/parameters to each jurisdiction and accommodate different time zones and currencies.

Another potential obstacle that multinational institutions must consider is the different privacy/data transmission laws and regulations that may exist in the jurisdictions in which the company operates. In some cases, these privacy regulations restrict the use of information and/or cross-border movement of information and may impose significant data protection fines for violations (e.g., General Data Protection Regulation [GDPR]).

Preparing for examinations and responding to regulators across the globe can prove difficult, because even when requirements are similar, understanding the nuances, examination approaches and foci can be minefields for the most seasoned compliance officer.

For guidance on AML/CFT requirements for U.S. financial institutions, please refer to the sections: Bank Secrecy Act, USA PATRIOT Act and Nonbank Financial Institutions and Nonfinancial Businesses.

88. Should multinational institutions organise their AML/CFT compliance functions the same way in every jurisdiction in which they operate?

To the extent feasible, there are advantages to having a consistently designed AML/CFT compliance function in every jurisdiction in which a financial institution operates. However, it is important to note that regulatory bodies in some jurisdictions have strong views on how compliance functions are organised and to whom the AML compliance officer reports; in these cases, it is important to make adjustments to respect the local requirements and expectations.

89. How does the AML/CFT Compliance Program converge with other compliance efforts combatting fraud and bribery?

Conceptually, the idea of merging AML/CFT and anti-fraud activities is widely embraced, but the actual seamless merger of process and technology has yet to be accomplished broadly in the industry today.

Historically, AML/CFT and anti-fraud programs viewed their missions as separate and distinct. Anti-fraud managers focused their efforts on internal and external embezzlement schemes resulting in financial loss to the institution, while AML/CFT managers primarily sought to protect the institution against money launderers and terrorists through the detection of potentially suspicious activity and potential sanctions violations. Today, many financial institutions recognise that most perpetrators of fraud schemes seek to launder their ill-gotten gains and most money launderers have committed other fraud. From this perspective, anti-fraud units and AML/CFT units have a shared mission that is quite clear: to prevent and detect criminal activity.

Financial institutions that are considering integrating AML/CFT Compliance and ABC Compliance Programs are motivated by the potential synergies afforded through cross channel alerts, access to broad financial intelligence, and the possibility of cost savings by leveraging technology platforms and pooling resources. Financial regulators, as well as the Director of FinCEN, have also expressed support

for a combined approach with other compliance departments (e.g., AML/CFT and anti-fraud) to take advantage of the potential efficiencies.

For further guidance, please refer to the following sections:

- AML/CFT and Anti-Fraud Programs
- Mortgage Fraud
- Identity Theft and Identify Theft Prevention Program
- Cyber Events and Cybersecurity
- Elder Financial Abuse
- Anti-Corruption and Bribery Compliance Program
- Offshore Tax Evasion, Voluntary Tax Compliance and Foreign Account Tax Compliance Act
- Illegal Internet Gambling and Fantasy Sports Wagering

90. Are financial institutions expected to take on the responsibilities of law enforcement when combating money laundering and terrorist financing?

No. A financial institution is required to report suspicious activity that may involve illicit activity; a financial institution is not obligated to determine, confirm or prove the underlying predicate crime (e.g., terrorist financing, money laundering, identity theft, wire fraud). The investigation of the underlying crime is the responsibility of law enforcement.

However, it is helpful for those responsible for conducting investigations in a financial institution to have a basic understanding of certain crimes to assist in detecting and reporting relevant information to law enforcement.

In addition to the aforementioned topics, additional guidance on predicate crimes have been provided in the following sections:

- Drug Trafficking
- Terrorism and Terrorist Financing
- Human Trafficking and Migrant Smuggling

91. How can financial institutions monitor for new money laundering and terrorist financing methods and trends?

Financial institutions can monitor for leading practices and emerging risks by:

- Conducting self-assessments, surveys and analysis on internal activities to identify risks and best practices
- Subscribing to notifications from FinCEN, OFAC and regulatory and law enforcement authorities (e.g., rulemakings, guidance, advisories, enforcement actions)

- Monitoring key international groups for new guidance and publications, including, but not limited to, the following:
  - United Nations
  - Financial Action Task Force (FATF)
  - Egmont Group of Financial Intelligence Units (Egmont Group)
  - Wolfsberg Group of Banks (Wolfsberg Group)
  - Basel Committee on Banking Supervision (BCBS)
  - Transparency International (TI)
- Attending internal and external trainings and conferences related to AML/CFT

92. How do the AML/CFT Compliance Program requirements correspond to the FATF Recommendations?

The following table shows how AML/CFT Compliance Program requirements correspond to the FATF Recommendations and where they are discussed in this publication.

No.	FATF Recommendation	U.S. AML/CFT FAQ Guide Topics
1	Assessing risks and applying a risk-based approach	• The Fundamentals • Risk Assessments: Enterprisewide, Horizontal, Line of Business/Legal Entity, Geographic, Product/Services, Customer
2	National cooperation and coordination	• The Fundamentals: Overview of the U.S. Regulatory Framework • USA PATRIOT Act: Section 314 – Cooperative Efforts to Deter Money Laundering
3	Money laundering offense	• The Fundamentals: Overview of U.S. AML/CFT Laws
4	Confiscation and provisional measures	• Office of Foreign Assets Control and International Sanctions Programs
5	Terrorist financing offense	• The Fundamentals: Overview of U.S. AML/CFT Laws
6	Targeted financial sanctions related to terrorism and terrorist financing	• Office of Foreign Assets Control and International Sanctions Programs: Counter Terrorism Sanctions Program
7	Targeted financial sanctions related to proliferation	• Office of Foreign Assets Control and International Sanctions Programs: Non-Proliferation Sanctions Program
8	Nonprofit organisations	• Know Your Customer Types: Charitable Organisations and Nongovernmental Organisations (NGO)
9	Financial institution secrecy laws	• The Fundamentals: Overview of U.S. AML/CFT Laws • USA PATRIOT Act: Section 314 – Cooperative Efforts to Deter Money Laundering
10	Customer due diligence	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act: Section 326 – Verification of Identification

No.	FATF Recommendation	U.S. AML/CFT FAQ Guide Topics
		• Know Your Customer, Customer Due Diligence and Enhanced Due Diligence • Beneficial Owners
11	Recordkeeping	• Bank Secrecy Act: BSA Recordkeeping Requirements
12	PEPs	• USA PATRIOT Act: Section 312 – Senior Foreign Political Figure • Know Your Customer Types: Politically Exposed Persons (PEPs)
13	Correspondent banking	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks • USA PATRIOT Act Section 319 – Forfeiture of Funds in United States Interbank Accounts (Foreign Bank Certifications) • Know Your Customer Types: Correspondent Banking
14	Money or value transfer services	• Nonbank Financial Institutions: Money Services Businesses (MSBs)
15	New technologies	• Know Your Customer's Activities: Product Considerations: Electronic Banking and Digital Value • AML/CFT Technology: The Future of AML/CFT Technology
16	Wire transfers	• Funds Transfer Recordkeeping Requirement and the Travel Rule • Know Your Customer's Activities: Product Considerations: Funds Transfers
17	Reliance on third parties	• Know Your Third Parties
18	Internal controls and foreign branches and subsidiaries	• USA PATRIOT Act: Section 352 – AML Program
19	Higher-risk countries	• Risk Assessments: Geographic Risk Assessments
20	Reporting of suspicious transactions	• Bank Secrecy Act: Suspicious Activity Reports
21	Tipping-off and confidentiality	• Suspicious Activity Reports: Confidentiality and Safe Harbor
22	DNFBPs: Customer due diligence	• Nonbank Financial Institutions and Nonfinancial Institutions
23	DNFBPs: Other measures	• Nonbank Financial Institutions and Nonfinancial Institutions
24	Transparency and beneficial ownership of legal persons	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act: Section 326 – Verification of Identification • Beneficial Owners
25	Transparency and beneficial ownership of legal arrangements	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act: Section 326 – Verification of Identification • Beneficial Owners

No.	FATF Recommendation	U.S. AML/CFT FAQ Guide Topics
26	Regulation and supervision of financial institutions	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
27	Powers of supervisors	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
28	Regulation and supervision of DNFBPs	• Nonbank Financial Institutions and Nonfinancial Institutions
29	Financial Intelligence Units	• The Fundamentals: Financial Crimes Enforcement Network • International Perspectives and Initiatives
30	Responsibilities of law enforcement and investigative authorities	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
31	Powers of law enforcement and investigative authorities	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
32	Cash couriers	• Bank Secrecy Act: Report of International Transportation of Currency or Monetary Instruments (CMIR) • Know Your Customer's Activities: Product Considerations: Bulk Shipments of Currency and Bulk Cash Smuggling
33	Statistics	• Suspicious Activity Reports: SAR Statistics and Trends
34	Guidance and feedback	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies • Suspicious Activity Reports: SAR Statistics and Trends
35	Sanctions	• The Fundamentals: Enforcement Actions
36	International instruments	• The Fundamentals: Overview of U.S. AML/CFT Laws
37	Mutual legal assistance	• International Perspectives and Initiatives
38	Mutual legal assistance: freezing and confiscation	• Office of Foreign Assets Control and International Sanctions Programs • International Perspectives and Initiatives
39	Extradition	• International Perspectives and Initiatives
40	Other forms of international cooperation	• International Perspectives and Initiatives

BANK SECRECY ACT

BSA Basics

93. What is the Bank Secrecy Act (BSA)?

The key U.S. AML/CFT law is the Bank Secrecy Act (BSA) (also known as the Financial Recordkeeping of Currency and Foreign Transactions Act of 1970), which was significantly amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act).

The BSA was the first major money laundering legislation in the United States. It was designed to deter the use of secret foreign bank accounts and provide an audit trail for law enforcement by establishing regulatory reporting and recordkeeping requirements to help identify the source, volume and movement of currency and monetary instruments into or out of the United States or deposited in financial institutions.

94. What does the term "financial institution" mean for BSA purposes?

As originally defined in the BSA, "financial institution" means each agent, agency, branch or office within the United States of any person doing business, whether or not on a regular basis or as an organised business concern, in one or more of the capacities listed below:

- Bank (except bank credit card systems)
- Broker-dealer in securities
- Money services business (MSB)
- Telegraph company
- Casino or card club
- Person subject to supervision by any state or federal bank supervisory authority
- Futures commission merchant (FCM)
- Introducing broker (IB) in commodities

However, the USA PATRIOT Act significantly expanded "financial institutions" so that the definition includes, but is not necessarily limited to:

- Depository institutions (e.g., insured banks, private banks, credit unions, thrift and savings institutions, commercial banks or trust companies, agencies or branches of foreign banks in the United States)
- Broker-dealers registered or required to register with the U.S. Securities and Exchange Commission (SEC)
- Securities/commodities broker-dealers

- Futures commission merchants (FCMs), introducing brokers (IBs), commodity pool operators (CPOs) and commodity trading advisers (CTAs) registered or required to register under the Commodity Exchange Act (CEA)
- Investment bankers or investment companies
- Casinos (state-licensed or Indian) with annual gaming revenue of more than US$1 million
- Money services businesses (e.g., licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally; currency exchanges; issuer or seller of traveller's checks, money orders or similar instruments; sellers or providers of prepaid access)
- Operators of credit card systems
- Insurance companies
- Dealers in precious metals, precious stones or jewels
- Pawnbrokers
- Loan or finance companies (e.g., nonbank residential mortgage lenders or originators [RMLOs])
- Travel agencies
- Telegraph companies
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Persons involved in real estate closings and settlements
- The U.S. Postal Service
- Agencies of the federal government or any state or local government carrying out a duty or power of a business described in the definition of a "financial institution"
- Any business or agency that engages in any activity that the U.S. Secretary of the Treasury determines, by regulation, to be an activity that is similar to, related to, or a substitute for any activity in which any of the above entities are authorised to engage (e.g., housing government-sponsored enterprises [GSEs])
- Any other business, designated by the U.S. Secretary of the Treasury, with cash transactions that have a high degree of usefulness in criminal, tax or regulatory matters

The United States has not issued AML/CFT regulations for a number of the types of nonbank financial institutions (NBFIs) even though they are included in the list of financial institutions under the USA PATRIOT Act.

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM) "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator" that will expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT

requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to, the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations
- State-chartered non-depository trust companies
- International banking entities

95. How does the BSA's definition of "financial institution" compare to that outlined by the Financial Action Task Force (FATF)?

The BSA definition of "financial institution" largely parallels the FATF's definitions of "financial institution" and "designated nonfinancial business and professions (DNFBPs)" except that it does not include professional service providers such as lawyers, notaries and other independent legal professionals and accountants.

Although not required to maintain an AML Program, professional service providers are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments [CMIR], Report of Foreign Bank and Financial Accounts [FBAR]). Additionally, assuming they are U.S. persons, professional service providers are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations. For further guidance, please refer to the Professional Service Providers section.

For further guidance on international standards for AML/CFT laws, please refer to the Financial Action Task Force section.

96. Are foreign financial institutions subject to the requirements of the BSA?

The requirements of the BSA apply to the U.S. operations of foreign financial institutions (FFIs) in the same manner as they apply to domestic financial services companies. As a practical matter, however, non-U.S. offices of FFIs will find they are directly and indirectly affected by BSA requirements in their efforts to support the AML/CFT Compliance Programs of their U.S.-based affiliates. For further guidance on international standards for AML/CFT laws, please refer to the International Perspectives and Initiatives section.

97. What BSA-related reports are financial institutions required to file with FinCEN?

Depending on the type of financial institution involved, the following are reports mandated by the BSA:

- **Currency Transaction Report (CTR), FinCEN Form 112** – For further guidance, please refer to the Currency Transaction Reports section.

- **Designation of Exempt Person (DOEP), FinCEN Form 110** – For further guidance, please refer to the CTR Exemptions and the Designation of Exempt Person Form and Filing of DOEP sections.
- **Report of Cash Payments Over US$10,000 Received in Trade/Business, FinCEN Form 8300** – For further guidance, please refer to the Form 8300 section.
- **Suspicious Activity Reports (SAR), FinCEN Form 111** – For further guidance, please refer to the Suspicious Activity Reports section.
- **Report of Foreign Bank and Financial Accounts (FBAR), FinCEN Form 114** – For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section.
- **Report of International Transportation of Currency or Monetary Instruments (CMIR), FinCEN Form 105** – For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.
- **Registration of Money Services Businesses (RMSB), FinCEN Form 107** – For further guidance, please refer to the Registration of Money Services Businesses section.

Financial institutions are also required to maintain records for designated transactions in accordance with BSA recordkeeping requirements:

- **Funds Transfer Recordkeeping Requirement and the Travel Rule** – For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.
- **Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments** – For further guidance, please refer to the Recordkeeping Requirement for the Purchase and Sale of Monetary Instruments section.

98. Do all financial institutions have to comply with all the same reporting requirements of the BSA?

No. Not all provisions of the BSA apply to all financial institutions. Requirements are generally determined by the type of financial institution and the nature of the services (e.g., products, transactions) it provides.

For further guidance, please refer to each BSA Report section outlined above and the Nonbank Financial Institutions and Nonfinancial Businesses sections.

99. Are BSA Reports limited to reports on cash transactions?

No. While many of the BSA Reports are focused on cash and monetary instruments (e.g., currency in excess of US$10,000, cross-border movement), others include reporting of suspicious activities involving all types of transactions, self-disclosures of financial interests held abroad and registration of money services businesses (MSBs) with FinCEN.

Additionally, there are proposals that would expand BSA reporting requirements to include reporting on products such as prepaid access transactions and virtual currency transactions. For further

guidance, please refer to the Providers and Sellers of Prepaid Access and Virtual Currency Systems and Participants sections.

100. What is the value to law enforcement of the various reporting and recordkeeping requirements imposed by the BSA?

In general, these reports are extremely useful to law enforcement in the identification, investigation and prosecution of money laundering, terrorist financing and other criminal activity, especially those generating large amounts of cash. Data contained in BSA Reports also are used to identify and trace the disposition of proceeds from illegal activity for possible seizure and forfeiture. In addition, agencies can analyse reports on a strategic level to obtain trends and assess the threat(s) in particular areas.

101. Do financial institutions have other AML/CFT Compliance Program requirements beyond the BSA reporting requirements?

Yes. The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) (as amended) made significant changes to the BSA which, among others, imposes specific requirements for AML Programs. It requires financial institutions to establish AML Programs that include policies, procedures and controls, designation of an AML compliance officer, ongoing employee training and independent reviews. In addition, it requires certain financial institutions to have customer identification procedures for new accounts and enhanced due diligence (EDD) for correspondent and private banking accounts maintained by non-U.S. persons, including politically exposed persons (PEPs).

For further guidance, please refer to the USA PATRIOT Act section.

102. What are the consequences of failing to comply with the BSA?

In addition to other regulatory consequences, failures to comply with the BSA can result in civil monetary penalties (CMPs) and imprisonment. CMPs can be assessed per violation, and in some cases, per day. Fines can range from US$1,078 to US$1,338,420. The Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Inflation Adjustment Act) adjusted penalties for inflation in 2016 with adjustments scheduled to occur every five years. The increased fines became applicable after August 1, 2016.

BSA Reporting Requirements

CTR Basics

103. What is a Currency Transaction Report?

A Currency Transaction Report (CTR), FinCEN Form 112, is a report filed by certain types of financial institutions, identified below, for cash currency transactions of more than US$10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge that they are by or on behalf of the same person and result in cash-in or cash-out totalling more than US$10,000 in any one business day.

CTR requirements for depository institutions are implemented under regulation 31 C.F.R. 1010.310 – Reports of Transactions in Currency.

104. What does the term "currency" mean for CTR filing purposes?

"Currency" is defined as the coin and paper money (including Federal Reserve notes and circulating notes of Federal Reserve banks and national banks) of the United States or of any other country that:

- Is designated as legal tender (i.e., form of payment defined by law which must be accepted by creditors as payment for debts);
- Circulates; and
- Is customarily used and accepted as a medium of exchange in the country of issuance.

105. What types of currency transactions require CTR filings?

Any physical transfer of currency from one person to another requires the filing of a CTR. This would include, for example:

- Cash withdrawals
- Cash deposits
- Foreign currency exchange
- Check cashing paid in cash
- Cash payments
- Cash purchase of monetary instruments (e.g., bank check or draft, foreign draft, cashier's check, money order, traveller's check)
- Automated Teller Machine (ATM) cash transactions
- Incoming or outgoing wire transactions paid in cash

Wire and check transactions that do not involve the physical transfer of cash would not be considered currency transactions for CTR filing requirements.

106. Is virtual currency considered "currency" for purposes of CTR filings?

No. Financial institutions are only required to file CTRs on currency transactions in excess of US$10,000 as defined above. Per FinCEN guidance, virtual currency does not meet the definition of currency for BSA reporting purposes as it does not have legal tender status.

State laws may soon require virtual currency businesses to submit reports on virtual currency transactions greater than US$10,000, similar to CTRs. In July 2014, The New York State Department of Financial Services (DFS) was the first to propose a regulatory framework for virtual currency businesses, which was finalised in 2015.

Though they are not required to file CTRs on virtual currency transactions, a virtual currency exchanger dealing in certain types of virtual currency may fall under the definition of money

transmitter and be subject to the AML/CFT requirements of a money services business (MSB). For further guidance, please refer to the sections: Money Services Businesses and Virtual Currency Systems and Participants.

107. Are financial institutions required to file CTRs for transactions involving monetary instruments?

Financial institutions are required to file CTRs only for *cash* purchases or *cash* sales of monetary instruments that exceed US$10,000 in one business day. Financial institutions are also required to maintain records of *cash* purchases or *cash* sales between US$3,000 and US$10,000, commonly referred to as a log of negotiable instruments. For further guidance, please refer to the Recordkeeping Requirement for the Purchase and Sale of Monetary Instruments section.

108. Are financial institutions required to file CTRs for transactions involving prepaid access devices?

As with monetary instruments, financial institutions are only required to file CTRs if cash in excess of US$10,000 was used to purchase and/or redeem a prepaid access device.

For further guidance, please refer to the Prepaid Access and Stored Value section.

109. Are financial institutions required to file CTRs for bulk currency shipments?

Yes. For all receipts or disbursement of currency in excess of US$10,000, financial institutions are required to file a CTR. For additional guidance on bulk currency shipments, please refer to the Bulk Shipments of Currency and Bulk Cash Smuggling section.

110. Are financial institutions required to file CTRs for reportable transactions even when the cash may never be transferred physically to the financial institution (e.g., deposited directly into a Federal Reserve account by a third party acting as an agent for the financial institution)?

Yes. If a financial institution contracts a third party (e.g., common carrier of currency service such as an armoured car service [ACS]) to receive and transport cash physically from the financial institution's customers and deposit the cash directly into the Federal Reserve account of the financial institution, the financial institution is required to file CTRs on transactions in excess of US$10,000, even if it never physically receives the currency.

The CTR requirement applies when the contracted third party conducts the reportable transaction with the financial institution (or the Federal Reserve), not when it receives the currency from the financial institution's customers.

For further guidance, please refer to the Completion of a CTR, Filing of CTRs and Armored Car Service Exception for CTRs sections.

111. What does the term "business day" mean for CTR aggregation purposes?

A business day is the reporting period on which transactions are routinely posted to customers' accounts each day. For additional guidance on the definition of "business day," please refer to the Casinos and Card Clubs section.

112. What financial institutions are obligated to file CTRs?

The following financial institutions are subject to CTR filing requirements:

- Depository institutions (e.g., commercial banks, private banks, savings and loan associations, thrift institutions, credit unions)
- Broker-dealers in securities
- Mutual funds
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Money services businesses (MSBs)
- Casinos and card clubs

113. Are nonfinancial institutions required to file CTRs?

Businesses not subject to CTR requirements must file Form 8300 on designated reportable transactions that involve currency in excess of US$10,000. For additional guidance on Form 8300, please refer to the Form 8300 section.

114. How do CTR requirements correspond to FATF Recommendations?

In an interpretive note to FATF Recommendation 29 – Financial Intelligence Units, FATF advises countries to develop a centralised system for financial institutions and designated nonbank financial businesses and professions (DNFBP) to report domestic and international currency transactions above a fixed amount. The CTR requirement is consistent with this recommendation.

For further guidance on international standards, please refer to the Financial Action Task Force section.

115. How do financial institutions submit CTRs to FinCEN?

Beginning July 1, 2012, financial institutions have had to submit CTRs through the BSA E-Filing System, an internet-based e-filing system developed by FinCEN to enable financial institutions to file FinCEN reports electronically.

For further guidance on completing and filing CTRs, please refer to the Completion of a CTR and Filing of CTRs sections.

116. What is the time frame for filing CTRs?

All CTRs must be filed within 15 calendar days of the date of the reportable transaction.

117. How long should a financial institution retain CTRs?

CTRs must be retained for a minimum of five years from the date of filing. For further guidance on recordkeeping requirements, please refer to the BSA Recordkeeping Requirements section.

118. Since financial institutions submit CTRs to FinCEN through the BSA E-Filing System, are they still required to retain copies in accordance with AML/CFT laws and regulations?

Yes. The BSA E-Filing System is not a recordkeeping program. Financial institutions are required to retain CTRs for a minimum of five years from the date of filing in accordance with AML/CFT laws and regulations. For further guidance on recordkeeping requirements, please refer to the BSA Recordkeeping Requirements section.

119. Can a financial institution inform a customer of the requirement to file CTRs?

Yes. A financial institution can inform a customer of the CTR filing requirement. However, financial institutions and/or their employees cannot assist customers in evading the reporting requirement by "structuring" their transactions. For additional guidance on evasion, please refer to the CTR Evasion section.

If, after being informed of the CTR filing requirement, the customer breaks his or her transaction into smaller amounts in an attempt to evade reporting requirements, the financial institution, in most cases, should consider filing a suspicious activity report (SAR) on the basis of structuring. For further guidance on SARs, please refer to the Suspicious Activity Reports section.

120. Are financial institutions obligated to inform the customer that the financial institution will file a CTR on the customer's activity since it is over the reporting threshold?

No. Financial institutions are not obligated to notify customers when filing CTRs.

121. What should a financial institution do if it discovers it has failed to file CTRs on reportable transactions?

If a financial institution finds it has failed to file CTRs on reportable transactions, it should move forward to file the CTRs as soon as the failure is discovered. If there are a significant number of CTRs at issue, or if they cover transactions that are not relatively recent in time, the financial institution should contact the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center) to request a determination on whether the back-filing of unreported transactions is necessary. Prior to doing this, the institution may wish to seek advice from counsel to ensure that communication with the authorities is handled properly.

122. What are some of the common challenges to completing and filing CTRs?

The following include some of the challenges that companies have experienced when completing and filing CTRs:

- Use of non-specific occupations (i.e., unclear source of income) when recording the occupation, profession or nature of business (e.g., student, retired, unemployed, businessman, homemaker)
- Lack of aggregation across accounts and customer relationships (e.g., joint account holders, affiliated businesses, beneficial owners)
- Inadequate training of employees to determine if reportable transactions are being conducted "by or on behalf of" the conductor
- Incorrect treatment of armoured car service (ACS) transactions (e.g., determining if an ACS is acting on behalf of the reporting financial institution or the financial institution's customer or other third party)

123. What guidance has been issued related to CTRs?

The following, though not intended to be all-inclusive, lists key guidance that has been issued on the completion and filing of CTRs and exemptions:

- Completion and filing of CTRs
  - Frequently Asked Questions Regarding the FinCEN Currency Transaction Report (CTR) (2013) by FinCEN
  - FinCEN Educational Pamphlet on the Currency Transaction Reporting Requirement (2009) by FinCEN
  - BSA E-Filing System Frequently Asked Questions (2010) by FinCEN
  - BSA Electronic Filing Requirements for the Currency Transaction Report (CTR) (FinCEN Form 104) and Designation of Exempt Person (DOEP) (FinCEN Form 110) (2012) by FinCEN
  - Notice to Customers: A CTR Reference Guide (2009) by FinCEN
  - FinCEN Currency Transaction Report (FinCEN CTR) Electronic Filing Requirements (2012) by FinCEN
  - Filing FinCEN's New Currency Transaction Report and Suspicious Activity Report (2012) by FinCEN
  - Reporting of Certain Currency Transactions for Sole Proprietorships and Legal Entities Operating Under a "Doing Business As" (DBA) Name (2008) by FinCEN
  - Currency Transaction Report Aggregation for Businesses with Common Ownership (2012) by FinCEN
  - FinCEN to Receive Currency Reports from Clerks of Court (2012) by FinCEN
- Exemptions
  - Guidance on Determining Eligibility for Exemption from Currency Transaction Reporting Requirements (2012) by FinCEN

- Amendment to the Bank Secrecy Act Regulations – Exemption from the Requirement to Report Transactions in Currency (2012) by FinCEN
- Definition of Motor Vehicles of Any Kind, Motor Vehicles, Vessels, Aircraft, and Farm Equipment as it Relates to Potential CTR Exemption (2012) by FinCEN
- Bank Secrecy Act Designation of Exempt Person (FinCEN Form 110) Electronic Filing Requirements (2012) by FinCEN
- Designation of Exempt Person (DOEP) and Currency Transaction Reporting (CTR): Assessing the Impact of Amendments to the CTR Exemption Rules Implemented on January 5, 2009 (2010) by FinCEN
- Report to Congressional Committee: Bank Secrecy Act: Increased Use of Exemption Provisions Could Reduce Currency Transaction Reporting While Maintaining Usefulness to Law Enforcement Efforts (2008) by the United States Government Accountability Office (GAO)
- Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that Is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements (2009) by FinCEN
- Definition of Motor Vehicles of Any Kind, Motor Vehicles, Vessels, Aircraft, and Farm Equipment as it Relates to Potential CTR Exemption for a Non-Listed Business (2012) by FinCEN
- CTR Exemption Regulation Amended to Include MMDAs (2000) by FinCEN

- Casinos
  - Frequently Asked Questions: Casino Recordkeeping, Reporting, and Compliance Program Requirements (2007, 2009, 2012) by FinCEN
  - Casino Industry Currency Transaction Reporting: An Assessment of Currency Transaction Reports Filed by Casinos between July 1, 2006, and June 30, 2008, by FinCEN
  - FinCEN's Guidance on Determining Whether Tribally Owned and Operated Casinos Are Eligible for Exemption from CTR Requirements (2002) by FinCEN

CTR Threshold and Aggregation

124. At what threshold must a CTR be filed for currency transactions?

CTRs must be filed for currency transactions in excess of US$10,000. For example, a currency transaction of exactly US$10,000 does not require the filing of a CTR. However, a currency transaction of US$10,000.01 would.

125. Are there any circumstances under which a financial institution would need to file a CTR for amounts of US$10,000 or less?

Yes. A Geographic Targeting Order (GTO) gives the U.S. Treasury Department, and in some instances states, the authority to require a financial institution or a group of financial institutions or companies in a geographic area to file additional reports or maintain additional records above and beyond ordinary AML/CFT requirements for (e.g., less than US$10,000 for CTRs). GTOs are used to collect information on individuals/entities suspected of conducting transactions under reportable thresholds.

126. What are examples of GTOs which have been issued?

FinCEN issued a GTO that requires enhanced cash reporting by common carriers of currency (e.g., armoured car services) in the land border between southern California, United States, and the Mexican border states. The GTO outlined special reporting, recordkeeping, and customer identification obligations of common carriers of currency.

FinCEN issued a GTO requiring even more business types (e.g., garment and textile stores, transportation companies, travel agencies, perfume stores, electronics stores, shoe stores, lingerie stores, flower/silk flower stores, beauty supply stores, stores with "import" or "export" in their names) to report cash transactions greater than or equal to US$3,000.

More recently, FinCEN renewed GTOs in specified cities and counties of California, Florida, New York and Texas requiring title insurance companies to collect and report purchases of residential real property over a specified amount (e.g., US$500,000 to US$3 million), made without external financing (e.g., bank loan) that partially used currency or monetary instruments (e.g., cashier's check, traveller's check, money order). GTOs increase reportable information submitted to law enforcement, which can enhance investigations of businesses in high-risk areas.

127. How does the US$10,000 threshold apply to foreign currency transactions?

For transactions conducted in foreign currency, the CTR requirements are applicable at the amount equivalent to more than US$10,000 in U.S. dollars.

128. If the country of origin is unknown for transactions conducted in Euros, how should financial institutions complete the critical "country of origin" field in the BSA E-Filing System?

According to FinCEN, financial institutions should enter "BE" (for Belgium) for unknown countries of origin in the BSA E-Filing System until directed otherwise.

129. Has there been any consideration given to increasing the minimum threshold for CTR filing?

Periodically, there have been discussions about the benefits to the industry and law enforcement of increasing the reporting threshold. In March 2007, a bill was introduced in the U.S. House of Representatives that would, among other things, increase the CTR filing threshold to US$30,000 and allow for more CTR exemptions. Such legislation could significantly reduce the burden of reporting

requirements for financial institutions. In 2008, the bill expired prior to being passed by Congress. However, later that year, FinCEN amended CTR exemption rules in an effort to simplify the process for depository institutions. For further guidance, please refer to the CTR Exemptions and the Designation of Exempt Persons Form section.

130. What does it mean to aggregate transactions for CTR filing purposes?

Multiple cash transactions conducted on a single business day by one customer must be aggregated if the financial institution has knowledge that they are by, or on behalf of, one person, and result in either cash-in or cash-out totalling more than US$10,000 during any one business day. For example, if a customer deposits US$6,000 in cash into his or her account at 9:30 a.m. and returns at 2:30 p.m. to make a cash loan payment of US$5,000, the two transactions must be aggregated. The cash transactions of this customer total US$11,000, and a CTR must be filed.

131. Are financial institutions required to aggregate transactions conducted by related entities for CTR filing purposes?

In some instances, currency transactions should be aggregated across different entities (e.g., businesses with different taxpayer identification numbers) for CTR reporting purposes. For example, if businesses are not "operated separately and independently" and the financial institution is aware of this fact, then multiple currency transactions conducted in the accounts of the related businesses must be aggregated and reported on a CTR. Factors to determine if multiple businesses are operated "separately and independently" include, but are not limited to, the following:

- Businesses are staffed by the same employees
- Bank accounts of one business are used to pay the expenses of another business
- Bank accounts are used to pay the personal expenses of the owner

132. Are financial institutions required to aggregate transactions conducted by beneficial owners for CTR filing purposes?

Yes. If reportable currency transactions are conducted by or on behalf of beneficial owners, CTRs are required to be filed.

133. In practice, how should financial institutions with multiple tellers and/or multiple locations identify multiple cash transactions by the same customer in a single business day?

Financial institutions with multiple tellers/locations may not always be able to identify, on a real-time basis, multiple transactions by the same customer in a single business day. For purposes of CTR filings, a "financial institution" includes all of its branches and agents. For example, a customer may make a cash deposit of US$6,000 in the morning and return in the afternoon to a different teller with an additional US$5,000 cash deposit. A financial institution may not be able to identify the need to file a CTR for the customer immediately. If there are multiple transactions that trigger a CTR, but the financial institution only learns a CTR is required after the customer has left, and the financial

institution does not have all the information required on a CTR form, then certain items on the CTR form may be left blank and the "multiple transactions" box on the CTR form should be checked.

However, financial institutions should have procedures to monitor transactions at the close of business or on the following day to identify multiple cash transactions conducted by the same customer. Numerous software products are available to assist organisations with this effort. For additional guidance, please refer to the Large Currency Transaction Monitoring and Filing of Currency Transaction Reports (CTRs) section.

134. Should deposits and withdrawals be netted for CTR purposes?

No. CTRs are reported on a gross cash-in and/or cash-out basis. Deposits and withdrawals should not be netted. For example, if a customer deposits US$7,500 in cash and on the same day withdraws US$3,000 in cash from an ATM, even though the total value of cash transactions exceeds US$10,000, neither the gross value of the withdrawal nor the deposit exceeds US$10,000. However, in this case, a financial institution might question why the customer would want to deposit cash and withdraw cash separately on the same day. There could be a legitimate business reason for these two cash transactions, but the two transactions raise the question of whether this is suspicious activity that warrants further investigation by the financial institution and, possibly, a SAR filing.

Completion of a CTR

135. How can financial institutions determine who should be included in Part I: Person Information of the CTR?

It is the responsibility of the financial institution to ascertain the real person of interest when filing CTRs. When possible, employees should ask if the conductor of the reportable transaction is being completed by or on behalf of him/herself or for a third party and collect the required information as required by AML/CFT laws and regulations.

136. What identification is required for the filing of a CTR?

Prior to completing any transaction that would require a financial institution to file a CTR, financial institutions are required to do the following:

- Review an acceptable form of identification (in most cases) and verify and record the name and address of the individual presenting the transaction
- Record the full name and address, type and account number of the identification obtained, and the taxpayer identification number (TIN) (e.g., Social Security Number [SSN] or employer identification number [EIN]) of any person or entity on whose behalf such transaction is to be effected

137. What identification should a financial institution require when conducting cash transactions for a business entity?

Documentary verification may include proof of identity or incorporation. Examples include, but are not limited to, business license, certificate of good standing with the state, or documents showing the existence of the entity, such as articles of incorporation.

138. What identification requirements should a financial institution implement when conducting cash transactions for noncustomers?

If cash transactions are processed for individuals who are not customers of the financial institution, procedures should exist to review an acceptable form of identification and record the name and address of individuals who conduct cash transactions at a certain threshold below the CTR requirement, so that a CTR (and, if warranted, a SAR) can be completed if multiple cash transactions are detected through monitoring.

139. What identification method is acceptable for a non-U.S. person for CTR filing purposes?

For an individual who is an alien or non-resident of the United States, a passport, cedular card, alien identification card or other official document evidencing nationality or residence can be used to verify the identity of that person. Leading practice dictates that the form of identification be current (i.e., unexpired) and bear a photograph and address.

140. If the person conducting the reportable transaction is a customer of the financial institution, does the information need to be obtained prior to the completion of the transaction?

If the financial institution previously obtained acceptable identification information and maintained it in its records, then such information may be used. For example, if documents verifying the individual's identity were reviewed and recorded on a signature card at account opening, then this may suffice. However, the financial institution still must record the method, type and number of identification on the CTR, and a statement such as "signature card on file" or "known customer" is not sufficient. Leading practice suggests that the employee handling the transaction verify, at a minimum, that all necessary information is available and accurate while the customer is present.

141. When should a financial institution select "Courier service (private)" as the conductor?

The "Courier service (private)" category should be selected if the conductor is a courier service (e.g., armoured car service [ACS]) contracted by the person on whose behalf the transaction takes place and *not* by the financial institution itself.

For further guidance on the treatment of armoured car service transactions, please refer to the Armored Car Service Exception for CTRs section.

142. For the type of transaction, when should financial institutions select "Armored Car (FI Contract)"?

An armoured car service (ACS) provides the secured transport services of goods, including currency and other valuables for various third parties including, but not limited to, financial institutions and private companies.

Financial institutions should select "Armored Car (FI Contract) if a reportable transaction involved an ACS contracted by the financial institution itself. "Armored Car (FI Contract)" should not be selected if the armoured car service was under contract to the financial institution's customer or third party.

For further guidance, please refer to the Armored Car Service Exception for CTRs section.

143. Should the amount reported in the CTR be rounded?

Yes. The dollar amount reported in the CTR should be rounded up to the nearest whole dollar.

144. What is the difference between "multiple transactions" and "aggregate transactions"?

The following factors determine whether a financial institution should select "aggregate transactions" or "multiple transactions" when completing a CTR:

- Amount of each transaction(s) (e.g., below reportable threshold);
- Involvement (or lack thereof) of teller(s); and
- Identification (or lack thereof) of transactor(s).

"Multiple transactions" must be treated as a single transaction (aggregated) for CTR filing purposes if the financial institution has knowledge that they are by or on behalf of the same person and result in cash-in or cash-out totalling more than US$10,000 in any one business day. "Multiple transactions" can involve individual transactions that are above the reporting requirement.

"Aggregate transactions" are transactions commonly detected by a financial institution's large currency monitoring software that identifies reportable transactions after the date of the transaction(s). Since the reportable transactions were not identified at the time of the transaction, there is no opportunity to collect the required information for a CTR (e.g., person conducting the transaction). "Aggregate transactions" do not involve individual transactions above the reportable threshold, but must involve at least one teller transaction.

Whether the reportable transactions are categorised as "multiple transactions" or "aggregate transactions," a CTR filing is required.

For further guidance, please refer to FinCEN's "Frequently Asked Questions Regarding the FinCEN Currency Transaction Report (CTR)."

145. What should a financial institution do if it is unable to complete all fields marked as critical on the CTR within the BSA E-Filing System?

Financial institutions are expected to provide information for which they have direct knowledge consistent with existing regulatory expectations, for critical and noncritical fields.

If a financial institution is unable to populate a critical field, it should select "unknown" (i.e., "unk") to indicate that the information was not known at the time of the filing as opposed to inadvertently omitted by the financial institution.

146. Can a financial institution report potentially suspicious activities on the CTR?

No, unlike the Form 8300, financial institutions cannot report potentially suspicious activities on the CTR. If a financial institution believes a customer is deliberately evading a reporting requirement for any reason (e.g., structuring), it should file a Suspicious Activity Report (SAR). For further guidance on red flags for potentially suspicious activity, please refer to the CTR Evasion and Currency Red Flags sections. For further guidance on reporting suspicious activities, please refer to the Suspicious Activity Reports section.

147. What recent updates were made to the CTR?

In May 2017, FinCEN announced new and updated CTR fields to adhere to evolving AML/CFT reporting requirements (e.g., filing under alternative reporting models such as a parent company filing on behalf of a subsidiary) and other technical updates to improve the layout of the CTR. Changes included adding a checkbox to reflect "Shared Branching" and cash in and cash out amounts for transaction locations. These updates do not change existing regulatory requirements for CTRs.

Armored Car Service Exception for CTRs

148. Is there an exception to the CTR data collection and aggregation requirement for armoured car service transactions?

Yes. In 2013, FinCEN published guidance on the treatment of armoured car service (ACS) transactions for CTR filing purposes. If the ACS is acting on behalf of the financial institution, the reporting financial institution is no longer required to collect information on the ACS for CTR filing purposes.

Prior to this guidance, financial institutions were required to collect information (e.g., name, date of birth, identification information) on all customers and person(s) conducting transactions on behalf of the customer, including the ACS employee who conducted the reportable transaction (i.e., the employee that made the delivery or pickup that resulted in a deposit to or withdrawal from the reporting financial institution's account).

For further examples, please refer to FinCEN's guidance:

- Treatment of Armored Car Service Transactions Conducted on Behalf of Financial Institution Customers or Third Parties for Currency Transaction Reports Purposes;
- Appendix I: Examples of the Completion of the FinCEN Currency Transaction Report (CTR) for Transactions Involving Armored Car Services

149. What should a financial institution do if it is unable to determine on whose behalf the ACS is conducting transactions?

If unable to determine on whose behalf the ACS is conducting transactions, financial institutions should include all customer(s) and persons conducting transactions on behalf of the customer(s), including the ACS on the CTR.

150. When collecting data on the ACS for CTR filing purposes, should the financial institution collect information on the employee or the corporation?

When required, financial institutions should collect information on the ACS (e.g., corporate name, address, employer identification number [EIN]), and not the employee of the ACS who made the delivery or pickup that resulted in a deposit to or withdrawal from the reporting financial institution's account.

151. Does the CTR exception for the treatment of ACS transactions impact a financial institution's other regulatory requirements (e.g., suspicious activity reporting)?

No. The CTR exception for the treatment of ACS transactions does not affect financial institutions' obligations to report suspicious transactions to FinCEN. For further guidance, please refer to the Suspicious Activity Reports section.

For further guidance on the AML/CFT requirements for ACSs, please refer to the Common Carriers of Currency and Armored Car Services section.

Filing of CTRs

152. How do financial institutions submit CTRs to FinCEN?

Beginning July 1, 2012, financial institutions have had to submit CTRs through the BSA E-Filing System, an e-filing system developed by FinCEN to enable financial institutions to file FinCEN Reports electronically, through discrete or batch filings.

FinCEN has provided multiple resources to assist financial institutions in utilising the BSA E-Filing System, including, but not limited to, the following:

- FinCEN Currency Transaction Report (FinCEN CTR) Electronic Filing Requirements (2013)
- FinCEN Webinar on the FinCEN CTR and DOEP
- FinCEN Webinar on the Updated BSA E-Filing Technical Specifications for FinCEN's New SAR, CTR and DOEP
- FinCEN Webinar on the Introduction to the BSA E-Filing System
- BSA E-Filing System: Batch File Testing Procedures (2012)
- FinCEN Regulatory Hotline: 800.949.2732
- FinCEN Help Desk: 866.346.9478 or BSAEFilingHelp@fincen.gov

Additionally, field-specific instructions are provided within the discrete filing version of the CTR when the filer scrolls over each field within the BSA E-Filing System.

153. Are financial institutions limited to completing the CTR within the BSA E-Filing System?

No. Financial institutions can download the CTR template from the BSA E-Filing System, complete the CTR form off-line and submit the completed CTR form in a discrete or batched filing within the BSA E-Filing System.

154. Will FinCEN accept CTRs submitted in paper format?

No. After March 31, 2013, FinCEN no longer accepted legacy paper reports. All CTRs must be filed utilising FinCEN's BSA E-Filing System.

155. What is "shared branching" and who is required to file CTRs under these conditions?

"Shared branching" occurs when a holding company or parent company files CTRs on behalf of subsidiary institutions. The transaction(s) takes place at a subsidiary institution, whereas the filing is completed by the holding/parent company, either of which can file CTRs on reportable transactions.

156. How can financial institutions file corrected or amended CTRs through the BSA E-Filing System?

Financial institutions can file amended or corrected CTRs by entering the Document Control Number (DCN)/BSA Identifier (ID) of the previous CTR and selecting "Correct/Amend Prior Report" in the BSA E-Filing System. The DCN/BSA ID can be retrieved from the acknowledgement received by the filer after successful submission and acceptance of the previous CTR filing.

157. Within what time frame must financial institutions correct primary file errors and file corrected/amended CTRs?

FinCEN recommends that corrections be made no later than 30 calendar days after receiving the error notification from FinCEN.

158. What should financial institutions do if they are unable to implement corrections within 30 calendar days?

Financial institutions should notify FinCEN by providing in writing:

- An explanation of the technical issues that prevented them from implementing corrections within the recommended time frame,
- An estimate of when the issues will be resolved; and
- Contact information (name and telephone number).

Correspondence should be addressed to:

Financial Crimes Enforcement Network
Office of Compliance
P.O. Box 39
Vienna, VA 22183

159. Does the rejection of a batch file obviate the financial institution's responsibility to file a CTR within 15 calendar days following the day on which the reportable transaction occurred?

No. Financial institutions must file initial CTRs within 15 calendar days following the day on which the reportable transaction occurred, regardless of when or how the batch file was processed.

Financial institutions should file corrected/amended CTRs no later than 30 calendar days after receiving the error notification from FinCEN.

160. What are "alerts" within the BSA E-Filing System?

FinCEN uses "alerts" within the BSA E-Filing System to send direct messages (which may include attachments) to system users with alert privileges (e.g., designated employees at financial institutions authorised to file BSA reports and receive system alerts).

161. Since financial institutions submit CTRs to FinCEN through the BSA E-Filing System, are they still required to retain copies in accordance with AML/CFT laws and regulations?

Yes. The BSA E-Filing System is not a recordkeeping program. Financial institutions are required to retain CTRs for a minimum of five years from the date of filing in accordance with AML/CFT laws and regulations.

162. What records are maintained within the BSA E-Filing System?

The BSA E-Filing System maintains the following records:

- **Acknowledgements** – Confirmations of submitted FinCEN reports are maintained for 30 calendar days after being opened or 60 calendar days after being posted, whichever comes first;
- **Alerts** – Retained for 30 calendar days after posting; and
- **Track Status Data** – Retained for five years (1825 calendar days) after achieving "Accepted" or "Rejected" status.

Financial institutions should periodically archive this administrative data to comply with recordkeeping requirements in accordance with AML/CFT laws and regulations.

163. How can financial institutions utilise AML/CFT technology in filing CTRs?

Available CTR filing solutions range from stand-alone systems that function only in the back office to fully integrated solutions that provide real-time aggregation to the front office. Additionally, some

systems include functionality to monitor for suspicious currency activity and manage the financial institution's CTR exemption process.

For further guidance, please refer to the AML/CFT Technology and Large Currency Transaction Monitoring and Filing of Currency Transaction Report (CTRs) sections.

CTR Exemptions and the Designation of Exempt Persons Form

164. What are CTR exemptions?

CTR exemptions are designations filed by eligible financial institutions that alleviate the requirement for filing CTRs when "exempted" customers conduct (deposit or withdraw) transactions in currency that exceed US$10,000 in one business day. Financial institutions can designate exempt customers by filing the Designation of Exempt Persons (DOEP), FinCEN Report 110, with FinCEN.

165. What protection does the DOEP provide financial institutions as it relates to the CTR filing requirements?

Financial institutions that have complied properly with the exemption requirements are not liable for any failure to file a CTR for the exempt customer during the period of the exemption.

166. What is the value of CTR exemptions to depository institutions and law enforcement?

CTR exemptions reduce the compliance burden and liability on depository institutions. Additionally, they reduce the filing of CTRs that have little or no value for law enforcement investigations.

167. What types of financial institutions are eligible to grant CTR exemptions?

Only depository institutions (e.g., private banks, commercial banks, savings and loan associations, thrift institutions, credit unions) can grant exemptions.

168. Can branches and agencies of foreign banking organisations (FBOs) operating in the United States grant CTR exemptions?

Yes. A branch or agency of an FBO operating in the United States may grant CTR exemptions so long as exempted customers meet eligibility criteria. Given the criteria for exemption and the nature of the customer base of many FBOs, the opportunity for FBOs to grant exemptions may be limited.

169. What types of customers can be granted CTR exemptions?

The following types of customers of depository institutions can be exempted from CTR filing requirements under what are referred to as "Phase I" or "Tier I" exemptions:

- Banks, to the extent of the bank's U.S. subsidiaries (including U.S. branches and agencies of international banks)
- Entities, to the extent of an entity's U.S. operations that have shares or other equity interests listed on the NYSE, Amex or NASDAQ (except stock listed under "NASDAQ Small-Cap Issuers")

- Certain subsidiaries of listed entities (see bullet point above) that are organised under U.S. law and for which at least 51 percent of the common stock is owned by the listed entity that qualifies for exemption
- Departments and agencies of federal, state or local governments
- Any entity exercising governmental authority within the United States

"Phase II" or "Tier II" exemptions permit certain nonlisted businesses as well as payroll customers to be exempted, as explained further below.

170. How can a depository institution apply for CTR exemptions?

If a depository institution wishes to designate an "exempt person," the FinCEN Designation of Exempt Person (DOEP) Form 110 must be completed and filed within 30 calendar days after the first reportable transaction to be exempted. For customers that are themselves depository institutions operating in the United States and for customers that are federal or state governmental entities, no DOEP form or annual review of the customer is required. However, the depository institution is required to file a DOEP form for, and conduct an annual review of, all other Phase I-exempt customers.

171. If a depository institution exempts a publicly traded company, are all the franchises of that company automatically exempt?

A depository institution must determine whether the franchisee itself is a publicly traded corporation, rather than the franchisor. In many cases, the depository institution will find that the franchise is not exempt. Only to the extent of domestic operations, subsidiaries meeting the following criteria may qualify for exemption:

- Organised under the laws of the United States.
- At least 51 percent of the common stock is owned by the listed entity that qualifies for exemption. Bank subsidiaries may not be exempted on this basis.

172. What types of nonlisted businesses are eligible for exemption?

A nonlisted business is any other commercial enterprise, to the extent of its domestic operations and only with respect to transactions conducted through its exemptible accounts, that:

- Has maintained a transaction account at the bank for at least two months
- Frequently engages in currency transactions at the bank for amounts in excess of US$10,000
- Is incorporated or organised under the laws of the United States or a state, or is registered as and eligible to do business within the United States or a state and where 50 percent of its gross revenues (as opposed to sales) per year are not derived from one or more of the following ineligible activities:
    - Serving as financial institutions or agents of financial institutions of any type

- The purchase or sale to customers of motor vehicles of any kind, or vessels, aircraft, farm equipment or mobile homes
- The practice of law, accountancy or medicine
- The auctioning of goods
- The chartering or operation of ships, buses or aircraft
- Pawn brokerage
- Gaming of any kind (other than licensed pari-mutuel betting at race tracks)
- Investment advisory services or investment banking services
- Marijuana-related businesses [MRBs]
- Real estate brokerage
- Title insurance and real estate closings
- Trade union activities
- Any other activities that may be specified by FinCEN

173. Can marijuana-related businesses be eligible for CTR exemption?

No. FinCEN has issued guidance indicating that MRBs may not be treated as a nonlisted business, and therefore are not eligible for CTR exemption. For further guidance, please refer to the Marijuana-Related Businesses section.

174. What guidance has been issued on the definition of "motor vehicles and other vessels" as it relates to CTR exemption eligibility?

In 2012, FinCEN issued a ruling on the CTR exemption eligibility of businesses that sell or purchase "motor vehicles, vessels, aircraft and farm equipment." Relying upon other federal statutes and results, these terms have been defined as follows:

- Motor vehicle includes "self-propelled vehicle or machine" (e.g., automobiles, trucks, low-speed vehicles, motorised wheelchairs, snowmobiles, scooters, mopeds)
- Vessel includes "every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water" (e.g., jet skis, non-motorised boats, paddle boats, canoes, submarines, rafts)
- Aircraft includes a "device that is used or intended to be used for flight in the air" (e.g., airplanes, hang gliders, experimental planes, gliders, hot-air balloons, blimps)
- Farm equipment includes "equipment used in the production of livestock or crops, including, but not limited to, mowers, harvesters, loaders, slaughter machinery, agricultural tractors, farm engines, farm trailers, farm carts, and farm wagons, excluding automobiles and trucks"

Businesses that derive more than 51 percent of their gross revenues from the purchase or sale of the aforementioned vehicles and equipment are not eligible for CTR exemption.

175. How can a depository institution determine if a nonlisted business derives greater than 50 percent of gross revenue from an ineligible activity?

According to FinCEN's "Guidance on Supporting Information Suitable for Determining the Portion of a Business Customer's Annual Gross Revenues that Is Derived from Activities Ineligible for Exemption from Currency Transaction Reporting Requirements" issued in April 2009, a depository institution is not required to establish an exact percentage of gross revenue derived from ineligible activity. Instead, it is expected to conduct due diligence in order to make a reasonable determination that a nonlisted business derives no greater than 50 percent of gross revenue from an ineligible activity. At minimum, the due diligence conducted should include examining the nature of the customer's business, the purpose of the account, and the actual or expected account activity.

176. What does the term "transaction account" mean for CTR exemption purposes?

As defined in 19(b)(1)(C) of the Federal Reserve Act, 12 U.S.C. 461(b)(1)(C) and its implementing regulation, 12 C.F.R. Part 204, the term "transaction account" means a deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers, or other similar items for the purpose of making payments or transfers to third persons or others. The term "transaction account" includes demand deposit accounts (DDAs), negotiable order of withdrawal (NOW) accounts, savings deposits subject to automatic transfers, and share draft accounts.

177. What does the term "payroll customer" mean for CTR exemption purposes?

A payroll customer is one that:

- Has maintained a transaction account at the bank for at least two months
- Operates a firm that frequently (i.e., five or more times per year) withdraws more than US$10,000 in order to pay its U.S. employees in currency
- Is incorporated or organised under the laws of the United States or a state, or is registered as and is eligible to do business within the United States or a state

178. Are all transactions conducted by an exempted person excluded from the reporting requirement?

Exemptions may not apply to all accounts maintained or transactions conducted by an exempt customer. For example, accounts and/or transactions that are maintained or conducted other than in connection with the exempted commercial enterprise are not exemptible accounts or transactions and would require the filing of a CTR.

179. Can individuals be exempted from CTR filing requirements?

No. CTR exemptions cannot be granted to individuals.

180. What does the term "frequent" mean for CTR exemption purposes?

According to FinCEN's "Guidance on Determining Eligibility for Exemption from Currency Transaction Reporting Requirements," issued in June 2012, a customer should be conducting at least five large currency transactions throughout the year to be considered for CTR exemption.

181. Can a depository institution grant an exemption to a new customer?

Depository institutions can immediately grant a new customer an exemption if it qualifies as a Phase I exemption. Phase II exemptions may be granted two months after establishing a transaction account, or before two months if the institution makes a risk-based decision that the customer has a legitimate business purpose for making frequent deposits based on the customer's nature of business, customers served, location, and past relationship with the customer.

182. If customers meet the exemption criteria, are depository institutions required to grant them CTR exemption status?

Exemptions are not mandatory, and a depository institution can choose to file CTRs on the customers.

183. Should depository institutions file separate exemptions for each account or one for all accounts an eligible customer has?

A single DOEP should be filed for each customer at a financial institution who/that is eligible for exemption, regardless of the number of accounts held by the customer.

184. How often does a depository institution need to recertify its exempt customers?

Depository institutions that exempt customers need only make a one-time filing of the DOEP form.

185. How often should CTR-exempt customers be reviewed?

Depository institutions should review, on at least an annual basis, all their Phase II-exempt persons and entities listed on the major national stock exchanges, or subsidiaries (at least 51 percent-owned) of entities listed on the major national stock exchanges, to ensure the determination to exempt the customer continues to be valid and justified.

186. Does a financial institution need to report the revocation of exempt status to FinCEN?

No. Depository institutions are not required to file a report with FinCEN; however, they should document the reason the customer no longer meets the exemption criteria. In addition, once it is determined a customer is no longer exempt, the depository institution should begin to file CTRs for reportable transactions.

187. Is a depository institution required to back file CTRs on reportable transactions after the revocation of exempt status?

No. Depository institutions are not required to back file CTRs with respect to designated Phase II customers that were previously eligible for exemption in a preceding year.

188. If an exempt customer conducts a transaction as an agent for another customer, does the exemption apply?

No. Exemption status cannot be transferred to another customer. It is critical that employees be trained to ask customers if they are acting on their own behalf or as an agent for another person when processing a reportable transaction.

189. Can an exemption be transferred from one financial institution to another?

No. CTR exemptions do not travel with the customer from institution to institution. The new institution must follow either the Phase I or Phase II exemption requirements when granting exemptions.

190. Can an exemption be revoked?

Yes. An exemption can be revoked at any time by the depository institution that applied for it or at the request of FinCEN.

191. What are some of the reasons an exemption would be revoked?

Customers lose their automatic exemption status if they cease to be listed on an applicable stock exchange, if a subsidiary of a listed company ceases to be owned at least 51 percent by the listed company, or if they no longer meet the requirement of an exempt person and the depository institution knows of such a change.

192. Are depository institutions that do not file CTRs on exempt customers afforded any protection under the law?

A depository institution that has complied with the exemption requirements in general is not liable for any failure to file a CTR for the exempt customer for the period of the exemption. This safe harbour, however, is provided to financial institutions that did not knowingly provide false or incomplete information or have reason to believe the customer did not qualify as an exempt customer.

193. Should a depository institution maximise its ability to exempt qualified customers from the CTR filing requirement?

FinCEN encourages depository institutions to use exemption provisions to reduce the filing of CTRs that have little or no value for law enforcement investigations.

194. What are some of the reasons a depository institution does not participate in the CTR exemption process?

The most common reasons a depository institution chooses not to exempt qualified customers are:

- Additional costs associated with the exemption process (e.g., resources, system modifications)
- Fear of regulatory criticism surrounding the depository institution's exemption process
- Difficulty in determining whether a customer is eligible for exemption

Filing of DOEPs

195. When must a depository institution start submitting DOEPs in the BSA E-Filing System?

After March 31, 2013, depository institutions must submit DOEPs in the BSA E-Filing System as FinCEN will no longer accept legacy reports.

196. Will FinCEN accept DOEPs submitted in paper format?

No. After March 31, 2013, FinCEN will no longer accept legacy reports. All DOEPs must be filed utilising FinCEN's BSA E-Filing System.

197. What date should depository institutions enter for "Effective Date of the Exemption"?

The date that should be entered as the "Effective Date of the Exemption" depends on the type of DOEP filing:

- For **Initial DOEPs**, depository institutions should enter the date of the first transaction to be exempted.
- For **Amended DOEPs**, assuming that the date of the exemption is not being amended, depository institutions should enter the same date as the initial DOEP, otherwise the revised date should be entered.
- For **Revoked DOEPs**, depository institutions should enter the day after the date of the last transaction that was exempted.

198. How can depository institutions file corrected or amended DOEPs through the BSA E-Filing System?

Depository institutions can file amended DOEPs by entering the Document Control Number (DCN)/BSA Identifier (ID) of the previous DOEP and selecting "Exemption Amended" in the BSA E-Filing System. The DCN/BSA ID can be retrieved from the acknowledgement received by the filer after successful submission and acceptance of the previous CTR filing.

199. Within what time frame must depository institutions correct primary file errors and file amended DOEPs?

FinCEN recommends that corrections be made no later than 30 calendar days after receiving the error notification from FinCEN.

200. What should depository institutions do if they are unable to implement corrections within 30 calendar days?

Depository institutions should notify FinCEN by providing in writing:

- An explanation of the technical issues that prevented them from implementing corrections within the recommended time frame;

- An estimate of when the issues will be resolved; and
- Contact information (name and telephone number).

Correspondence should be addressed to:

Financial Crimes Enforcement Network
Office of Compliance
P.O. Box 39
Vienna, VA 22183

201. Does the rejection of a batch file obviate the depository institution's responsibility to file a DOEP within 30 calendar days after the first reportable transaction to be exempted?

No. Depository institutions must file initial DOEPs within 30 calendar days after the first reportable transaction to be exempted, regardless of when or how the batch file was processed.

202. How soon should a financial institution file corrected/amended DOEPs after receiving an error notification from FinCEN?

Depository institutions should file amended DOEPs no later than 30 calendar days after receiving the error notification from FinCEN.

203. Is a depository institution required to file a "Revoked Exemption" to notify FinCEN of the change in exemption status?

No. Depository institutions are not required to file a "Revoked Exemption" with FinCEN; however, they should document the reason the customer no longer meets the exemption criteria. In addition, once it is determined a customer is no longer exempt, the depository institution should begin to file CTRs for reportable transactions.

204. How long should a depository institution retain DOEPs?

DOEPs must be retained for a minimum of five years from the date of filing. For further guidance on recordkeeping requirements, please refer to the BSA Recordkeeping Requirements section.

205. Since depository institutions submit DOEPs to FinCEN through the BSA E-Filing System, are they still required to retain copies in accordance with the BSA?

Yes. The BSA E-Filing System is not a recordkeeping program. Depository institutions are required to retain DOEPs for a minimum of five years from the date of filing in accordance with AML/CFT laws and regulations.

206. What recent updates were proposed for the DOEP?

In June 2017, FinCEN proposed removing "Document Control Number" since it was no longer used and adding a country field to accommodate reporting from U.S. territories. These updates do not change existing regulatory requirements for DOEPs.

CTR Evasion

207. What are some ways customers attempt to evade the filing of CTRs?

Customers can attempt to evade the filing of a CTR by structuring or "smurfing" transactions, omitting material information, providing misstatements of facts, or refusing to complete the transaction(s) altogether. All of these actions are considered criminal activities. For further guidance, please refer to the Suspicious Activity Red Flags section.

208. What does the term "structuring" mean?

Structuring is the attempt to evade CTR filing requirements by breaking transactions into smaller amounts, typically just below the reportable threshold (e.g., US$9,999). For example, a customer may deposit US$9,900 cash into his or her account on one business day and return later that day or the next day with an additional US$9,000 cash deposit. The funds may be deposited in one or multiple accounts held by the customer. Without any further information about the customer, it would appear he or she may be intentionally trying to avoid the CTR filing requirement, which is a crime.

209. What does the term "micro structuring" mean?

Micro structuring is a form of structuring that involves breaking transactions into small amounts, typically ranging from US$500 to US$1,500, and more frequent depositing of currency into a higher number of accounts than is done in classic structuring schemes. A micro structuring scheme often involves small cash deposits followed by withdrawals conducted through international ATMs.

210. What does the term "smurfing" mean?

Smurfing is the attempt to evade CTR filing requirements and/or detection by conducting numerous transactions at different locations of either the same institution or different institutions. For example, a group of individuals may go to multiple branches of a bank and send monies to the same beneficiary, acting on behalf of the same organisation or person.

211. Can employees of a financial institution advise a customer that it can avoid reporting if it conducts transactions under the reporting limit?

Employees may not suggest to their customers that they disaggregate transactions into smaller amounts in order to avoid reporting requirements; this would be deemed as structuring or assisting in structuring, both of which are prohibited by the BSA and are criminal acts.

212. If it appears a customer is structuring transactions below the reportable threshold, should financial institutions file a CTR?

If a customer's cash transactions do not meet the CTR filing requirements of aggregated deposits or withdrawals in excess of US$10,000 in one business day, a CTR is not warranted. However, if a financial institution suspects a customer is structuring transactions, the financial institution should file a SAR, as structuring is a criminal offense.

213. Is it a problem if a customer deliberately evades CTR filing requirements even though the source of the customer's funds is known to be legitimate?

Yes. The CTR requirement deals with reporting of the specified currency transactions and not with the legitimacy of the funds, per se. If a financial institution believes a customer is deliberately evading a reporting requirement for any reason, it should file a SAR, regardless of the perceived legitimacy of the customer's source of funds.

For further guidance on filing SARs and indicators of potentially suspicious activity, please refer to the Suspicious Activity Reports and Suspicious Activity Red Flags sections.

Form 8300

Form 8300 Basics

214. What is Form 8300, and when should it be used?

BSA Form 8300 (Cash Over 10K Received in Trade/Business) should be completed and submitted to the Internal Revenue Service (IRS) if a person engaged in trade or business who, in the course of that trade or business, receives more than US$10,000 in single or multiple related transactions in currency or covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

Form 8300 reporting requirements are implemented under regulation 31 C.F.R. 1010.330 – Reports Relating to Currency in Excess of US$10,000 received in a Trade or Business.

215. What is the value of Form 8300?

Form 8300 is useful to the IRS and law enforcement because it can be used to trace cash movements into the retail sector of the economy and link abnormal uses of cash with possible illicit sources of that cash. Additionally, it can be used by businesses not subject to Suspicious Activity Report (SAR) filing requirements to report suspicious activity.

216. What does the term "currency" mean for Form 8300 filing purposes?

"Currency" is defined, for Form 8300 purposes, as:

- U.S. and foreign coin and currency received in any transaction
- A cashier's check, money order, bank draft or traveller's check having a face amount of US$10,000 or less received in a designated reporting transaction, or received in any transaction in which the recipient knows the instrument is being used in an attempt to avoid reporting requirements

217. Is virtual currency considered "currency" for Form 8300 filing purposes?

No. Businesses are only required to file Form 8300 on currency transactions in excess of US$10,000 as defined above. Per FinCEN guidance, virtual currency does not meet the definition of currency for BSA reporting purposes as it does not have legal tender status.

State laws may soon require virtual currency businesses to submit reports on virtual currency transactions greater than US$10,000, similar to Form 8300 and CTRs. The New York State Department of Financial Services (DFS) was the first to propose in July 2014 a regulatory framework for virtual currency businesses, which was finalised in 2015.

Though they are not required to file Form 8300 on virtual currency transactions, a virtual currency exchanger dealing in certain types of virtual currency may fall under the definition of money transmitter and be subject to the AML/CFT requirements of a money services business (MSB). For further guidance, please refer to the sections: Money Services Businesses and Virtual Currency Systems and Participants.

218. What does the term "monetary instrument" mean for Form 8300 purposes?

"Monetary instrument" is defined, for Form 8300 purposes, as "a cashier's check (by whatever name called, including treasurer's check and bank check), bank draft, traveller's check, or money order having a face amount of not more than US$10,000."

219. What does the term "designated reporting transactions" mean for Form 8300 purposes?

A "designated reporting transaction" is a retail sale (i.e., "any sale … made in the course of a trade or business if that trade or business principally consists of making sales to ultimate consumers") or the receipt of currency or monetary instrument by an intermediary on behalf of the principal in connection with a retail sale of the following:

- A consumer durable (e.g., automobile, boat);
- A collectible (e.g., art, rug, antique, metal, gem, stamp); or
- Travel or entertainment activity (e.g., single trip, events).

220. Are there exceptions to the definition of "designated reporting transactions"?

Yes. In certain circumstances, cashier's checks, bank drafts, traveller's checks and money orders should not be treated like currency; therefore, are exempted from the definition of "designated reporting" transaction subject to Form 8300 reporting requirements. Examples of transactions exempted from reporting on Form 8300 include, but are not limited to, the following:

- Payments constituting proceeds from bank loans
- Payments made on certain instalment sales contracts or promissory notes
- Payments made in certain down payment plans

For further guidance and applicable restrictions, please refer to the examples provided in 31 C.F.R. 1010.330 – Reports Relating to Currency in Excess of $10,000 in a Trade or Business.

221. What are some examples of "designated reporting transactions" subject to Form 8300 reporting requirements?

The IRS provided the following examples of designated reporting transactions:

- Sale of goods, services or real or intangible property
- Cash exchanged for other cash
- Conversion of cash to a negotiable instrument, such as a check or a bond
- Establishment, maintenance of or contribution to a trust or escrow account
- Rental of goods or real or personal property
- Repayment of a loan

222. What does the term "related transactions" mean for Form 8300 purposes?

The term "related transactions" means transactions between a buyer or agent of the buyer and a seller that occur within a 24-hour period.

In addition, transactions more than 24 hours apart are "related" if the recipient of the cash knows, or has reason to know, that each transaction is one of a series of connected transactions. A series of connected transactions occurring within a 12-month period is considered reportable on Form 8300. For example, on February 1, a customer makes an initial payment in currency to a jewellery store in the amount of US$13,000 for a diamond necklace. The jewellery store receives subsequent currency payments for the necklace from the customer on March 30, April 1, and April 28 in the amounts of US$5,000, US$4,000 and US$11,000, respectively. All payments would be considered related transactions.

223. Should additional Form 8300s be filed on subsequent related payments aggregating to over US$10,000?

Each time payments aggregate in excess of US$10,000, the business must file another Form 8300 within 15 calendar days of the payment that causes the payments to exceed US$10,000. Using the previous example, the jewellery store must make a report by February 16 with respect to the payment received on February 1. The jewellery store also must make a report by May 13 with respect to the payments totalling US$20,000 received from March 30 through April 28 (i.e., within 15 days of the date that the subsequent payments, all of which were received within a 12-month period, exceeded US$10,000).

224. Do cash payments of exactly US$10,000 require a Form 8300?

No. Cash payments that aggregate to US$10,000 or less do not require Form 8300 to be submitted.

225. Can Form 8300 be submitted if the US$10,000 threshold is not met?

Yes, although Form 8300 would not be required to report the cash payment, it may be filed voluntarily with the Internal Revenue Service (IRS) for any suspicious transaction(s), even if the total does not

exceed US$10,000. For example, a business may opt to file Form 8300 to report a transaction that does not exceed US$10,000 because a customer is attempting to evade reporting requirements. For additional guidance on common red flags, please refer to the Suspicious Activity Red Flags section.

226. Do Form 8300 filing requirements apply to cash transactions received by financial institutions?

Financial institutions subject to CTR filing requirements are not required to file Form 8300 for designated reporting transactions.

227. Do Form 8300 filing requirements apply to cash payments received by court clerks?

Form 8300 is required to be filed by clerks of federal or state criminal courts who receive more than US$10,000 in cash as bail for the following offenses:

- Any federal offense involving a controlled substance;
- Racketeering;
- Money laundering; or
- Any state offenses substantially similar to the three listed above.

This became effective as of July 9, 2012.

Form 8300 reporting requirements for court clerks are implemented under regulation 31 C.F.R. 1010.331 – Reports Relating to Currency in Excess of US$10,000 Received as Bail by Court Clerks.

228. What does the term "court clerk" mean for Form 8300 filing purposes?

"Court clerk" is defined, for Form 8300 filing purposes, as "the clerk's office or the office, department, division, branch, or unit of the court that is authorised to receive bail."

229. Why was this exception made for court clerks?

Large currency payments to make bail in connection with the aforementioned offenses could be indicative of underlying criminal activity.

230. Are wholesalers subject to Form 8300 reporting requirements?

Wholesalers are required to file Form 8300 only for cash payments greater than US$10,000.

They are not required to report transactions paid with cashier's checks, bank drafts, traveller's checks or money orders, unless they know such instruments are being used to attempt to avoid the CTR or Form 8300 reporting requirements.

231. If a retailer also conducts wholesale transactions, must it report all transactions or just the retail ones?

If the trade or business of the seller principally consists of sales to ultimate consumers, then all sales, including wholesale transactions, are considered "retail sales" and are subject to Form 8300 reporting

requirements. Retail sales also include the receipt of funds by a broker or other intermediary in connection with a retail sale.

232. Are there exceptions to the Form 8300 reporting requirement?

Cash or covered monetary instruments in excess of US$10,000 received in a retail sale are not required to be reported if received:

- By financial institutions required to file CTRs
- By certain casinos having gross annual gaming revenue in excess of US$1 million
- By an agent who receives the cash from a principal, if the agent uses all of the cash within 15 days in a second transaction that is reportable on Form 8300 or a CTR, and discloses the name, address and taxpayer identification number (TIN) of the principal to the recipient of the cash in the second transaction
- In a transaction occurring entirely outside the United States, Puerto Rico, or a U.S. territory or possession (the negotiation of the transaction payment and delivery must all take place outside the United States)
- In a transaction that is not in the course of a person's trade or business

Governmental units are not required to file Form 8300, except for criminal court clerks.

233. Who has the authority to enforce compliance of the Form 8300 requirement?

The IRS Criminal Investigation Division (IRS-CI) has the authority to investigate possible criminal violations of the Form 8300 requirement. FinCEN retained the authority to assess civil money penalties against any person who violates the Form 8300 requirement.

234. What are the consequences for failing to file Form 8300?

Businesses can be subject to civil and/or criminal penalties for failure to: file timely forms; include complete and correct information on the forms; and furnish annual notifications to the subjects of Form 8300 filings. The type and size of assessed penalties are based on the following:

- Whether the failure was negligent or wilful
- Whether the failure was rectified in a timely manner (e.g., within 30 days of the date of detection)
- Whether annual gross receipts of the business exceed US$5 million

Criminal penalties may include imprisonment up to five years, plus the costs of prosecution.

235. What should a business do if it discovers it has failed to file Form 8300 on reportable transactions?

If a business finds it has failed to file Form 8300 on reportable transactions, it should move forward to file Form 8300 as soon as the failure is discovered. If there are a significant number of reports at issue, or if they cover transactions that are not relatively recent in time, the business should contact the IRS

to request a determination on whether the back-filing of unreported transactions is necessary. Prior to doing this, the business may wish to seek advice from counsel to ensure that communication with the authorities is handled properly and to inquire about obtaining an administrative waiver (i.e., Reasonable Cause Penalty Waiver).

236. What is the procedure for seeking a "Reasonable Cause Penalty Waiver"?

A "Reasonable Cause Penalty Waiver" is an administrative decision from the IRS that the failure to properly file Form 8300 was due to reasonable cause and not wilful neglect. Penalties for failure to file Form 8300 can be waived if the failure is due to reasonable cause and not due to wilful neglect.

To obtain a Reasonable Cause Penalty Waiver, a business must submit a written statement to the IRS campus to which it must file Form 8300 with the following information:

- Specific provision(s) under which the waiver is requested (e.g., mitigating factors, events contributing to the failure)
- The facts alleged as the basis for reasonable cause
- The signature of the person required to file the forms
- Declaration that the statement is made under penalties of perjury

The filer must establish that the failure arose from events beyond the filer's control; that the filer acted in a responsible manner before and after the failure occurred; and that attempts to rectify the failure were made promptly (e.g., within 30 days after the date the impediment was removed or the failure was discovered). Special rules apply to Taxpayer Identification Number (TIN) issues.

Annual Notification

237. Is a company required to inform the customer if a Form 8300 is filed?

Yes. The company must give a written or electronic statement to each person named on a required Form 8300 on or before January 31 of the year following the calendar year in which the reportable cash or monetary instrument is received.

238. Is a business required to notify a customer of the filing of Form 8300 at the time of sale?

No. A business is only required to inform the customer annually, as stated above. If there is only one Form 8300 filed on a customer during the year, a copy of Form 8300 can satisfy the annual statement requirement if it is sent to the last known address of the customer.

If more than one Form 8300 were filed, a single statement that aggregates the reportable transactions is required. Copies of Form 8300 are not required to be sent with the annual notification. Providing copies of Form 8300 to the payer at the time of sale does not satisfy the annual notification requirement.

It is important to note that if the suspicious transaction box was checked on Form 8300, a copy cannot be provided to the customer to satisfy the annual notification requirement. In this case, the business must send a statement with the required information in lieu of a copy of the form.

239. Is there a specific format for or guidance on how the customer should be notified of the filing of Form 8300?

There is no guidance on the format of the statement and only minimum requirements on the content of the statement. The statement can be written or electronic and must include the following:

- The name, telephone number, address and contact information of the business filing Form 8300
- The aggregate amount of reportable cash received by the person who filed Form 8300 during the calendar year in all related cash transactions
- A notification that the information contained in the statement is being reported to the IRS

240. If a business filed Form 8300 on an individual and checked the suspicious transaction box and Form 8300 was not required, does the business have to inform the individual that it filed Form 8300?

No. A business is only required to notify individuals if the filing of Form 8300 is required. More important, similar to Suspicious Activity Reports (SARs), a business is prohibited from informing the buyer that the suspicious transaction box was checked.

Completing and Filing of Form 8300

241. What is the time frame for filing Form 8300 with the IRS?

Each Form 8300 must be filed within 15 calendar days of the initial cash payment if it is more than US$10,000 or within 15 calendar days after receiving the payment that causes the aggregate amount to exceed US$10,000.

242. If the business is unable to obtain the TIN of a customer making a cash payment of more than US$10,000, should the business file a Form 8300 anyway?

Yes. The business should file Form 8300 with a statement explaining why the taxpayer identification number (TIN) is not included. Nevertheless, as a business is required to ask for the person's TIN, it may be subject to penalties for an incorrect or missing TIN.

243. Is the business required to verify the identity of the person from whom the currency is received?

Yes. The business is required to verify the identity of the person from whom the currency is received.

244. Are there additional filing requirements for court clerks subject to Form 8300 reporting requirements?

Yes. By the 15th day after reportable cash bail is received, court clerks must send a copy of each Form 8300 to the U.S. attorney in the jurisdiction in which the individual charged with the specified crime resides, and the jurisdiction in which the specified crime occurred, if different.

245. How can businesses submit Form 8300 to the IRS?

Although electronic filing is not mandatory, Form 8300 can be submitted electronically to the IRS through the BSA E-Filing System or manually.

Paper Form 8300 should be mailed to the IRS Enterprise Computing Center – Detroit.

246. Will FinCEN accept Form 8300 submitted in paper format?

After March 31, 2013, FinCEN no longer accepted legacy reports (e.g., previous or paper versions of FinCEN Reports), except Form 8300. As stated above, Form 8300 can be submitted via the BSA E-Filing System or through the mail.

247. How long should a copy of Form 8300 be retained?

A company should retain each Form 8300 for a minimum of five years from the date of filing.

248. In addition to Form 8300, should additional documentation relating to the filing be maintained?

A copy of the notice to the person named on Form 8300 also should be maintained for a minimum of five years from the date of filing.

249. Has any guidance been issued on the reporting requirements of Form 8300?

Yes. The following guidance has been issued by the IRS on the reporting requirements of Form 8300:

- **Publication 1544, Reporting Cash Payments of Over $10,000 (Received in a Trade or Business)** (2012)
- **Form 8300 – Report of Cash Payments Over $10,000 Received in a Trade or Business** (Online Video) (2011)
- **When Businesses Should File Form 8300 for Cash Transactions** (Webinar) (2009)
- **Workbook on Reporting Cash Payments of Over $10,000** (2012)
- **FAQs Regarding Reporting Cash Payments of Over $10,000** (Form 8300) (2012)

Reporting Suspicious Activity on Form 8300

250. Can potentially suspicious activity be reported on Form 8300?

Yes. There is a checkbox on the top of Form 8300 that indicates if the reported transaction is considered suspicious.

251. Do the details of the suspicious nature of the transaction need to be provided on Form 8300?

The details of the suspicious nature of the transaction can be provided in the "Comment" field on Form 8300. The local IRS Criminal Division or other law enforcement also can be contacted to report suspicious transactions and provide additional detail.

252. Does the Safe Harbor provision apply to reports of suspicious activity made on Form 8300?

Yes. The Safe Harbor provision applies to all reports of suspicious activity to FinCEN, whether mandatory or voluntary, including suspicious activity reported on Form 8300. For further guidance, please refer to the Safe Harbor section.

253. Can Form 8300 be submitted for suspicious activity if the US$10,000 threshold is not met?

Yes. Although Form 8300 is not required to report the cash payment, it may be filed voluntarily with the IRS for any suspicious transaction(s), even if the total does not exceed US$10,000. For example, a business may opt to file Form 8300 to report a transaction that does not exceed US$10,000 because a customer is attempting to evade reporting requirements.

For additional guidance on common red flags, please refer to the Suspicious Activity Red Flags section.

Suspicious Activity Reports

SAR Basics

254. What is a Suspicious Activity Report?

A Suspicious Activity Report (SAR), FinCEN Form 111, is a report that documents suspicious or potentially suspicious activity (e.g., has no business purpose or apparent lawful purpose) attempted or conducted at or through a financial institution.

SARs for depository institutions are required by 31 C.F.R. 1020.320 – Reports by banks of suspicious transactions.

255. What is the value of SARs to law enforcement?

SARs have been instrumental in enabling law enforcement to initiate or supplement major money laundering or terrorist financing investigations. Information provided in SARs also presents FinCEN

with a method of identifying emerging trends and patterns associated with financial crimes, which is vital to law enforcement agencies.

256. Which entities are required to file SARs?

At the time of this publication's preparation, the following entities were required to file SARs:

- Depository institutions (including insured banks, savings associations, savings associations service corporations, credit unions, U.S. branches and agencies of foreign banks)
- Broker-dealers in securities
- Futures commission merchants (FCMs)
- Introducing brokers (IBs) in commodities
- Money services businesses (MSBs) (e.g., money transmitters, check cashers, providers and sellers of prepaid access)
- Casinos and card clubs
- Mutual funds
- Insurance companies
- Loan or finance companies (e.g., nonbank residential mortgage lenders or originators [RMLOs])
- Housing Government-Sponsored Enterprises (GSEs)

Additionally, bank holding companies (BHC), nonbank subsidiaries of bank holding companies, Edge and agreement corporations (and any branch thereof) are required to file SARs.

As AML/CFT regulations continue to evolve, other types of financial institutions also may be required to file SARs. Many other types of financial institutions may voluntarily file SARs. Suspicious activity also can be reported voluntarily to FinCEN through Form 8300. For further guidance, please refer to the Form 8300 section.

257. Are there different types of SAR reports for various filers?

No. Beginning March 29, 2012, FinCEN replaced industry-specific SARs with a single report that must be submitted electronically through the BSA E-Filing System. A one-year transition period to e-filing was permitted, but after March 21, 2013, legacy SARs are no longer accepted.

For additional guidance on the SAR reporting requirements for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

258. What types of activities require a SAR to be filed for depository institutions?

Upon the detection of the following activities, a depository institution should file a SAR:

- **Insider abuse involving any amount** – An institution should file a SAR whenever it detects any known or suspected federal criminal violations or pattern of violations to have been committed or attempted through it or against it. An institution also should file a SAR for any

transactions, regardless of the transaction amount(s) conducted through it, where the institution believes that one of its directors, officers, employees, agents or any other institution-affiliated party has committed or aided in any criminal act of which the financial institution believes it was either an actual or a potential victim of a crime, or series of crimes, or was used to facilitate a criminal transaction.

- **Violations aggregating to US$5,000 or more where a suspect can be identified** – A SAR should be filed in any instance where the financial institution detects or feels it was either an actual victim or a potential victim of a federal criminal violation, or detects or feels it was used as a vehicle to facilitate illicit transactions that total or aggregate to US$5,000 or more in funds or other assets by an identified suspect or group of suspects that it had a substantial basis for identifying. If the financial institution believes the suspect used an alias, it should document as much information as is available pertaining to the true identification of the suspect or group of suspects, including any of the alias identifiers (e.g., driver's license number, Social Security number [SSN], address, telephone number) and report such information.
- **Violations aggregating to US$25,000 or more regardless of a potential suspect** – A SAR should be filed in any instance where the financial institution detects or feels it was either an actual victim or a potential victim of a federal criminal violation, or detects or feels it was used as a vehicle to facilitate illicit transactions that total or aggregate to US$25,000 in funds or other assets, even if there is no substantial basis for identifying a possible suspect or group of suspects.
- **Transactions aggregating to US$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA)** – A SAR should be filed when any transaction(s) totalling or aggregating to at least US$5,000 conducted by a suspect through the financial institution where the institution knows, suspects or has reason to suspect that the transaction involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; is designed to evade any BSA regulations; or has no business nor apparent lawful purpose or is not the type in which the particular customer normally would be expected to engage, and the financial institution knows of no reasonable explanation for the transaction after examining available facts, including the background and possible purpose of the transaction.
- **Unauthorised Electronic Intrusion** – A SAR should be filed whenever it is discovered that access has been gained to a computer system of a financial institution either to remove, steal, procure or otherwise affect funds of the institution, funds of the institution's customers, critical information of the institution, including customer account information, or to damage, disable or otherwise affect critical systems of the institution. Computer intrusion does not include attempted intrusions of websites or other noncritical information systems of the financial institution or customers of the institution.

For additional types of activities requiring a SAR filing for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section. For red flags to assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

259. Is the aggregate threshold of US$5,000 for potentially suspicious activity the same for all types of financial institutions required to file SARs?

No. The aggregate threshold for all other types of financial institutions required to file SARs (e.g., broker-dealer in securities, insurance companies, casinos and card clubs), is the same as for deposit institutions, US$5,000; but the aggregate threshold for money services businesses (MSBs) is US$2,000. For further guidance, please refer to the Nonbank Financial Institution and Nonfinancial Businesses section.

260. What is the difference between "unauthorised electronic intrusion" and "account takeover"?

The primary target of "account takeovers" is the customer. The primary target of "unauthorised electronic intrusion," formerly "computer intrusion," is the financial institution.

261. What does the term "transaction" mean for SAR filing purposes?

The term "transaction" includes deposits, withdrawals, inter-account transfers, currency exchanges, extensions of credit, purchases/sales of stocks, securities or bonds, certificates of deposit or monetary instruments or investment security, automated clearing house (ACH) transactions, ATM transactions or any other payment, transfer or delivery by, through or to a financial institution, by any means.

262. Should a financial institution refuse to execute the transaction if it believes the transaction will be included in a future SAR filing?

In circumstances where a SAR is warranted, the financial institution is not expected to stop the processing of the transaction. However, financial institutions proceed at their own risk when continuing to allow the suspect transactions to occur.

263. Are there exceptions to the SAR filing requirement for depository institutions?

Yes. Robberies and burglaries that are reported to local authorities (except for savings associations and service corporations), or lost, missing, counterfeit or stolen securities that are reported through the Lost and Stolen Securities Program Database (LSSP), do not require SAR filings.

For additional guidance on exceptions to the SAR reporting requirements for NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

264. Are transactions that were not completed exempt from the SAR filing requirement?

No. Transactions that were not completed (e.g., customer changed his or her mind before the transaction was executed) are not exempt from the requirement.

265. Where are SARs filed?

SARs are filed with FinCEN at the IRS Enterprise Computing Center – Detroit (formerly the Detroit Computing Center). They are then made available to appropriate law enforcement agencies to assist with the investigation and prosecution of criminal activity. Some states require that copies of SARs involving their state be sent to them as well.

Beginning July 1, 2012, financial institutions must submit SARs through the BSA E-Filing System, an internet-based e-filing system developed by FinCEN to enable financial institutions to file FinCEN Reports electronically. For further guidance, please refer to the Filing SARs section.

266. Who should make the final decision on whether to file a SAR?

The filing of a SAR should not be a business decision, but rather a compliance decision. As such, the decision usually rests with a member of the compliance department, often the AML compliance officer.

Alternatively, some financial institutions assign the decision-making role to an AML compliance committee that should include representatives of the compliance department and senior management.

It is important to note that the board of directors only needs to be notified of SAR filings; the board does not need to be involved in the decision to file or not file a SAR. Prudent risk management dictates that senior management, aside from AML compliance personnel, also be apprised.

267. Should a financial institution file SARs on activity outside of the United States?

Consistent with SAR requirements, financial institutions should file SARs on suspicious activity involving the United States even when a portion of the activity occurs outside of the United States or when suspicious funds originate from, or are disbursed outside of, the United States.

Although, in general, non-U.S. operations of U.S. organisations are not required to file SARs in the United States, an institution may wish, for example, to file a SAR voluntarily on activity that occurs outside of the United States, especially if it has the potential to have an impact on the reputation of the overall institution. In any case, institutions also should report suspicious activity to local authorities consistent with local laws and regulations.

Financial institutions should seek the advice of legal counsel or other appropriate advisers regarding their regulators' expectations on filing a SAR on activity that occurs outside of the United States, but the transaction data flows through one, or more, of their U.S. systems, or otherwise involves an individual or business in the United States.

268. FinCEN has discouraged the filing of defensive SARs. What does the term "defensive SAR" mean?

A defensive SAR is one not necessarily supported by a thoughtful and thorough investigation, which may be made on cursory facts to guard against receiving citations during regulatory examinations for not filing SARs. Defensive SARs can dilute the quality of information forwarded to FinCEN and used by law enforcement and, therefore, are discouraged. Financial institutions are encouraged to implement a risk-based process for identifying potentially suspicious activity and document all

decisions to file or not file a SAR to prevent regulatory criticism. Regulatory agencies continue to emphasise that examinations are focused on whether a financial institution has an effective SAR decision-making process in place, and not on individual SAR decisions, unless the failure to file a SAR is significant or accompanied by evidence of bad faith.

269. How do U.S. SAR requirements correspond to FATF Recommendations related to suspicious activities?

U.S. SAR requirements parallel the FATF Recommendations as outlined below:

- **Recommendation 20 – Reporting of Suspicious Transactions** – FATF recommends financial institutions be required by law to report suspicious transactions involving funds derived from all predicate offenses for money laundering through suspicious transaction reports (STRs) to its financial intelligence unit (FIU). Recommendation 20 applies to attempted transactions as well. FATF Recommendation 3 outlines suggested predicate offenses.

  The SAR, the STR-equivalent, is filed with FinCEN, the U.S. FIU.

- **Recommendation 21 – Tipping-Off and Confidentiality** – FATF recommends that a financial institution and its directors, officers and employees be protected by law from criminal and civil liability when reporting suspicious transactions in good faith to its FIU. Additionally, FATF recommends that STRs and related information be kept confidential.

  The BSA prohibits financial institutions from disclosing the filing of SARs. Financial institutions are also protected by law under the safe harbour provision. For further guidance, please refer to the Confidentiality and Safe Harbor sections.

- **Recommendation 33 – Statistics and Recommendation 34 – Guidance and Feedback** – FATF recommends the collection, maintenance, analysis and dissemination of comprehensive statistics related to the effectiveness and efficiency of a country's AML/CFT system. Types of feedback include, but are not limited to statistics on suspicious transaction reports (STRs); ML and TF investigations, prosecutions and convictions; frozen, seized and confiscated assets; and mutual legal assistance and international requests for cooperation. FATF also recommends the sharing of guidance and feedback from FIUs with financial institutions to assist in improving AML/CFT measures, particularly as it relates to STRs.

  FinCEN regularly issues statistics and guidance on SARs and other BSA-related matters. For further guidance, please refer to the SAR Statistics and Trends section.

For further guidance on the FATF Recommendations, please refer to the Financial Action Task Force section.

270. What information and guidance have been issued with respect to SARs?

FinCEN has issued the following key guidance to assist persons with the completion, filing and sharing of Suspicious Activity Reports (SARs):

- The SAR Activity Review: "Trends, Tips & Issues"

- SAR Stats (formerly The SAR Activity Review: "By the Numbers")
- Index to Topics for The SAR Activity Review: An Assessment Based Upon Suspicious Activity Report Filing Analysis
- Confidentiality and Joint Filings:
  - Unauthorised Disclosure of Suspicious Activity Reports (2004)
  - Confidentiality of Suspicious Activity Reports (2011)
  - SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions (2012)
  - FinCEN Rule Strengthens SAR Confidentiality (2010)
  - Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (2006)
  - Unitary Filing of Suspicious Activity and [OFAC] Blocking Reports/Interpretation of Suspicious Activity Reporting Requirements to Permit the Unitary Filing of Suspicious Activity and Blocking Reports (2004)
  - Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies (2006)
- Completing and Filing SARs:
  - Frequently Asked Questions Regarding the FinCEN Suspicious Activity Report (SAR) (2013)
  - BSA E-Filing System: Frequently Asked Questions (FAQs) (2010)
  - Filing FinCEN's New Currency Transaction Report & Suspicious Activity Report (2012)
  - Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting (2007)
  - Requirements for Correcting Errors in Electronically Batch-Filed Suspicious Activity Reports (2009)
  - Suspicious Activity Report Supporting Documentation (2007)
- Guidance by Industry:
  - Reporting Suspicious Activity – A Quick Reference Guide for MSBs (No date found)
  - Suspicious Activity Reporting Guidance for Casinos (2003)
  - How Casino SAR Reporting Has Increased Since 2004 (2012)
  - Frequently Asked Questions: Suspicious Activity Reporting Requirements for Mutual Funds (2006)

  - Frequently Asked Questions: Anti-Money Laundering Program and Suspicious Activity Reporting Requirements for Insurance Companies (2006)

- Mortgage Fraud and Real Estate SAR-Related Guidance:
  - FinCEN Mortgage Fraud SAR Datasets
  - Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding Loan Modification/Foreclosure Rescue Scams (2009)
  - Mortgage Loan Fraud Update: Suspicious Activity Report Filings (various dates)
  - Suspicious Activity Related to Mortgage Loan Fraud (August 16, 2012)
  - FinCEN Assesses Suspicious Activity Involving Title and Escrow Companies (2012)
  - California, Nevada, Florida Top Mortgage Fraud SAR List (2012)
  - FinCEN Attributes Increase in Suspicious Activity Reports Involving Mortgage Fraud to Repurchase Demands (2011)
  - Mortgage Loan Fraud Connections with Other Financial Crime (2009)
  - Filing Trends in Mortgage Loan Fraud (2007)
  - Mortgage Loan Fraud: An Update of Trends Based Upon an Analysis of Suspicious Activity Reports (2008)
  - FinCEN Mortgage Loan Fraud Assessment (2006)
  - FinCEN's 2010 Mortgage Fraud Report: SAR Filings Up; Potential Abuse of Bankruptcy Identified (2011)
- Trade-Based Money Laundering, Corruption, Identity Theft and Other Topics Related to SARs:
  - Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption (2008)
  - Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering (2010)
  - Identity Theft: Trends, Patterns, and Typologies Based on Suspicious Activity Reports (2011)
  - FinCEN Examines Identity-Theft Related SARs Filed by Securities & Futures Firms (2011)
  - FinCEN Study Examines Rise in Identity Theft SARs (October 2010)
  - Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency (2010) (related to inclusion of "MX Restriction" in SAR Narratives)

The U.S. Government Accountability Office (GAO) has also issued reports to Congress on SARs and the sharing of information on suspicious activities, including, but not limited to, the following:

- Bank Secrecy Act: FinCEN Needs to Further Develop Its Form Revision Process for Suspicious Activity Reports (2010)
- Bank Secrecy Act: Suspicious Activity Report Use is Increasing, but FinCEN Needs to Further Develop and Document its Form Revision Process (2009)
- Information Sharing: Federal Agencies are Sharing Border and Terrorism Information with Local and Tribal Law Enforcement Agencies, but Additional Efforts are Needed (2009)
- Information Sharing Environment: Definition of the Results to be Achieved in Improving Terrorism-Related Information Sharing is Needed to Guide Implementation and Assess Progress (2008)
- Intellectual Property: Better Data Analysis and Integration Could Help U.S. Customs and Border Protection Improve Border Enforcement Efforts (2007)
- Money Laundering: Oversight of Suspicious Activity Reporting at Bank-Affiliated Broker-Dealers Ceased (2001)

SAR Filing Time Frame and Date of Initial Detection

271. What is the time frame for filing SARs?

SARs must be filed within 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If the identity of the suspect is not known on the date of initial detection of the incident, a financial institution may delay filing the SAR for an additional 30 calendar days to identify the suspect. In no case may the reporting be delayed more than 60 calendar days after the date of initial detection of a reportable transaction.

272. What does the term "date of initial detection" mean for SAR filing purposes?

The period for filing a SAR begins when the financial institution, during its review of transaction or account activity or because of other factors, knows or has reason to suspect that the activity or transactions under review meet one or more of the definitions of suspicious activity. FinCEN recognises that it can take some time for an institution to conduct the research to reach this conclusion, but recommends that internal reviews be as expeditious as possible. The term "date of initial detection" does not necessarily mean the moment a transaction is highlighted for review. However, an expeditious review of the transaction or account should occur, and in any event, the review should be completed in a reasonable amount of time.

In instances where a financial institution uses automated software to detect unusual transactions, the date of initial detection is usually considered the date on which the financial institution concludes that the activity is suspicious, not the date an alert was generated by the system. However, the financial institution should have protocols in place to establish the length of time after which a transaction, flagged by the system, should be investigated, and those procedures should be documented and followed.

273. What if 30 calendar days is not a sufficient amount of time for a financial institution to investigate fully the circumstances surrounding suspicious activity?

Regardless of the status of a financial institution's internal investigation, a SAR must be filed within 30 calendar days after the date of detection, except as described below. If a financial institution has not completed its internal investigation, a SAR should be filed with the qualification that the filing is on a preliminary basis and that a follow-up SAR will be filed once the institution has completed its investigation and has more information.

Financial institutions that file follow-up SARs should ensure the follow-up SAR provides full details of the initial SAR to aid law enforcement agencies in their investigative efforts.

274. Are there any exceptions to the 30-calendar-day time frame for filing SARs?

If the identity of the suspect is not known, a financial institution may take 60 calendar days after the date of initial detection to file a SAR, in order to identify the suspect.

275. What is an example in which a financial institution would have 60 calendar days to file a SAR?

Example: An individual unsuccessfully attempts a fraudulent transaction at a bank teller line. In this case, the individual may walk away without the bank obtaining any information about the customer. The bank can use the 30-calendar-day extension to try to obtain the identity of the individual.

In reality, the 30-calendar-day filing extension is applied in very limited circumstances, as financial institutions generally will know or will not be able to obtain at all the identity of the potential suspect(s).

276. What should a financial institution do if it "detects" reportable suspicious activity at a significantly later time than its occurrence?

The SAR filing requirements indicate that a financial institution is required to file a SAR no later than 30 calendar days after the date of initial detection of facts that may constitute a basis for filing a SAR. If the financial institution did not discover the suspicious activity until later, the financial institution still likely will need to file the SAR, but should consult with counsel on how best to handle the filings.

277. How long should financial institutions monitor activity of a SAR subject after filing a SAR?

Regulatory guidance suggests that financial institutions should monitor continuing suspicious activity every 90 days and file a report within 30 days of the detection of potentially suspicious activity. Therefore, financial institutions should monitor activities of a SAR subject for at least 90 calendar days after a SAR filing to determine if a follow-up SAR should be filed on continuing activity. Many financial institutions elect to monitor for additional 90-day periods until they are comfortable that the suspicious activity is not continuing.

Completion of a SAR

278. Who should be included in Subject Information on the SAR?

A person who or an entity that is a subject of the investigation should be included in the Subject Information on the SAR. The subject might be the account holder; it might be a party transacting business with the account holder; or, in the case of correspondent banking relationships or other clearing arrangements, it might be the customer of the financial institution's customer. The narrative should describe the occupation, position or title of the subject, and the nature of the subject's business. However, if more than one individual or business is involved in the suspicious activity, all subjects and any known relationships should be described in the SAR narrative.

In cases where the account holder is not the subject of the investigation, but is involved (e.g., a victim of identity theft), the names of related parties should be captured in the narrative of the SAR.

279. Should all signers of an account be included in Subject Information on the SAR?

It is at a financial institution's discretion whether to list all signers as subjects on a SAR. For example, if there are two signers on an account, yet the activity or actions of only one is deemed suspicious, the financial institution should list only one subject on the SAR, but include the other signer in the narrative of the report.

280. Should beneficial owners be included in Subject Information on the SAR?

As with signers, it is at a financial institution's discretion to list all beneficial owners as subjects on a SAR. At a minimum, activity of beneficial owners should be reviewed during the investigation to determine if activity conducted by beneficial owners is deemed suspicious and warrants inclusion on the SAR.

281. What dates should be entered in Date or Date Range of Suspicious Activity on the SAR?

The Date or Date Range on the SAR is reserved for the beginning and end dates of the reported suspicious activity, not the date range during which the customer's accounts were reviewed. For example, an account may be reviewed from January 1, 2016, to June 30, 2016, as part of an internal investigation; however, the reportable activity only may have occurred from February 4, 2016, to February 28, 2016. It is this latter date range that should be entered as the date range of suspicious activity on the SAR.

Additionally, if the activity occurred on one day, the same date will be entered for the beginning date and end date of suspicious activity.

282. What steps should a financial institution take to calculate Total Dollar Amount Involved in Known or Suspicious Activity?

Suspicious activity should be reported on a gross transaction-in and transaction-out basis. Deposits and withdrawals should not be netted. Additionally, all transactions identified as suspicious should be included in the total. For example, if an individual structured cash deposits in the amount of

US$100,000 into his or her commercial account, and the funds were later wired out of the account to a luxury auto dealer, the total reportable suspicious activity would be US$200,000. In all instances, the amount reported should be rounded up to the nearest whole dollar.

283. What steps should a financial institution take to calculate Total Dollar Amount Involved in Known or Suspicious Activity, if the activity is conducted in a foreign currency?

The financial institution should convert the foreign currency amount(s) into U.S. currency. The type of foreign currency should be detailed in the SAR narrative.

284. What accounts should be included in Account Number(s) Affected on the SAR?

All accounts at a financial institution in which the reportable activity was discovered should be included on the SAR with the status of the account at the time of the filing (opened/closed).

Even when it is not necessary to include additional accounts in a SAR (such as where it is determined the account was not affected by the suspicious activity), financial institutions should identify and document the review of related accounts in internal investigations leading to the SAR. As stated above, the final action of the financial institution (e.g., close account, monitor relationship, exit relationship) should be documented in the narrative of the SAR.

285. What level of detail should a financial institution include in the Suspicious Activity Information Narrative on the SAR?

The Suspicious Activity Information Narrative on the SAR requires an explanation of the nature of the suspicious activity. The purpose of this section is to provide law enforcement agencies with as much information as possible to investigate the activity further. It is important that financial institutions provide sufficient detail in this section to transfer their knowledge of the activity to law enforcement agencies.

This section should provide the facts of the activity, and the narrative should cover who, what, where, when and why, including, but not limited to, the date(s), amount(s), location(s), type(s) of transaction(s), name(s) of the party(ies) involved in the transaction(s) and the alert(s)/trigger(s) that initiated the SAR. All account numbers at the institution affected by the suspicious activity should be identified and, when possible, account numbers, names and locations at other institutions as well. Transactions should be listed chronologically, individually and by type (e.g., cash, wires and checks).

Financial institutions can submit a comma-separated values (CSV) file as an attachment that details the potentially suspicious transactions to supplement information provided in the SAR narrative.

If the subject of the filing is a customer of the institution, sufficient background information about the customer should be provided, including, but not limited to, additional Know Your Customer (KYC) information, known relationships and customer statements. If the subject is not a customer, information must be provided about the party(ies) involved to the extent possible.

If previous SARs have been filed on the same party, it is important to provide references, such as the date and details of these previous filings. The narrative should “tell the story” of why the financial

institution believes the transaction activity is suspicious, and clearly state the final action taken (e.g., exit relationship, monitor the relationship) in the investigation.

286. When should financial institutions include key phrases such as "MX Restriction," "Advisory Human Trafficking," "Foreign Corruption," "Marijuana Termination," "BEC Fraud" and "EAC Fraud" in their SAR narratives?

Financial institutions should include the phrase "MX Restriction" within the narrative of SARs when reporting suspicious transactions that include activities that may have been impacted due to Mexico's regulation restricting U.S. currency transactions in Mexican financial institutions.

The "MX Restriction" phrase enables FinCEN to identify changes in money laundering methodologies by reporting on trends identified in SAR filings. Since the regulatory changes in Mexico, bulk cash smuggling has decreased and shifted to other methods to transfer funds (e.g., use of funnel accounts to move illicit proceeds).

FinCEN requested that financial institutions include the phrases "Advisory Human Trafficking," and "Advisory Human Smuggling" when reporting suspicious activity related to underlying crimes related to human trafficking and smuggling; "Foreign Corruption" related to corruption of foreign officials; and "Marijuana Limited," "Marijuana Priority" and "Marijuana Termination" related to the activities of marijuana-related business [MRB] customers.

When filing a SAR on Business E-Mail Compromise (BEC) or E-Mail Account Compromise (EAC), FinCEN requests financial institutions to include the appropriate key term "BEC Fraud" and/or "EAC Fraud" in the SAR narrative and in the SAR Characterisations field as well as wire and scheme details.

For further guidance, please refer to the sections: Restrictions on U.S. Currency Transactions with Mexican Financial Institutions, Human Trafficking and Migrant Smuggling Red Flags, Senior Foreign Political Figures, Politically Exposed Persons, Marijuana-Related Businesses and Business Email Compromise and Email Account Compromise.

287. What information should financial institutions include when filing SARs on cyber-related events or cyber-enabled crimes?

When filing a SAR, FinCEN requests financial institutions to include cyber-related information and identifiers including, but not limited to, the following:

- Source and Destination Information:
  - IP address and port information with respective date timestamps in UTC (Coordinated Universal Time)
  - Uniform Resource Locator (URL)
  - Attack vectors
  - Command-and-control nodes
- File Information:
  - Suspected malware filenames

  - MD5, SHA-1 or SHA-256 hash information
  - Email content
- Subject User Names:
  - Email addresses
  - Social media accounts/screen names
- System Modifications:
  - Registry modifications
  - Indicators of compromise (IOCs)
  - Common vulnerabilities and exposures (CVEs)
- Involved Account Information:
  - Affected account information
  - Involved virtual currency accounts

288. What recent updates were proposed for the SAR?

In February 2017, FinCEN announced new and updated SAR fields to improve the layout of the SAR. Significant changes included adding a note to identify SARs filed due to geographic targeting orders (GTOs) or BSA advisories, adding a field to identify human trafficking/smuggling and adding a field to distinguish between cyber events against the financial institution versus the customers of the financial institution.

These updates do not change existing regulatory requirements for SARs.

289. Is a financial institution required to identify the underlying predicate crime of the SAR?

No. A financial institution is required to report suspicious activity that may involve illicit activity; a financial institution is not obligated to determine, confirm or prove the underlying predicate crime (e.g., terrorist financing, money laundering, identity theft, wire fraud). The investigation of the underlying crime is the responsibility of law enforcement.

When evaluating suspicious activity and completing the SAR report, financial institutions should, to the best of their ability, describe the suspicious activity by selecting all applicable characteristics as provided on the SAR (e.g., bribery/gratuity, defalcation/embezzlement).

It is helpful for those responsible for conducting investigations in a financial institution to have a basic understanding of certain crimes to assist in detecting and reporting relevant information to law enforcement.

For further guidance on conducting investigations, please refer to the Transaction Monitoring, Investigations and Red Flags section.

Filing SARs

290. How can financial institutions submit SARs to FinCEN?

Beginning July 1, 2012, FinCEN requires that all SARs be filed through the BSA E-Filing System. Further information can be found on the U.S. Treasury Department website: http://bsaefiling.fincen.treas.gov/main.html.

291. How can financial institutions file corrected or amended SARs through the BSA E-Filing System?

Financial institutions can file amended or corrected SARs by entering the Document Control Number (DCN)/BSA Identifier (ID) of the previous SAR and selecting "Correct/Amend Prior Report" in the BSA E-Filing System. The DCN/BSA ID can be retrieved from the acknowledgement received by the filer after successful submission and acceptance of the previous SAR filing.

292. Within what time frame must financial institutions correct primary file errors and file corrected/amended SARs?

FinCEN recommends that corrections be made no later than 30 calendar days after receiving the error notification from FinCEN.

293. What should financial institutions do if they are unable to implement corrections within 30 calendar days?

Financial institutions should notify FinCEN, in writing, with:

- An explanation of the technical issues that prevented them from implementing corrections within the recommended time frame;
- An estimate of when the issues will be resolved; and
- Contact information (name and telephone number).

Correspondence should be addressed to:

Financial Crimes Enforcement Network
Office of Compliance
P.O. Box 39
Vienna, VA 22183

294. Does the rejection of a batch file obviate the financial institution's responsibility to file a SAR within 30 calendar days of the date of detection?

No. Financial institutions must file initial SARs within 30 calendar days of the date of detection regardless of when the batch file was processed.

295. How soon should a financial institution file corrected/amended SARs after receiving an error notification from FinCEN?

Financial institutions should file corrected/amended SARs no later than 30 calendar days after receiving the error notification from FinCEN.

296. How long should financial institutions retain SARs?

SARs and the supporting documentation (original or business record equivalent) to the SAR must be retained for a minimum of five years from the date of the SAR filing. An institution also should check applicable state documentation retention laws to understand if the state requires the institution to submit to it a copy of the SAR. All supporting documentation related to a SAR must be made available to appropriate authorities upon request. For further guidance, please refer to the BSA Recordkeeping section.

297. Since financial institutions submit SARs to FinCEN through the BSA E-Filing System, are they still required to retain copies in accordance with AML/CFT laws and regulations?

Yes. The BSA E-Filing System is not a recordkeeping program. Financial institutions are required to retain SARs for a minimum of five years from the date of filing in accordance with AML/CFT laws and regulations.

298. What does the term "supporting documentation" mean for SAR filing purposes?

The term "supporting documentation" refers to all documents or records that assisted a financial institution with making the determination that certain activity required a SAR filing and any related investigation. The amount of supporting documentation obtained during the course of the investigation (e.g., transaction records, new account information, tape recordings, email messages) depends on the facts and circumstances of each investigation. A financial institution's procedures should outline how documentation is collected and stored.

Financial institutions have the ability to submit supporting documentation electronically as a CSV file within the narrative section of the SAR. While the submission of a CSV file is not required nor does it constitute a completed narrative, financial institutions should consider any additional documentation that may aid law enforcement.

299. When filing a SAR, should a financial institution forward supporting documentation to FinCEN?

Since July 1, 2012, financial institutions have had the ability to electronically submit supporting documentation as a CSV file within the narrative section of the SAR. Submitting supporting documentation is not required. Whether or not the documents are submitted, such documentation should be retained by the institution for at least five years from the date the SAR is filed, or possibly longer, if a state or self-regulatory organisation (SRO) has more stringent requirements. Law enforcement and/or regulators may request additional information about or supporting documentation for SARs after they are filed. The importance of a solid case management and filing

system is critical in satisfying these requests within the specified time frame. The SAR should, however, within the SAR narrative, disclose the available documentation.

300. Should financial institutions submit CSV files with detailed transaction activity as a substitute for the SAR narrative?

No. The CSV attachments are considered a part of the SAR narrative and should not be submitted in lieu of a detailed SAR narrative.

301. What should a financial institution do if the SAR it submitted has errors?

FinCEN has issued specific guidance regarding correcting errors in SARs filed through the BSA Direct E-Filing System. FinCEN guidance divides the errors into two categories: Primary and Secondary Errors. Primary Errors are errors that make locating the SAR difficult or seriously degrade the quality of the SAR. Financial institutions are required to file a corrected SAR for a Primary Error. Secondary Errors are errors that violate the form's instructions, but still allow law enforcement to understand the nature and details of the suspicious activity. Financial institutions are not required to file a corrected SAR for a Secondary Error.

Institutions should take a similar approach to correcting SARs filed manually. If an institution is uncertain whether or not it should re-file, it should consult with counsel.

302. What date should be used when filing a SAR correcting the previously filed report?

When filing a SAR that corrects a previously filed report, financial institutions should use the date that the current filing was prepared as the date of preparation.

Confidentiality

303. What obligations do financial institutions have with respect to SAR filings?

Financial institutions are obligated to file SARs in good faith and maintain the confidentiality of the SAR filing and any information that would reveal the existence of a SAR (SAR information). This means no financial institution, and no director, officer, employee or agent of the institution who/which files a SAR may notify any person or entity (or their agent, such as their attorney) involved in the transactions on which the SAR was filed that it has been reported. It is a crime to do so.

304. Does the SAR disclosure prohibition apply to supporting documentation created in an investigation that results in a SAR filing?

No. The SAR disclosure prohibition does not apply to the underlying facts, transactions and documents upon which a SAR is based. However, the confidentiality provision would apply to any documentation stating that a SAR has or has *not* been filed, as it would implicitly reveal the existence of a SAR.

305. Are there exceptions to the SAR disclosure prohibition?

Provided that no person involved in the transaction is notified that the transaction has been reported, the SAR disclosure prohibition does not include disclosures of SAR information to the following:

- FinCEN
- Any federal, state or local law enforcement agency (with jurisdiction)
- Any federal regulatory agency that examines the depository institution for compliance with the BSA
- Any state regulatory authority that examines the depository institution for compliance with state laws requiring compliance with the BSA

Guidance also has been provided by FinCEN on a depository institution's ability to share SAR information within its organisational structure to fulfil its duties under the BSA. Depository institutions may share SAR information with the following (subject to the limitation on disclosing a SAR to a party involved in the suspicious activity):

- Head office or controlling companies, whether domestic or foreign
- Domestic affiliates and subsidiaries that are also subject to SAR requirements

306. Does the confidentiality requirement for SARs prohibit a financial institution from notifying its business units that a SAR was filed involving one of its customers?

The confidentiality requirements do not preclude telling business units, although financial institutions must consider balancing "need to know" against the need to protect confidentiality and avoid tipping. One argument for telling a business unit about a SAR filing or information that would reveal the existence of a SAR is to prevent the business unit from soliciting additional business from a client about whom/which the compliance department may have concerns. However, the same message may be able to be sent by alerting the business unit to the underlying activity without detailing the filing of the SAR itself.

307. Can a financial institution share SARs or any information that would reveal the existence of a SAR with its head office and controlling companies?

Depository institutions are permitted to share the SAR or information related to the SAR with individuals within its corporate structure, such as directors or officers, provided "the purpose is consistent with regulations and/or guidance" and as long as the subject of the SAR is not notified that the transactions have been reported.

A U.S. branch or agency of a foreign bank may share SARs and any information that would reveal the existence of the SAR with its head office outside of the United States. Likewise, a financial institution may disclose a SAR to its holding company, no matter where the entity is located. Financial institutions should have written confidentiality agreements or arrangements in place specifying that the head office or holding company must protect the confidentiality of the SAR through appropriate internal controls.

308. Can SARs be shared with subsidiaries and affiliates?

Depository institutions are permitted to share SARs and information related to SARs with U.S. subsidiaries and affiliates as long as the subsidiary or affiliate is also subject to SAR regulations.

309. Can SARs be shared with foreign affiliates?

No. At the time of this publication, SARs or information that would reveal the existence of a SAR cannot be shared with foreign affiliates.

310. Can SARs be shared under information sharing under Section 314(b) of the USA PATRIOT Act?

Information sharing under Section 314(b) of the USA PATRIOT Act enables qualifying financial institutions that have notified FinCEN, regardless of relationship, to share information concerning suspected money laundering or terrorist activity with other financial institutions. Even under this information-sharing agreement, financial institutions are not allowed to disclose the filing of SARs; only the underlying transactional and customer information may be shared. For further guidance on information sharing under 314(b), please refer to the Section 314 – Cooperative Efforts to Deter Money Laundering section.

311. Does contacting the customer under investigation or witnesses to obtain explanations of the potentially suspicious activity violate the confidentiality of the SAR?

No, if no mention of the SAR is made. Institutions are expected to conduct a thorough investigation of all potentially suspicious activity, which may include requesting an explanation from customers or witnesses of the purpose of the underlying transactions. However, staff members responsible for contacting customers must protect the confidentiality of the SAR filing itself, and it may be appropriate to remind them of the need for confidentiality and careful preparation for the conversation with the customer. Breaching confidentiality could jeopardise investigations conducted by law enforcement agencies and result in sanctions.

312. What is an example of a witness and when might a witness be contacted?

Witnesses might include financial institution personnel who observed a transaction taking place, or a party to a transaction who is not the suspect. A witness could be contacted at any point during an investigation by the financial institution or a law enforcement agency to clarify the facts of an investigation.

313. Should FinCEN be notified when an inquiry regarding a SAR filing is made by an unauthorised person (e.g., suspect, suspect's relatives)?

Yes. If an unauthorised person (i.e., someone other than a representative of FinCEN, law enforcement or an appropriate regulator) makes an inquiry regarding a SAR filing, the financial institution should:

- Refuse to produce the SAR or provide any information that would disclose the SAR; and
- Notify the institution's regulator and FinCEN within a reasonable time period.

Inquiries may come in the form of subpoenas or requests to produce documents that would include the SAR filing or information regarding the SAR filing within their scope.

Financial institutions should also seek the advice of legal counsel upon receipt of an inquiry from an unauthorised person.

Third-Party and Joint Filings of SARs

314. Can financial institutions jointly file a SAR?

Under certain circumstances, a joint SAR may be filed when two or more financial institutions subject to suspicious activity reporting requirements are involved in a common or related transaction, each financial institution has information about the transaction, and the SAR subject(s) is not an insider of either financial institution. However, sharing of such information must be done in compliance with regulatory guidance and applicable privacy laws.

315. What is the purpose of joint SAR filings?

Joint SAR filings by multiple financial institutions can help to reduce redundant filings on the same transactions.

316. Are there situations in which a joint SAR filing is not permissible?

Yes. A joint SAR may not be filed if the subject of the SAR is an insider of the financial institution (i.e., employed, terminated, resigned or suspended).

317. Can a holding company file a SAR for an affiliate bank?

Yes. A holding company can file a SAR for an affiliate bank. When completing the SAR, the report should reflect the location where the transaction or suspicious activity occurred and the entity on whose behalf the SAR is being filed.

Safe Harbor

318. What protection is available to a financial institution when filing a SAR?

The Annunzio-Wylie Anti-Money Laundering Act of 1992 gives protection from civil liability to any covered financial institution that, or director, officer or employee who, makes a suspicious transaction report under any federal, state or local law. Section 351 of the USA PATRIOT Act further clarifies the terms of the Safe Harbor from civil liability when filing SARs. This protection does not apply if an action against an institution is brought by a government entity.

It is important to note that the Safe Harbor is applicable if a SAR is filed in good faith by a covered financial institution, regardless of whether such reports are filed pursuant to the SAR instructions. The Safe Harbor does not apply to SARs filed maliciously.

319. Have the courts upheld the Safe Harbor provision?

In 1999, in the case *Lee v. Bankers Trust Co.*, docket 98-7504, the U.S. 2nd Circuit Court of Appeals issued a verdict in favour of Bankers Trust by ruling that any statements made by Bankers Trust in a SAR could not serve as the basis of a defamation claim by the plaintiff because of the immunity provided by the Safe Harbor provision.

In 2003, in the case *Stoutt v. Banco Popular de Puerto Rico,* docket 01-2275, the U.S. 1st Circuit Court of Appeals granted summary judgment in favour of Banco Popular de Puerto Rico, dismissing Palmer

Paxton Stoutt's claims for malicious prosecution, unlawful arrest and incarceration, and defamation. Stoutt argued that the original Criminal Referral Form (CRF), a predecessor of the SAR, was not filed in good faith and that the follow-up discussions with federal authorities regarding the activity reported in the CRF fell outside the scope of the statute's protection. Although criminal charges against Stoutt were later dismissed, the court upheld that Banco Popular de Puerto Rico did, by any objective test, identify a "possible violation" of the law and had filed the CRF in "good faith" and that all ordinary follow-up answers to investigators with respect to the original CRF would be footnotes to the CRF and therefore should be similarly protected.

320. Are there any examples of financial institutions losing their Safe Harbor protection?

In 2001, Carroll County Circuit Court, Western Division, found the Bank of Eureka Springs and John Cross, the Bank's president and chief executive officer, guilty of the malicious prosecution of their client, Floyd Carroll Evans. The Bank of Eureka Springs was found to have maliciously filed two SARs on its client, misrepresented material facts to the prosecutor in regard to Evans' loan and mortgage, and attempted to derive financial benefit from the criminal prosecution by attempting to settle the case. In 2003, the bank and Cross attempted to appeal the decision, arguing that financial institutions that file SARs in error still should be protected under the Safe Harbor provision. The original ruling was upheld by the Supreme Court of Arkansas, docket 02-623, due to a finding of overwhelming evidence of malicious intent on behalf of the Bank of Eureka Springs in the first trial.

321. Does the Safe Harbor provision apply in cases of voluntary SAR filings?

Yes. The Safe Harbor provision applies to all SAR filings filed by a covered financial institution, as that term is defined in the USA PATRIOT Act, whether mandatory or voluntary.

322. Does the Safe Harbor provision apply to all parties in cases of joint SAR filings?

Yes. The Safe Harbor provision applies to all parties to a joint filing and not simply the party who files the SAR with FinCEN.

323. Does the Safe Harbor provision apply to methods of reporting suspicious activity other than actually filing a SAR?

Yes. Certain other forms of reporting, whether written or verbal, are covered by the Safe Harbor provision, so long as the other forms of suspicious activity reporting are through methods considered to be in accordance with the regulations of the applicable agency and applicable law.

324. Does the Safe Harbor provision apply to disclosure of SARs to appropriate law enforcement and supervisory agencies?

Yes. Disclosure of SARs and supporting documentation to a SAR to appropriate law enforcement and supervisory agencies with jurisdiction is protected by the Safe Harbor provisions applicable to both voluntary and mandatory suspicious activity reporting by financial institutions.

325. Does the Safe Harbor provision apply to disclosure of SARs to self-regulatory organisations (SROs)?

To enable SROs to monitor and examine members (e.g., broker-dealers in securities, futures commission merchants [FCMs], introducing brokers [IBs] in commodities) for compliance with AML/CFT laws and regulations, FinCEN issued a ruling allowing members to share SAR and SAR-information with their SROs, under certain circumstances, with the protection of the Safe Harbor provision.

For further guidance, please refer to 31 C.F.R. 1023.320 – Reports by Brokers or Dealers in Securities of Suspicious Transactions.

326. Is the Safe Harbor provision limited to SARs?

No. A "bank, and any director, officer, employee or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency with jurisdiction, including a disclosure made jointly with another institution involved in the same transaction, shall be protected" under the Safe Harbor provision of Section 351 of the USA PATRIOT Act.

Monitoring and Terminating Relationships with SAR Subjects

327. Should a financial institution automatically close all accounts of customers on which SARs were filed?

Financial institutions are not obligated to close an account on which a SAR has been filed. However, because leaving an account open may subject a financial institution to legal actions, enforcement actions and reputation risk, financial institutions should have procedures in place for considering account closure, particularly in instances where multiple SARs may have been filed on the same account or customer.

328. Who should make the final decision on whether to exit a relationship with a SAR subject?

The decision to exit a relationship with a SAR subject is a business decision; however, regulators increasingly are expecting that AML compliance officers will provide credible challenge to decisions that may not appear to be in the best interest of an institution. In many institutions, this decision is made by a SAR committee or other management committee that includes representation from both AML compliance and the institution's business lines.

329. When a financial institution decides to close an account, should the entire relationship be exited across all business units and subsidiaries?

An AML Program should be managed at an enterprise level. Therefore, if a relationship is exited in one business unit or subsidiary, at a minimum, the customer's related accounts should be examined across the enterprise to determine if they should be subject to enhanced monitoring or closure. The fluid exchange of information across business units and subsidiaries, subject to applicable laws and regulations, can be just as critical in implementing an effective AML Program as information sharing

among financial institutions and law enforcement is in fighting money laundering and terrorist financing nationally and globally.

330. What should a financial institution do if the subject of a previous SAR filing continues to conduct suspicious transactions through the financial institution?

Regulatory agencies have recommended, as a rule of thumb, that repeat SARs be filed at least every 120 days if suspicious transactions continue for the same party, i.e., a review should be conducted every 90 days with a SAR filed as necessary within the 30-day time frame. Subsequent SARs should reference all previous SARs to assist law enforcement with following the investigation trail.

In the case of recurring suspicious activity, it is also important for a financial institution to consider the risks of continuing the business relationship with the subject of the SAR filing. A financial institution may consider the time burden of repeatedly filing SARs, as well as the potential risk of legal enforcement actions related to continuing to service such a customer, and risk to its reputation. As a result, it may consider terminating its relationship with the subject of the SAR filing, especially if suspicious activity continues. The institution may also need to notify law enforcement immediately of current ongoing suspicious activity, as further discussed in the Law Enforcement section.

331. If a financial institution exits a relationship that it deemed to be suspicious but does not file a SAR on reportable suspicious activity, has it failed to meet its SAR filing obligations?

Yes. Exiting a relationship does not absolve a financial institution's obligation to file a SAR if it detected suspicious activity. A SAR still should be filed.

332. Can law enforcement force a financial institution to exit a relationship or, conversely, request that a relationship remain open?

Law enforcement may ask a financial institution to maintain a customer relationship in order to gather more information for an investigation, or so as not to alert the suspect of a potential investigation. However, law enforcement cannot mandate that an account remain open unless there is an appropriate court order. Although unusual, regulators and law enforcement agencies can require accounts to be closed as part of an enforcement action. A financial institution should receive and maintain written records of such requests.

333. For what period should the subject of a SAR be subject to heightened scrutiny?

At a minimum, subjects of SAR filings should be monitored for 90 days to determine if the suspicious activity continues and a subsequent SAR filing is warranted. Financial institutions have taken various stances on extending the monitoring period beyond 90 days. Some financial institutions conduct enhanced scrutiny on subjects of SAR filings for a few years after the date of a SAR filing.

334. What is the difference between an amended SAR and a repeat SAR filing?

An amended SAR corrects a SAR previously submitted to FinCEN. A repeat or follow-up SAR details recurring suspicious activity not included in the previous SAR(s).

Law Enforcement

335. Are there instances in which a financial institution should notify law enforcement in advance of filing a SAR?

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including, but not limited to, ongoing money laundering schemes or detection of terrorist financing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

Additionally, FinCEN has established a hotline, 1.866.556.3974, for financial institutions to report to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States.

336. Does notifying law enforcement of suspicious activity serve as a replacement or in any way relieve a financial institution's obligation to file a SAR?

No. Notifying law enforcement does not remove or in any way affect a financial institution's obligation to file a SAR if it detects suspicious activity.

337. What should a financial institution do upon receipt of a law enforcement inquiry?

It is important that the first step a financial institution takes upon receipt of a law enforcement inquiry is to be diligent about verifying the identity of the requester of the information. The financial institution should obtain a comfort level that the requester is a representative of an appropriate law enforcement or supervisory agency with jurisdiction, such as FinCEN. Verification procedures may include verifying the requester's employment with the requester's local field office or examining the requester's credentials in person. All procedures for verification should be incorporated into the institution's AML/CFT Compliance Program.

No information should be given to any requester prior to validating the requester's authority to request the information. Supporting documentation to a SAR is to be provided promptly upon request by law enforcement with jurisdiction; there is no need for a subpoena. However, all other requests for information must be in compliance with applicable privacy laws. A financial institution should contact its counsel if it is unsure about whether to disclose information to a law enforcement agency or needs any further guidance, and also may choose to discuss the request with its regulator or FinCEN when appropriate. Such requests also may serve as red flags for the financial institution to investigate the accounts or customer for suspicious activity.

338. Is a legal process required for disclosure of SARs or supporting documentation?

No. Financial institutions usually must confirm that disclosure of a customer's financial records to government agencies complies with the Right to Financial Privacy Act and other applicable privacy laws. However, no such requirements apply if the financial institution is providing the financial records/information supporting the SAR to FinCEN or a supervisory agency in the exercise of its "supervisory, regulatory or monetary functions" or to law enforcement with jurisdiction in the United States.

339. What transaction and customer records are financial institutions able to provide to law enforcement agencies in the United States?

Any supporting documentation related to SAR filings, such as copies of the SAR or any supporting documentation, can be given to law enforcement agencies upon their request without any need for a grand jury or other subpoena. However, global institutions should consider privacy regulations in the other countries in which they operate prior to sharing any information about foreign transactions with U.S. law enforcement or regulatory agencies that would come from cross-border offices or vice versa.

Financial institutions should consider performing an analysis of privacy regulations in each country where they operate, and seeking the advice of legal counsel when requests for information require information to be provided to cross-border offices.

It is advisable that any time a financial institution is unsure whether to disclose information to a law enforcement agency, it contact its counsel and/or its primary regulator. It also may want to contact FinCEN for guidance if there is an unusual request for SAR information.

340. Should financial institutions automatically file a SAR upon receipt of law enforcement inquiries?

No. A financial institution should not automatically file a SAR upon receipt of a law enforcement inquiry. The decision to file a SAR should be based on the institution's own investigation into the activity of the party that/who is the subject of the law enforcement inquiry. A law enforcement inquiry may be relevant to a financial institution's overall risk assessment of its customers and accounts.

341. What is a National Security Letter, and should a financial institution file a SAR upon receipt of such a letter?

Pursuant to Section 505 of the USA PATRIOT Act, National Security Letters (NSLs) are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) office and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and internet service providers
- Information from credit bureaus
- Financial records from financial institutions

NSLs are highly confidential. Financial institutions, their officers, employees and agents are precluded from disclosing to any person that a government authority or the FBI has sought or obtained access to records. Financial institutions that receive NSLs must take appropriate measures to ensure the confidentiality of the letters.

A financial institution should not automatically file a Suspicious Activity Report (SAR) upon receipt of an NSL. The decision to file a SAR should be based on the institution's own investigation into the activity of the party(ies) that/who is the subject of the NSL. If a financial institution files a SAR after receiving an NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The

SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the financial institution.

Questions regarding NSLs should be directed to the financial institution's local FBI field office. Contact information for the FBI field offices can be found at www.fbi.gov.

342. If a financial institution decides not to file a SAR and regulatory or law enforcement agencies subsequently investigate the activity and conclude a SAR was warranted, is the financial institution liable?

If a financial institution investigated potentially suspicious activity and decided not to file a SAR as a result of its own internal investigation, the financial institution's best defence will be to have strong documentation supporting this decision. A financial institution can be liable for the failure to file a SAR if the failure was due to an insufficient AML Program, weak due diligence, bad faith or other significant failure.

Thus, it is essential that financial institutions fully document internal investigations whether or not a SAR is filed. In cases where a SAR is not filed, the documentation should support the decision clearly by summarising the reason for not filing and attaching supporting documentation. One way to help ensure investigative files are supportive of the decision to file or not file a SAR is to use an internal suspicious reporting form for the purpose of recording and summarising the outcome of investigations.

This documentation should be retained for a minimum of five years or possibly longer (depending on the state or self-regulatory organisation [SRO]) for the purpose of demonstrating (a) that the financial institution has a strong transaction-monitoring program, and (b) that an investigation of the activity was conducted in a timely manner, and the decision not to file a SAR was fully supported.

343. Has law enforcement provided any feedback on how SARs have helped with the investigation and prosecution of criminal activity?

Yes. FinCEN's *The SAR Activity Review – Trends, Tips & Issues* includes law enforcement investigations that were assisted by SAR information. Additional law enforcement cases can be found on FinCEN's website, www.fincen.gov, in the Law Enforcement link under Law Enforcement Cases Supported by BSA Filings. The Law Enforcement Cases Supported by BSA Filings section on FinCEN's website provides specific cases in which SAR filings assisted law enforcement with initiating, investigating and prosecuting money launderers and terrorist financiers. The section includes archives of specific cases by the following agencies:

- Federal Bureau of Investigation (FBI)
- Bureau of Immigration and Customs Enforcement (ICE)
- Internal Revenue Service – Criminal Investigation (IRS-CI)
- United States Secret Service (USSS)
- State and local law enforcement

SAR Statistics and Trends

344. Is there a target number or quota of SARs a financial institution should file?

No. The number of SAR filings by a financial institution is not necessarily an indicator of the quality of the AML Program. Many factors, including, but not limited to, the products and services a financial institution offers, the size and nature of its client base, and the markets in which it conducts business, will have an impact on the number of SARs filed.

345. Is there data on the number of SAR filings and trends?

Yes. FinCEN periodically issues *SAR Stats* (formerly *By the Numbers*) and *The SAR Activity Review – Trends, Tips & Issues*. SAR Stats, published annually, includes a collection of numerical data on SARs filed by type of financial institution (e.g., depository institution, money services business [MSB], securities, insurance, casinos) as well as Trends, SAR Narrative Spotlights and Sector Highlights. SAR Stats complements *The SAR Activity Review – Trends, Tips & Issues* and serves to provide information about the preparation, use and utility of SARs.

Additionally, FinCEN publishes an index of topics covered in *The SAR Activity Review* publications at www.fincen.gov.

346. Similar to *SAR Stats* analysis conducted by FinCEN, should a financial institution conduct a trend analysis on its own SAR filings?

Although it is not a requirement, conducting a trend analysis on SAR filings can assist in improving the overall AML Program of a financial institution.

Some SAR trends that may be useful include the following:

- Final actions on SARs (e.g., monitor, close/exit relationship)
- Nature of business/occupation of SAR suspect(s)
- Length of relationship with SAR suspect(s)
- SARs by branch(es)/line(s) of business
- SARs by jurisdiction

The better a financial institution understands the risks it faces, the more effective it can be in implementing controls to address these risks.

347. Has any feedback been provided on the quality of SARs filed?

Yes. FinCEN's "Suggestions for Addressing Common Errors Noted in Suspicious Activity Reporting," published in October 2007, outlines the most common errors found in SAR filings and ways in which these errors can be addressed. The most common errors found are as follows:

- Empty narrative fields
- Failure to explain information in supporting documents

- Inadequate narratives
- Inaccurate special responses
- Missing filer telephone number
- Missing, incomplete or invalid SSN or Employer Identification Number (EIN)
- Incomplete subject information; government-issued identification
- Missing category, type or characterisation of suspicious activity
- Incorrect characterisation of suspicious activity

Many of these errors have been addressed by mandatory, dynamic and interactive fields of the BSA E-Filing System.

348. What are some of the statistics and trends in SAR filings?

According to FinCEN, some of the statistics and trends of SAR filings include, but are not limited to, the following:

- The number of SAR filings increased from approximately 94,000 in 2012 to 1.98 million in 2016; 93 percent of the 6.8 million SARs during this five year period were filed by depository institutions and money services businesses (MSBs).
- There were 1.98 million SAR filings from January 1, 2016, through December 31, 2016, which were distributed as follows:
    - **Depository institutions** (e.g., banks, thrifts, savings and loans, credit unions) filed approximately 960,000 or 49 percent of all SARS filed during this period:
        - Forty-nine percent of SARs were filed on activity taking place in California, New York, Texas, Ohio, Delaware and Florida, and 19 states accounted for 80 percent of the SAR filings by depository institutions;
        - Fifty-eight percent of SARs were filed on customers, 26 percent on individuals with no relationship with the depository institution, 7 percent with a relationship of "other," 5 percent with unknown/blank or other relationship type, and 2 percent on borrowers;
        - Forty-six percent of SARs involved U.S. currency, 23 percent involved debit cards, 7 percent involved bank/cashier's checks, 21 percent involved credit cards, 21 percent involved personal/business checks, 20 percent involved funds transfers, 5 percent involved prepaid access, and 4 percent involved residential mortgages;
        - Top suspicious activity categories of SARs filed by depository institutions included:
            - Other Suspicious Activities: 32 percent included more than 110,000 cases related to identity theft, more than 20,000 cases related to elder financial

exploitation, more than 4,000 cases related to electronic intrusion, and 1,157 cases related to suspected corruption [foreign and domestic]);

- Money Laundering: 29 percent;
- Structuring: 13 percent;
- Fraud: 18 percent (separate from Mortgage Fraud, which accounted for less than 1 percent); and
- Terrorism/Terrorist Financing: 0.03 percent (778 cases).

– **Money services businesses (MSBs)** filed more than 870,000 SARs or 44 percent of all filings:

- Fifty-one percent of SARs were filed on activity taking place in California, New York, Texas, Florida, North Carolina, Virginia, Colorado and Georgia, while approximately 8 percent of SARs came from an unknown/blank state;
- Thirty-nine percent of SARs were filed on customers, 27 percent on "other" relationship types, 24 percent on unknown/blank relationship types and 11 percent on individuals with no relationship with the MSB;
- Forty-eight percent of SARs involved funds transfers, 23 percent involved U.S. currency, 22 percent involved money orders and 11 percent involved prepaid access;
- Top suspicious activity categories of SARs filed by MSBs included:
  - Structuring: 31 percent;
  - Other Suspicious Activities: 40 percent (included nearly 198,000 cases related to "suspicious use of multiple locations," more than 21,000 cases related to identity theft, nearly 30,000 cases related to elder financial exploitation, 459 cases related to unauthorised electronic intrusion, and 154 cases related to suspected corruption [foreign and domestic]);
  - Money Laundering: 8 percent;
  - Fraud: 15 percent (separate from Mortgage Fraud which accounted for less than 0.01 percent); and
  - Terrorism/Terrorist Financing: 0.06 percent (1,074 cases).

– **Casino and Card Clubs** filed more than 57,000 SARs or 3 percent of all filings during this period; 71 percent were filed by state-licensed casinos, 24 percent by tribal-licensed casinos and 4 percent by card clubs:

- Fifty percent of SARs were filed on activity taking place in Nevada, Louisiana, California and Oklahoma;

- Ninety percent of SARs were filed on customers, 7 percent on unknown/blank relationship types, 1 percent on agents and 1 percent on individuals with no relationship with the casino or card club;
- Forty-eight percent of SARs involved gaming instruments, 41 percent involved U.S. currency, 5 percent involved "other" instrument types and 2 percent involved funds transfers;
- Top suspicious activity categories of SARs filed by casinos and card clubs included:
  - Structuring: 36 percent;
  - Casinos: 26 percent (including more than 10,500 cases related to "minimal gaming with large transactions" and more than 1,200 cases related to "suspicious intra-casino funds transfers" and "suspicious use of counter checks or markers");
  - Money Laundering: 13 percent;
  - Other Suspicious Activities: 12 percent (included more than 5,000 cases related to "two or more individuals working together," more than 2,100 cases related to "transaction with no apparent economic, business or lawful purpose," nearly 1,000 cases related to counterfeit instruments, 66 cases related to suspected corruption [foreign and domestic] and 11 cases related to elder financial exploitation);
  - Identification Documentation: 11 percent (included more than 9,600 cases related to questionable or false documentation, refusal to provide documentation, single individual with multiple identities, multiple individuals with same or similar identities; separate from identity theft, which accounted for less than 0.4 percent of SARs filed by casinos and card clubs); and
  - Terrorism/Terrorist Financing: 0.07 percent (61 cases).

– **Securities and Futures Firms** (e.g., clearing brokers [securities], introducing brokers [securities], introducing brokers [commodities], futures commission merchants, investment companies, investment advisers, retail foreign exchange dealers, holding companies, subsidiaries of holding companies) filed nearly 19,000 SARs or 1 percent of all filings during this period:

- Sixteen percent of SARs were filed on activity taking place in California, 12 percent in Massachusetts, 11 percent in New York, and 10 percent in Rhode Island;
- Ninety percent of SARs were filed on customers, 7 percent on unknown/blank relationship types, and 1 percent on individuals with no relationship with the securities and futures firm;

- Fifty-eight percent of SARs involved funds transfers; 34 percent involved stocks; 24 percent involved personal/business checks; 16 percent involved mutual funds; 15 percent involved penny stocks/microcap securities; and 5 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by securities and futures firms:
  - Other Suspicious Activities: 42 percent (included more than 5,000 cases related to identity theft; nearly 2,700 cases related to account takeover; over 2,600 cases related to embezzlement/theft/disappearance of funds; over 1,100 cases related to unauthorised electronic intrusion; over 1,400 cases related to elder financial exploitation; and 147 cases related to corruption [foreign and domestic]);
  - Fraud: 30 percent (included more than 11,800 cases related to wire transfer, ACH and check fraud) (separate from Mortgage Fraud which accounted for less than 0.1 percent);
  - Securities/Futures/Options: 8 percent (included more than 1,300 cases related to insider trading and over 1,200 cases related to market manipulation/wash trading);
  - Money Laundering: 13 percent; and
  - Terrorism/Terrorist Financing: 0.04 percent (19 cases).

– **Insurance Companies** filed nearly 2,400 SARs or 0.1 percent of all filings during this period:

- Forty-six percent of SARs were filed on activity taking place in New York and Ohio; 42 states (and territories) filed fewer than 10 SARs; 19 did not file SARs;
- Sixty-two percent of SARs were filed on customers; 14 percent on individuals with no relationship with the insurance company; 11 percent on "other" relationship types; 6 percent were filed on unknown/blank relationship types; and 5 percent on agents;
- Ninety-five percent of SARs involved insurance/annuity products; 37 percent involved money orders; 30 percent involved personal/business checks; 19 percent involved funds transfers; 6 percent involved bank/cashier's checks; and 5 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by insurance companies:
  - Other Suspicious Activities: 40 percent (involved nearly 700 cases related to "transaction with no apparent economic, business or lawful purpose" and "little or no concern for product performance penalties, fees or tax consequences"; over 170 cases related to identity theft; over 200 cases

related to elder financial abuse; 32 cases related to unauthorised electronic intrusion; and 11 cases related to corruption [domestic and foreign]);

- Money Laundering: 24 percent;
- Structuring: 18 percent;
- Insurance: 8 percent (included more than 430 cases related to "excessive insurance," "excessive or unusual cash borrowing against policy/annuity," "proceeds related to unrelated third party," "suspicious life settlement sales insurance," "suspicious termination of policy or contract" and "unclear or no insurable interest");
- Fraud: 7 percent (separate from Mortgage Fraud which accounted for less than 0.1 percent); and
- Terrorism/Terrorist Financing: Less than 0.1 percent (4 cases).

– **Nonbank Residential Mortgage Lenders and Originators (RMLOs)/Loan or Finance Companies** filed more than 3,000 SARs or 0.2 percent of all filings during this period:

- Nearly 80 percent of SARs were filed on activity taking place in Michigan, Texas and California;
- Fifty percent of SARs were filed on the "unknown/blank" relationship type, 23 percent on borrowers, 16 percent on individuals with no relationship to the loan or finance company, 7 percent on customers and 2 percent on individuals with "other" relationship type;
- Ninety-eight percent of SARs involved residential mortgages, 27 percent involved personal/business checks, 22 percent involved funds transfers, 20 percent involved bank/cashier's checks and 8 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by loan or finance companies included:
  - Mortgage Fraud: 35 percent;
  - Fraud: 32 percent (included nearly 300 cases on consumer loan fraud and over 100 cases of check fraud);
  - Structuring: 1 percent;
  - Money Laundering: 3 percent;
  - Other Suspicious Activities: 16 percent (included nearly 270 cases related to forgeries, over 230 cases related to "two or more individuals working together," over 130 cases related to counterfeit instruments, 33 cases related to elder financial exploitation), 24 cases related to suspected corruption (foreign and domestic), and 15 cases related to unauthorised electronic intrusion;

- Identification Documentation: 12 percent (included more than 600 cases related to questionable or false documentation and refusal to provide documentation, separate from identity theft, which accounted for less than 0.3 percent of SARs filed by loan or finance companies); and
- Terrorism/Terrorist Financing: 0.01 percent (1 cases).

– **Housing Government Sponsored Entities (GSEs)** filed nearly 2,300 SARs or 0.1 percent of all filings during this period:

- Eighty percent of SARs were filed on activity taking place in the District of Columbia;
- Forty-five percent of SARs were filed on borrowers, 26 percent on individuals with unknown/blank relationship type, 24 percent with a relationship of "other," and 2 percent on agents;
- Ninety-nine percent of SARs involved residential mortgages, 43 percent involved funds transfers, 20 percent involved personal/business checks, 17 percent involved money orders, 13 percent involved bank/cashier's check, and 7 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by housing GSEs included:
  - Mortgage Fraud: 84 percent;
  - Money Laundering: 8 percent;
  - Other Suspicious Activities: 5 percent (included 22 cases related to identity theft, and 3 cases related to unauthorised electronic intrusion);
  - Fraud: 2 percent (separate from Mortgage Fraud which accounted for less than 84 percent of SARs filed by housing GSEs);
  - Structuring: 1 percent; and
  - Terrorism/Terrorist Financing: 0 percent (0 cases).

– "**Other**" types of financial institutions (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily) filed nearly 63,000 SARs or 3 percent of all filings during this period:

- Nearly 60 percent of SARs were filed in Utah, Michigan and Delaware;
- Forty percent of SARs were filed on customers, 21 percent on individuals with no relationship with the institution, 21 percent with other relationship type, and 11 percent with unknown/blank relationship type;
- Fifty-one percent of SARs involved credit cards; 50 percent involved funds transfers; 22 percent involved U.S. currency; 12 percent involved personal/business checks; 10 percent involved residential mortgages; 6

percent involved money orders; and 4 percent involved bank/cashier's checks;

- Top suspicious activity categories of SARs filed by "other" financial institution types:
  - Other Suspicious Activities: 35 percent (included more than 13,400 cases related to identity theft; over 4,000 cases related to account takeover; over 3,800 cases related to "two or more individuals working together"; over 900 cases related to elder financial abuse; 142 cases related to unauthorised electronic intrusion and 112 cases related to corruption [domestic and foreign]);
  - Fraud: 28 percent (included more than 16,000 cases related to credit/debit cards; over 10,000 cases related to consumer loans; nearly 1,200 cases related to wire transfers, independent of Mortgage Fraud, which accounted for 2 percent of SARs filed by "other" types of financial institutions);
  - Money Laundering: 17 percent;
  - Structuring: 6 percent; and
  - Terrorism/Terrorist Financing: 0.04 percent (57 cases).

Report of Foreign Bank and Financial Accounts

FBAR Basics

349. What is a Report of Foreign Bank and Financial Accounts?

Report of Foreign Bank and Financial Accounts (FBAR), FinCEN Form 114, is a report that must be filed by a U.S. person who has a financial interest in, or signature or other authority over, any foreign financial accounts, including bank, securities or other financial accounts in a foreign country, which have a maximum value exceeding US$10,000 (alone or in aggregate) at any time during a calendar year. Beginning in 2016, the report must be filed with the U.S. Department of the Treasury on or before April 15 of the following calendar year. Previously, the FBAR was due on June 30.

The FBAR requirement is implemented under regulation 31 C.F.R. 1010.350 – Reports of Foreign Financial Accounts.

350. What is the benefit of information reported on the FBAR to law enforcement?

Similar to other reporting mandated under the Bank Secrecy Act (BSA), the FBAR assists law enforcement in the detection of schemes by U.S. persons involving tax evasion, money laundering, terrorist financing or other criminal activities. The FBAR also assists with tax collection and other regulatory matters.

351. What does the term "U.S. person" mean for FBAR filing purposes?

A "U.S. person" includes a U.S. citizen, a U.S. resident for tax purposes and legal entities (including, but not limited to, corporations, partnerships, limited liability companies, trusts and estates) organised in the United States or under the laws of the United States, any state, the District of Columbia, the territories and insular possessions of the United States, or Indian Tribes. In addition, a limited liability company that is a disregarded entity for U.S. federal income tax purposes is still required to file an FBAR.

A U.S. resident for tax purposes includes an alien individual who has a permanent resident visa (i.e., "green card") or who meets a substantial presence test (e.g., generally, any alien who is present in the United States for 183 days or more in the current year, or who has been present for a weighted average of 183 days over the current year and the two preceding years, will be treated as a U.S. resident).

352. Do FBAR filing requirements apply to non-U.S. persons "in and doing business in the United States"?

No. Although the FBAR instructions issued in 2008 created uncertainty on this point, the final FBAR rules clarify that non-U.S. persons "in and doing business in the United States" are not subject to the FBAR filing requirement. However, another federal law that was enacted, the Foreign Account Tax Compliance Act (FATCA), requires foreign financial institutions to report directly to the Internal Revenue Service (IRS) information about financial accounts held by U.S. taxpayers, or held by foreign entities in which U.S. taxpayers hold a substantial ownership interest. For further guidance, please refer to the Foreign Account Tax Compliance Act section.

353. Are foreign financial accounts of U.S. financial institutions required to be reported on FBARs?

An FBAR is required if an officer or employee of a regulated U.S. financial institution with signature or other authority has a personal financial interest in a foreign financial account valued in excess of US$10,000. A U.S. financial institution also may be required to file an FBAR if the financial institution maintains customer accounts in which the financial institution has a financial interest, or the financial institution has signature or other authority.

354. What does the term "foreign country" mean for FBAR filing purposes?

The term "foreign country" includes all geographical areas outside of the United States. For purposes of this requirement, the United States includes the states; the District of Columbia; the Commonwealth of Puerto Rico; the Commonwealth of the Northern Mariana Islands; U.S. territories and possessions, including Guam, American Samoa and the U.S. Virgin Islands; and Indian lands, as defined in the Indian Gaming Regulatory Act.

355. What does the term "financial interest" mean for FBAR filing purposes?

The term "financial interest" in a bank, securities or other financial account in a foreign country means an interest as described below:

- A U.S. person has a financial interest in each account for which such person is the owner of record or has legal title, regardless of whether the account is maintained for the U.S. person's own benefit or for the benefit of others, including non-U.S. persons.
- A U.S. person has a financial interest in each bank, securities or other financial account (including credit and debit cards) in a foreign country for which the owner of record or holder of legal title is:
  - A person acting as an agent nominee, attorney, or in some other capacity on behalf of the U.S. person with respect to the account;
  - A corporation in which the U.S. person owns directly or indirectly more than 50 percent of the total value of shares of stock or more than 50 percent of the voting power of all shares of stock;
  - A partnership in which the U.S. person owns an interest in more than 50 percent of the profits (distributive share of income) or an interest in more than 50 percent of the partnership capital;
  - A trust of which the U.S. person is the trust grantor and has an ownership interest in the trust for U.S. federal tax purposes;
  - A trust in which the U.S. person either has a present beneficial interest in more than 50 percent of the assets or from which such person receives more than 50 percent of the current income; or
  - Any other entity in which the U.S. person owns directly or indirectly more than 50 percent of the voting power, total value of equity interests or assets, or interest in profits.

356. What constitutes "signature or other authority" over an account for FBAR filing purposes?

"Signature or other authority" is defined as "the authority of an individual (alone or in conjunction with another individual) to control the disposition of assets held in a foreign financial account by direct communication (whether in writing or otherwise) to the bank or other financial institution that maintains the financial account."

357. Why are both persons with "financial interest" and "signature or other authority" required to file FBARs on the same foreign financial accounts?

Although some reporting may be duplicative, law enforcement has indicated that FBARs filed by persons with only signature or other authority are useful in investigations as they often provide additional information (e.g., different individuals with access to the account), especially if the person with financial interest fails to file an FBAR.

358. What does the term "financial account" mean for FBAR filing purposes?

The term "financial account" includes any bank, securities brokerage, securities derivatives or other financial instruments account. Usually, such accounts also include accounts in which the assets are

held in a commingled account, and the account owner holds an equity interest in the fund (such as a mutual fund, unless another filing exception applies). Bank accounts include any savings, demand, checking, deposit, time deposit or any other account (including debit card and prepaid credit card accounts) maintained with a financial institution or other person engaged in the business of a financial institution. A financial account also includes any commodity futures or options account, an insurance policy with a cash value, and shares in a mutual fund or similar pooled fund. Individual bonds, notes or stock certificates held by the filer do not qualify as a financial account, nor does an unsecured loan to a foreign trade or business that is not a financial institution.

359. Are accounts held in international offices of U.S. banks exempted from FBAR filing requirements?

The geographical location of a financial account, not the nationality of the financial entity institution in which the account is found, determines whether it is an account in a foreign country. With the exception of a financial account held in a financial institution that is a U.S. military banking facility, any financial account that is located in a foreign country, even if it is held at an affiliate of a U.S. bank or other institution, is to be reported. A financial account maintained with a branch, agency or other office of a foreign bank or other institution that is located in the United States is not to be reported.

360. If an account (e.g., securities, pension fund) contains holdings or assets of foreign entities, is it included within the definition of "foreign bank and financial account" for FBAR filing purposes?

The foreign status of the holdings or assets does not render the account "foreign" for FBAR filing purposes. If the account is maintained at a U.S. financial institution, it does not need to be reported on an FBAR.

361. If a custodian holds assets for investors in an omnibus account at a foreign financial institution, is it included within the definition of "foreign bank and financial account" for FBAR filing purposes?

Yes; however, the type of custodial arrangement will dictate which parties will be responsible for filing the FBAR on the foreign bank and financial account. If investors have direct access to the foreign holdings in the foreign omnibus account, the customer(s) and the custodial financial institution are required to file an FBAR if the maximum value exceeds US$10,000.

362. Are there exceptions to the FBAR filing requirement?

Yes. FBARs are not required to be filed by the following:

- The spouse of an individual who has filed an FBAR if all reportable financial accounts are jointly owned with the filing spouse, the FBAR is filed in a timely manner and both spouses sign the FBAR (or the spouse authorises the other to file on their behalf though a Record of Authorisation to Electronically File FBARs [Form 114a]).
- An entity that is named in a consolidated FBAR filed by its owner (an entity that has a greater than 50 percent ownership stake).

- A governmental entity of the United States (e.g., a college or university that is an agency of, an instrumentality of, owned by, or operated by a governmental entity, or an employee retirement or welfare benefit plan of a governmental entity).
- The owner or beneficiary of an IRA with respect to foreign accounts held in the IRA.
- A participant in or beneficiary of a tax-qualified retirement plan described in Internal Revenue Code sections 401(a), 403(a) or 403(b) with respect to the foreign accounts held by or on behalf of the retirement plan.
- A trust beneficiary with greater than 50 percent present beneficial interest with respect to the trust's foreign financial accounts if the trust or the trustee of the trust is a U.S. person and files an FBAR on behalf of the trust disclosing the trust's foreign financial accounts.
- Correspondent or nostro accounts maintained by banks for the sole purpose of bank-to-bank settlements.
- Foreign financial accounts of any international financial institution if the U.S. government is a member.
- Financial accounts maintained with U.S. military banking facilities, defined as banking facilities operated by a U.S. financial institution designated by the U.S. government to serve U.S. government installations abroad, even if the military banking facility is located in a foreign country.
- Officers or employees who have signature or other authority over, but no personal financial interest, in a foreign financial account maintained by their employer are not required to file FBARs on foreign financial accounts maintained by the following:
    - Financial institutions that are subject to supervision by the Office of the Comptroller of the Currency (OCC), Federal Reserve Bank (FRB), Federal Deposit Insurance Corporation (FDIC) or the National Credit Union Administration (NCUA)
    - Financial institutions that are registered with and examined by the U.S. Securities and Exchange Commission (SEC) or Commodity Futures Trading Commission (CFTC)
    - Entities that are registered with and examined by the SEC that provide services to an investment company registered under the Investment Company Act of 1940, also known as Authorised Service Providers
    - Entities that have a class of equity securities listed (or American depository receipts [ADR] listed) on any U.S. national securities exchange
    - U.S. subsidiaries of U.S. parent companies that have a class of equity securities listed on any U.S. national securities exchange, and the subsidiaries are included in a consolidated FBAR report of the U.S. parent companies

- Entities that have a class of equity securities registered (or American depository receipts in respect of equity securities registered) under section 12(g) of the Securities Exchange Act

Additionally, a U.S. person may also be eligible for modified FBAR reporting if he/she:

- Resides outside of the United States;
- Is an officer or employee of an employer located outside the United States; or
- Has signature authority over the employer's foreign financial account(s) but no financial interest.

363. What information do U.S. persons who are eligible to file modified FBARs need to provide?

U.S. persons eligible for modified FBAR filings are required to complete the following sections on an FBAR:

- Part I – Filer information; and
- Part IV: Items 34-43 – Account owner information (e.g., name, tax identification number [TIN], address, title of filer).
- If filing for multiple accounts, Part IV need only be completed one time with information about the filer's employer.
- Part II – Information on Financial Accounts is not required to be completed by the filer, except the number of accounts. Records of the information should be maintained by the filer.

364. Are tax-exempt organisations absolved from the FBAR filing requirement?

No. Status as tax-exempt does not obviate an organisation's requirement to file an FBAR for covered accounts. FBARs are used to detect criminal activity in addition to assisting in tax-related matters.

365. How will FinCEN's Notice of Proposed Rulemaking on FBARs impact current requirements?

FinCEN issued a Notice of Proposed Rulemaking on FBARs in March 2016 that would make the following adjustments to the FBAR requirement:

- Eliminate the special rule for filers with 25 or more foreign financial accounts by requiring all U.S. persons to file FBARs on all eligible accounts;
- Eliminate the FBAR filing requirement that officers and employees of institutions for which they have signature authority, but not financial interest, if the employing financial institution has filed FBARs on eligible accounts; and
- Require financial institutions to maintain a list of all officers and employees with signature authority over eligible accounts that can be made available to FinCEN and law enforcement upon request.

366. Does the filing requirement under the Foreign Account Tax Compliance Act (FATCA) obviate the need to file an FBAR?

No. The reporting thresholds for Internal Revenue Form 8938 – Statement of Specified Foreign Financial Assets under FATCA and FBARs are different. Filers may be required to file one or both. Key differences include, but are not limited to, the following:

- Reporting thresholds
- Due dates
- Definition of "interest" in an account or asset
- Types of reportable foreign assets
- Valuation of reportable foreign assets

For further guidance on FATCA, please refer to the Foreign Account Tax Compliance Act section.

367. What key guidance has been issued related to FBARs?

The following are examples of key guidance that has been issued related to FBARs:

- **FBAR Filing for Individuals Made Easier** (2014) by FinCEN
- **BSA Electronic Filing Requirements for Report of Foreign Bank and Financial Accounts (FinCEN Report 114)** (2013) by FinCEN
- **FinCEN Introduces New Form for Authorizing FBAR Filings by Spouses and Third Parties** (2013) by FinCEN
- **Foreign Bank and Financial Accounts Report (FBAR) Responsibilities** (2011) by FinCEN
- **Guidance on Reports of Foreign Financial Accounts (FBARs) Requirements for Former Employees** (2011) by FinCEN
- **Comparison of Form 8938 and FBAR Requirements** (2012) by the Internal Revenue Service (IRS)

Completing the FBAR and Third-Party Authorisation

368. Can an FBAR be filed by a third party on behalf of the person subject to the FBAR filing requirement?

Yes. A Record of Authorisation to Electronically File FBARs (Form 114a) must be completed and signed by both the account owner and the preparer who is authorised to file the FBAR on behalf of the account owner. The third party (e.g., preparer) must be registered on the BSA E-Filing System to file FBARs electronically.

369. Who is required to retain copies of Form 114a, the account owner or the preparer?

Both the account owner and the preparer are required to retain copies of Form 114a for 5 years. Form 114a should not be sent to FinCEN but be retained and made available upon request.

370. Can Form 114a be used to authorise one's spouse to file an FBAR on jointly held accounts?

Yes. In that instance, Form 114a should be completed by both spouses and retained for 5 years.

371. Can a corporation file one FBAR for all of its foreign financial interests and on behalf of its subsidiaries?

Yes. A corporation that owns, directly or indirectly, more than a 50 percent interest in one or more other entities is permitted to file a consolidated FBAR form on behalf of itself and such other entities provided that the listing of those subsidiaries is made part of the consolidated report. An authorised official of the parent corporation should sign such consolidated reports.

372. Are there special rules for FBARs when a filer has an interest or signatory or other authority over multiple foreign financial accounts?

Yes. Filers with a financial interest in or signature or other authority over 25 or more foreign financial accounts need only provide the number of accounts on the FBAR and be prepared to provide further details upon request by government authorities. According to proposed rules by FinCEN this special rule will be eliminated. All U.S. persons will be required to file FBARs on all foreign financial accounts for which they are required to file an FBAR.

373. What does the term "maximum value of account" mean for FBAR filing purposes?

The term "maximum value of account" means a reasonable approximation of the greatest value of the account during the calendar year. Periodic account statements may be relied on to determine the maximum value, provided that the periodic account statements fairly reflect the maximum account value during the calendar year. If periodic account statements are not issued, the maximum account value is the largest amount of currency and nonmonetary assets in the account at any time during the year.

In the case of non-U.S. currency, the maximum account value for each account must be determined by converting the foreign currency into U.S. dollars using the U.S. Treasury's Financial Management Service rate from the last day of the calendar year or, if not available, another verifiable exchange. The value of stock, other securities or other nonmonetary assets in an account is the fair market value at the end of the calendar year. If the asset was withdrawn from the account, the value is the fair market value at the time of the withdrawal.

374. Should the maximum value of the account be reported in U.S. currency or the currency of the country in which the foreign account is held?

The maximum value of the account should be reported in U.S. currency and rounded up to the next whole dollar.

375. What exchange rate should be used to convert the foreign currency to U.S. currency?

The IRS requires using the official exchange rate at the end of the applicable year to convert the foreign currency to U.S. currency.

376. Is an FBAR required if the foreign account did not generate interest or dividend income?

Yes. An FBAR is required regardless of whether the foreign account generated income.

377. Who is responsible for filing an FBAR on eligible accounts of a child?

Generally, the child is responsible, however, the parents or legal guardian of the child can file the FBAR if, for any reason (e.g., age), the child cannot.

Filing of FBARs

378. What is the time frame for filing the FBAR?

For each calendar year, the FBAR must be filed with the IRS on or before April 15 of the following calendar year.

379. What should filers do if they cannot submit an FBAR by April 15?

Filers should submit an FBAR as soon as possible and provide an explanation for the late filing. If the reason for the late filing is due to a natural disaster or other emergency situation, filers should contact FinCEN's Regulatory Helpline at 800.949.2732 (for U.S. callers) or 703.905.3975 (for callers outside the U.S.). Filers may also request an exception to e-filing by sending an email to frc@fincen.gov. Additional questions can be sent to BSAEFilingHelp@fincen.gov or the E-File Help Line at 866.346.9478.

380. Who is required to file FBARs on foreign financial accounts of U.S. financial institutions?

Currently, officers and employees with signature authority, but no financial interest, are required to file FBARs on eligible accounts. According to proposed rules by FinCEN this requirement will be eliminated if the financial institutions have filed FBARs on eligible accounts.

381. Can FBARs be filed with the filer's federal income tax return?

No. FBARs and federal tax returns should be filed separately.

382. Do extensions of time to file federal income tax returns extend to FBARs?

No. However, reporting guidelines separate from federal income tax reporting allow for certain FBAR filing extensions.

383. How should FBARs be submitted to the IRS?

FBARs can be mailed or filed electronically through the BSA Direct E-Filing System. Unlike other BSA Reports, FBARs are not required to be filed electronically.

384. How can financial institutions file corrected or amended FBARs through the BSA E-Filing System?

Financial institutions can file amended or corrected FBARs by entering the Document Control Number (DCN)/BSA Identifier (ID) of the previous FBAR and selecting the "Amend" box in the BSA E-Filing System. The DCN/BSA ID can be retrieved from the acknowledgement received by the filer after successful submission and acceptance of the previous FBAR filing.

385. How long must FBARs be retained?

FBARs must be retained for a minimum of five years from the date of filing.

386. Since filers submit FBARs to FinCEN through the BSA E-Filing System, are they still required to retain copies in accordance with AML/CFT laws and regulations?

Yes. The BSA E-Filing System is not a recordkeeping program. Filers are required to retain FBARs for a minimum of five years from the date of filing in accordance with AML/CFT laws and regulations.

387. Are financial institutions required to retain records beyond filed FBARs?

According to a proposed rule issued in March 2016 by FinCEN, financial institutions will be required to maintain a list of all officers and employees with signature authority over eligible accounts that can be made available to FinCEN and law enforcement upon request.

388. What are the consequences for failing to file an FBAR in a timely manner?

Failure to file an FBAR may result in both civil and/or criminal penalties. Wilful violations may also be subject to additional criminal penalties. In some instances, the IRS has the discretion to decrease or terminate penalties as it deems appropriate. In the event an individual or institution discovers that he/she or it has failed to file an FBAR, a delinquent FBAR should be submitted, and a statement attached explaining why the FBAR is being filed late. It is possible for cumulative FBAR penalties to exceed the balance in the foreign financial account.

For first-time filers, recent legislation allows for potential relief. Potential penalties may be waived.

Recent Tax Scandals

389. What are some examples of tax scandals?

Some high-profile tax scandals have highlighted the use of non-reported foreign accounts by U.S. taxpayers. Congressional testimony reported widespread use of accounts held in foreign financial facilities located in certain foreign jurisdictions for the purpose of violating U.S. law. Secret foreign bank accounts held at foreign financial institutions allegedly permitted proliferation of white-collar crimes, and were used by U.S. citizens and others to evade income taxes, illegally conceal assets,

purchase gold, and avoid security laws and regulations. Such foreign bank accounts allegedly have been used to facilitate fraud schemes, serve as sources of questionable financing for certain stock and merger activity, and allegedly facilitate conspiracies to steal from the U.S. defence and foreign aid funds, as well as commit money laundering.

Additional tax-related cases include, but are not limited to, the following:

- In February 2016, the DOJ filed a deferred prosecution agreement against Swiss bank Julius Baer requiring payment of US$547 million for conspiracy to defraud the IRS, file false federal income tax returns and evade federal income taxes. Julius Baer assisted U.S. taxpayers in hiding assets in offshore accounts and in evading U.S. taxes on income earned in those accounts. Additionally, two Julius Baer client advisers plead guilty to felony tax charges for their role in these criminal acts and faced a maximum sentence of five years in prison. To help U.S. taxpayers hide assets, the advisers took the following types of actions:
  - Held U.S. taxpayers' assets in undeclared accounts managed by third-party asset managers;
  - Utilised "code word arrangements" to avoid identifying U.S. taxpayers by name;
  - Opened and maintained accounts in the name of various structures (e.g., foundations, trusts) or non-U.S. relatives to conceal the beneficial ownership of the accounts of U.S. taxpayers.

  Julius Baer earned approximately US$87 million in profits on nearly 2,600 undeclared accounts between 2001 and 2011 but had helped U.S. taxpayers evade their U.S. tax obligations from at least the 1990s. In 2008, Julius Baer began exiting relationships on U.S. taxpayer accounts that lacked evidence of U.S. tax compliance. In 2009, Julius Baer decided to voluntarily approach U.S. law enforcement authorities regarding its conduct related to U.S. taxpayers but ultimately did not self-report at the request of its Swiss regulator.
- In April 2016, over 11.5 million documents (Panama Papers) from Mossack Fonseca (MF), a Panama-based law firm specialising in the formation and management of entities in tax havens, were leaked by an anonymous source, identifying the beneficial owners of 214,000 offshore entities, according to the International Consortium of Investigative Journalists (ICIJ). In September 2016, the same source that leaked the Panama Papers also leaked information from the Bahamas corporate registry, linking approximately 140 international and local politicians to offshore companies in the Bahamas. The ICIJ published the leaked information in its Offshore Leaks Database. According to media reports, in February 2017, the two founders of Mossack Fonseca were arrested for their alleged involvement in a separate money laundering investigation involving corruption in Latin America. These leaks had corruption, tax evasion and cybersecurity implications. For further guidance, please refer to the sections: Corruption, Anti-Bribery and Corruption Compliance Programs and Cyber Events and Cybersecurity.

390. Given the likelihood that there are a substantial number of unreported foreign accounts, has the U.S. government taken any specific steps to encourage reporting?

The IRS still encourages voluntary disclosure and considers it a factor when determining whether to recommend criminal proceedings to the U.S. Department of Justice. For example, the Offshore Voluntary Disclosure Program (OVDP), which was initiated in January 2012, is a VTC program administered by the IRS for U.S. taxpayers to resolve their civil tax and penalty obligations as a path to avoid criminal liability. The OVDP is designed specifically for taxpayers facing potential criminal liability and/or substantial civil penalties for the wilful failure to report foreign financial assets and pay tax liabilities on those assets. The OVDP is a continuation of past similar programs of the IRS (e.g., Offshore Voluntary Disclosure Initiative [OVDI] from 2011).

For further guidance, please refer to the Offshore Tax Evasion, Voluntary Tax Compliance and Foreign Account Tax Compliance Act section.

Report of International Transportation of Currency or Monetary Instruments

CMIR Basics

391. What is the Report of International Transportation of Currency or Monetary Instruments?

The Report of International Transportation of Currency or Monetary Instruments (CMIR) is required to be filed by:

- Each person who physically transports, mails or ships, or causes (or attempts to cause) to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States
- Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding US$10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States

CMIR requirements are implemented under regulation 31 C.F.R. 1010.340 – Reports of Transportation of Currency or Monetary Instruments.

392. What is the benefit of the CMIR to law enforcement?

The CMIR is useful to law enforcement because it can be used to trace the international transportation of currency or monetary instruments which can aid in detecting underlying criminal activity (e.g., drug trafficking, human trafficking, bulk cash smuggling).

393. What does the term "persons" mean for CMIR filing purposes?

Persons are one of the following: an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, a joint venture or other unincorporated organisation or

group, an Indian Tribe (as that term is defined in the Indian Gaming Regulatory Act), and all entities perceived as legal personalities.

394. What does the term "currency" mean for CMIR filing purposes?

Currency is defined by the BSA as the coin and paper money of the United States or any other country that is:

- Designated as legal tender;
- Circulates; and
- Is customarily accepted as a medium of exchange in the country of issuance.

395. What does the term "monetary instrument" mean for CMIR filing purposes?

Monetary instruments are defined by the BSA as follows:

- Coin or currency of the United States or of any other country;
- Traveller's checks in any form;
- Negotiable instruments (e.g., checks, promissory notes, money orders) in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery;
- Incomplete instruments (including checks, promissory notes, and money orders) that are signed but on which the name of the payee has been omitted; and
- Securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery.

Monetary instruments do not include:

- Checks or money orders made payable to the order of a named person which have not been endorsed or which bear restrictive endorsements;
- Warehouse receipts; or
- Bills of lading.

396. What does "cause or attempts to cause the physical transportation of currency or monetary instruments" mean for CMIR purposes?

A person is deemed to have caused such transportation, mailing or shipping when the person "aids, abets, counsels, commands, procures, or requests it to be done by a financial institution or any other person."

397. Who is obligated to file a CMIR, the transporter or the recipient of the currency and monetary instruments?

Although only one CMIR is required of a particular transportation, mailing, or shipping of currency or the monetary instruments, multiple parties involved in the cross-border physical transportation of

currency or monetary instruments in excess of US$10,000 may need to file as no person otherwise required to file a report is excused from liability for failure to do so, if in fact, a complete and truthful report has not been filed by another party.

The obligation to file the CMIR is on the person who transports, mails, ships or receives, or causes or attempts to transport, mail, ship or receive.

These parties include:

- The **originator** who transports, mails or ships or caused to be physically transported, mailed or shipped the currency or monetary instruments (e.g., individuals or businesses that have an aggregate amount of cash or covered monetary instruments exceeding US$10,000 at one time that is transported, mailed or shipped cross-border or that causes such transportation, mailing or shipment);
- The **shipper** or mailer (e.g., the person who engages a common carrier who may also be the originator);
- The **common carrier** (e.g., the business that transports the currency or monetary instruments in exchange for a fee such as an armoured car service; certain types of common carriers are not required to file);
- The **consignee** (e.g., the person who receives the shipment who may also be the ultimate beneficiary and may be appointed by the shipper); and
- The **recipient** of the currency and monetary instruments (e.g., the ultimate beneficiary).

398. Are financial institutions required to file CMIRs?

Yes. Financial institutions are included within the definition of "person" for CMIR purposes, although financial institutions may qualify for exceptions.

Subject to certain exceptions, if a financial institution physically transports, mails or ships, or causes (or attempts to cause) to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000, in many cases, it is required to file a CMIR. For example, per the FFIEC BSA/AML Examination Manual, a bank is required to file a CMIR to report a shipment of currency or monetary instruments in excess of US$10,000 to foreign offices when those shipments are performed directly by bank personnel (e.g., currency shipments transported by bank employees using bank-owned vehicles), because the bank transported the covered items.

A financial institution is not, however, required to file with respect to currency or other monetary instruments mailed or shipped through the postal service or by common carrier. For further guidance on exceptions, please refer to the CMIR Exceptions section.

399. Should a financial institution file a CMIR on behalf of its customer if it has knowledge that the currency or monetary instruments were received or transported from outside of the United States?

No. Unless the financial institution itself transported, mailed, shipped or received or caused or attempted to transport, mail, ship or receive in excess of US$10,000 and it does not otherwise qualify for an exception, if a customer comes to the bank and states that he or she has received or transported currency in an aggregate amount exceeding US$10,000 from outside of the United States, the bank is not required to file a CMIR on behalf of the customer. The customer (or other parties involved in the transportation of the currency or monetary instruments) is obligated to file a CMIR. Financial institutions may advise the customer of its CMIR filing obligations and may be required to file a Currency Transaction Report (CTR), and, if the transaction is unusual or suspicious, a SAR.

400. When a financial institution receives a pouch containing currency and monetary instruments in excess of US$10,000 from outside of the United States, is it considered a recipient and therefore required to file a CMIR?

If the currency and monetary instruments are intended for the financial institution, then the financial institution has an obligation to file a CMIR, unless it otherwise qualifies for an exception. A commercial bank or trust company organised under state or U.S. law is not required to file with respect to overland shipments of currency or monetary instruments shipped to or received from an established customer maintaining a deposit relationship with the bank, in amounts which the bank may reasonably conclude do not exceed amounts commensurate with the customary conduct of the business, industry or profession of the customer concerned.

401. Is virtual currency considered "currency" for CMIR filing purposes?

No. Currently, financial institutions are only required to file CMIRs on covered transactions in excess of US$10,000 as defined above. Per current FinCEN guidance, virtual currency does not meet the definition of currency for BSA reporting purposes as it does not have legal tender status.

State laws may, under certain circumstances, require virtual currency businesses to submit reports on virtual currency transactions greater than US$10,000, similar to CTRs. In July 2014, the New York State Department of Financial Services (DFS) was the first to propose a regulatory framework for virtual currency businesses, which were finalised in 2015.

Virtual currency exchangers dealing in certain types of virtual currency may be subject to AML/CFT requirements of money transmitters. For further guidance, please refer to the sections: Money Services Businesses and Virtual Currency Systems and Participants.

402. Are persons transporting or shipping prepaid access devices across the U.S. border in an aggregate amount of more than US$10,000 required to file a CMIR?

Not currently. However, in October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on CMIRs; no final rule on this proposed change has yet been issued. The term "tangible prepaid access device" would be defined as the following:

- Any physical item that can be transported, mailed, or shipped into or out of the United States and the use of which is dedicated to obtaining access to prepaid funds or the value of funds by the possessor in any manner without regard to whom the prepaid access is issued.

This definition would include devices such as general-use prepaid cards, gift cards, store cards, payroll cards, government benefit cards, and any tangible device to the extent that they can provide access to prepaid funds or the value of funds by being readable by a device employed for that purpose by merchants (e.g., cell phones, key fobs). The definition does not extend to credit and debit cards.

Similar to the exclusion for a traveller's check issuer or its agent, a business or its agent offering prepaid access devices prior to their delivery to a seller for sale to the public would not be subject to the CMIR filing requirement.

For additional guidance on prepaid access devices, please refer to the Prepaid Access and Stored Value section.

403. If the proposed rule were adopted, what value would be reported on CMIRs as it relates to prepaid access devices?

The reportable balance would be the amount available through a prepaid access device at the time of the physical transportation, mail or shipment into or out of the United States.

404. Are financial institutions required to file CMIRs on shipments of bulk currency?

Yes. Cross-border shipments of currency greater than US$10,000 transported through air couriers or airlines must be reported via the CMIR, unless the financial institution qualifies for an exception from filing. For further guidance on exceptions, please refer to the CMIR Exceptions section.

For additional guidance on bulk currency shipments, please refer to the Bulk Shipments of Currency and Bulk Cash Smuggling section.

405. Are CMIRs required for cross-border transportation of precious stones, precious metals or jewels valued at greater than US$10,000?

No. CMIRs are required on reportable currency transactions in excess of US$10,000 as defined above. Per FinCEN guidance, precious metals, precious stones or jewels do not meet the definition of currency or monetary instruments for CMIR reporting purposes. For further guidance on the AML/CFT requirements related to precious metals, precious stones or jewels, please refer to the Dealers in Precious Metals, Precious Stones or Jewels section.

406. Can a financial institution assume that the source of funds of a cross-border movement of currency or monetary instruments is legitimate if a CMIR accompanies the transport?

No. CMIRs serve to document the cross-border physical transportation of currency and monetary instruments. They have no bearing on the legitimacy of the source of funds of the bulk shipment of currency.

407. What are the consequences for failing to file CMIRs?

Civil and/or criminal penalties for failure to file timely forms or failure to include complete and correct information on CMIR forms can include fines, imprisonment up to 10 years and/or seizure of funds.

408. How does the CMIR requirement correspond to FATF Recommendations?

FATF Recommendation 32 – Cash Couriers suggests the implementation of measures to detect, report, and if necessary, confiscate currency and bearer negotiable instruments (BNI) that are physically transported across a border (incoming and outgoing). A threshold of US/EUR 15,000 is recommended. Suggested measures include a declaration system (e.g., written or oral reporting of covered instruments to regulatory authorities), a disclosure system (e.g., provide information only at the request of relevant authorities) and penalties for noncompliance (e.g., fine, confiscation). The CMIR requirement is consistent with the declaration system suggested in Recommendation 32, although at a lower threshold of US$10,000.

For further guidance on international standards, please refer to the Financial Action Task Force section.

CMIR Exceptions

409. Are there exceptions to the CMIR requirement?

CMIRs are not required to be filed by the following:

- A Federal Reserve Bank;
- A bank, a foreign bank, or a broker-dealer in securities, with respect to currency or other monetary instruments mailed or shipped through the postal service or by common carrier;
- A commercial bank or trust company organised under the laws of any state or of the United States with respect to overland shipments of currency or monetary instruments shipped to or received from an established customer maintaining a deposit relationship with the bank, in amounts that the bank may reasonably conclude do not exceed amounts commensurate with the customary conduct of the business, industry or profession of the customer concerned;
- A person who is not a citizen or resident of the United States with respect to currency or other monetary instruments mailed or shipped from abroad to a bank or broker-dealer in securities through the postal service or by common carrier;
- A common carrier of passengers with respect to currency or other monetary instruments in possession of its passengers;
- A common carrier of goods in respect to shipments of currency or monetary instruments not declared to be such by the shipper;
- A traveller's check issuer or its agent with respect to the transportation of traveller's checks prior to their delivery to selling agents for eventual sale to the public;

- A person with a restrictively endorsed traveller's check that is in the collection and reconciliation process after the traveller's check has been negotiated; and
- A person engaged as a business in the transportation of currency, monetary instruments and other commercial papers, also known as common carriers of currency, with respect to the transportation of currency or other monetary instruments overland between established offices of bankers or broker-dealers in securities and foreign persons.

410. Are financial institutions required to file CMIRs on cross-border shipments of currency or monetary instruments via the postal service?

No. A bank, a foreign bank, or a broker-dealer in securities is not required to file CMIRs on currency or other monetary instruments mailed or shipped through the postal service or by common carrier.

However, currency or monetary instruments shipped by other methods, including via air courier or the airlines, are not exempt.

Cross-Border Bulk Shipments of Currency

411. Are common carriers of currency required to file CMIRs on cross-border shipments of currency or monetary instruments they transport in excess of US$10,000?

Yes. With limited exceptions, common carriers of currency are required to file CMIRs on cross-border shipments of currency or monetary instruments in excess of US$10,000. Common carriers of currency can also be required to file multiple CMIRs on separate deliveries within one shipment, even if the individual delivery is less than US$10,000, unless they otherwise qualify for an exception. Moreover, although the CMIR regulations include a number of exemptions that apply to other parties, a common carrier of currency may not claim for itself any exemption for filing a CMIR that might be applicable to other parties.

For example, a bank may be exempted from filing a CMIR with respect to currency that it ships or mails via a common carrier, but the common carrier cannot apply this exemption to itself. For example, if a common carrier of currency picks up at an airport a cargo of currency air-shipped to a U.S. bank from another country, the common carrier has an obligation to file a CMIR, even though the bank does not.

412. Can common carriers of currency rely on other parties to file a CMIR on the cross-border shipment of currency or monetary instruments they transport in excess of US$10,000?

Yes, however, if a CMIR is not filed appropriately (e.g., timely, accurately), the parties who are required to file by law will be held liable, which can include the common carrier.

413. What is the limited exception for common carriers of currency as it relates to CMIRs?

Common carriers of currency are not required to file CMIRs when all of the following conditions are met:

- The entity is engaged as a business in the transportation of currency, monetary instruments and other commercial papers;
- The transportation consists of currency or other monetary instruments imported into the United States or exported out of the United States in an aggregate amount of more than US$10,000 in currency or other covered monetary instruments;
- The transportation takes place overland;
- The transportation takes place between a bank or a broker-dealer in securities, on the U.S. side, and a non-U.S. person, on the foreign side; and
- The shipment is picked up or delivered at the established office of the bank or a broker-dealer in securities on the U.S. side.

For further guidance, please refer to FinCEN's "CMIR Guidance for Common Carriers of Currency, Including Armored Car Services."

414. Are common carriers of currency subject to other AML/CFT requirements?

Depending upon their specific operations, a common carrier could fall within the BSA's definition of a money services business (MSB) (e.g., money transmitter) and be subject to additional AML/CFT requirements. Although not required to maintain an AML Program, common carriers of currency are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, professional service providers are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

For further guidance on carriers, please refer to the Common Carriers of Currency and Armored Car Services section. For further guidance on the AML/CFT requirements of money transmitters, please refer to the Money Services Businesses section. For further guidance on sanctions requirements, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

CMIR Filing

415. What is the time frame for filing CMIRs?

Each person who receives currency must file the CMIR within 15 calendar days after receipt of the currency or monetary instruments. Travelers carrying currency or monetary instruments are required to file a report at the time of entry to or departure from the United States. If unaccompanied by the person entering or departing the United States, CMIRs may be filed by mail with the Commissioner of Customs on or before the date of entry, departure, mailing or shipping of the currency or monetary instruments.

416. Where are CMIRs filed?

All CMIRs should be filed with the customs officer in charge at any port of entry or departure, or as otherwise specified by the Commissioner of Customs.

417. Are CMIRs required to be filed electronically?

No. Unlike many other BSA reports, CMIRs are not required to be filed electronically.

418. How long should CMIRs be retained?

CMIRs must be retained for a minimum of five years from the date of filing.

Registration of Money Services Businesses

RMSB Basics

419. What is a Money Services Business (MSB)?

The BSA defines an MSB as "a person wherever located doing business, whether on a regular basis or as an organised or licensed concern, wholly or in substantial part within the United States, in one or more capacities" listed below:

- **Issuer or seller of traveller's checks or money orders** – A person that:
  - "Issues traveller's checks or money orders that are sold in an amount greater than US$1,000 to any person on any day in one or more instances or
  - Sells traveller's checks or money orders in an amount greater than US$1,000 to any person on any day in one or more transactions."
- **Check casher** – A person that accepts checks or monetary instruments in return for currency or a combination of currency and other monetary instruments or other instruments, in an amount greater than US$1,000 for any person on any day in one or more transactions.
- **Dealer in foreign exchange –** A person that "accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds or other instruments denominated in the currency, of one or more countries in an amount greater than US$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery."
- **Providers of prepaid access** – The participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access (provider). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program.
  - **"Prepaid access" is defined as** "Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number." Prepaid access applies to a very broad range of prepaid services, including but not limited to open-

loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, many prefunded employee programs such as a Health Savings Account.

- **Sellers of prepaid access** – Any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if:
  - That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or
  - That person sells prepaid access (including closed-loop prepaid access) to funds that exceed US$10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales.
- **Money transmitter** – A money transmitter is defined as the following:
  - Any person engaged in the transfer of funds
  - A person who provides money transmission services
    - "**Money transmission services**" is defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."
    - "**By any means**" includes money transmission through the following:
      - A financial agency or institution;
      - A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both;
      - An electronic funds transfer network; or
      - An informal value transfer system.
- **U.S. Postal Service** – **"**The United States Postal Service, except with respect to the sale of postage or philatelic products" (e.g., stamp-related collectible products)

For further guidance on the limitations and exceptions of the aforementioned MSB activities, please refer to the Money Services Businesses section.

420. What is a Registration of Money Services Business (RMSB) form?

Completion and submission of FinCEN 107 form, Registration of Money Services Business (RMSB), satisfies the covered MSB requirement to register with FinCEN. The RMSB must be filed within 180 calendar days after the date the business is established. MSBs must reregister every two years on or before December 31 using the same RMSB form.

The RMSB requirement is implemented under regulation 31 C.F.R. 1022.380 – Registration of Money Services Businesses.

421. Approximately how many MSBs are currently registered with FinCEN?

As of mid-2017, more than 25,000 MSBs were registered with FinCEN.

422. What is the purpose of the registration requirement for MSBs?

The purpose of the registration requirement is to identify MSBs that are operating so they may be monitored for compliance with AML/CFT laws and regulations.

423. Is registration the same as licensing?

No. Registration is administered by FinCEN. Licensing is administered by each state and imposes separate requirements on MSBs. Operating an unlicensed MSB where licensing is required is illegal. For additional details on unlicensed MSBs, please refer to the Informal Value Transfer Systems section.

424. Are there exemptions to the regulatory definition of MSBs?

Yes. The following are exempt from the regulatory definition of MSB:

- Bank or a foreign bank;
- Persons registered with and functionally regulated or examined by the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) or a foreign financial agency that engages in financial activities that, if conducted in the United States, would require the foreign financial agency to be registered with the SEC or CFTC (e.g., broker-dealers in securities, futures commission merchants [FCMs]); and
- Natural person who engages in the aforementioned activities infrequently and not for gain or profit.

425. Are foreign-located businesses engaged in MSB activities within the United States subject to AML/CFT laws and regulations?

Yes. FinCEN clarified that all businesses engaged in MSB activities within the United States, regardless of the physical location of its agents, agencies, branches or offices, are required to comply with AML/CFT laws and regulations, including registering with FinCEN. Examples include foreign entities with U.S. customers and foreign entities transmitting funds to or from U.S. recipients via the internet.

Foreign-located businesses engaged in MSB activities are also required to designate a person who resides in the United States to function as an agent to accept service of legal process.

426. Are all types of MSBs required to register with FinCEN?

No. The following types of MSBs are not required to register with FinCEN:

- MSBs that serve solely as an agent of another MSB
- U.S. Postal Service

427. How is the term "agent" defined for MSBs?

The term "agent," distinct from the agent acting as a legal representative described above, is a separate business entity from the MSB that the MSB authorises, through written agreement or otherwise, to sell its MSB services (e.g., monetary instruments, funds transfers). MSB agents engaging in covered activities are MSBs, too, and are subject to the AML/CFT requirements. Agents may include businesses such as grocery stores, convenience stores, travel agencies and gas stations. For further guidance, please refer to the Money Services Businesses section.

428. Are MSBs required to reregister after the initial registration with FinCEN?

Registrations must be renewed every two years on or before December 31. FinCEN provides an MSB Registration Renewal Calculator to assist in determining the appropriate renewal deadline.

429. Under what circumstances are MSBs required to reregister earlier than the two year period?

Reregistration also is required when one of the following events occurs:

- A change in ownership or control of the MSB requiring reregistration under state registration law
- More than 10 percent of voting power or equity interest of the MSB is transferred (except certain publicly traded companies)
- A 50 percent or more increase in the number of agents

The reregistration form must be filed within 180 calendar days after such a change occurs.

430. Can unlicensed MSBs register with FinCEN?

Yes. MSB registration is required for all covered MSBs, regardless of whether the business is subject to state licensure. However, most licensed MSBs are covered MSBs and, thus, are required to register.

431. What are the consequences of not registering?

MSBs that fail to register or to renew their registrations may be subject to civil and criminal penalties.

432. Are businesses required to de-register if they no longer meet the regulatory definition of an MSB?

No. Businesses are not required to de-register if they no longer meet the regulatory definition of an MSB.

433. How do the U.S. licensing and registration requirements for MSBs correspond to FATF Recommendations?

U.S. licensing and registration requirements for MSBs parallel FATF Recommendations. In **Recommendation 14 – Money or Value Transfer Services**, FATF recommends measures to license and register businesses that provide money or value transfer services (MVTS). Measures should

be applied to agents as well, independently or as part of the AML/CFT Compliance Program of the principal business.

FATF defines MVTS as "financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, message, transfer or through a clearing network to which the MVTS provider belongs."

For further guidance on international standards, please refer to the Financial Action Task Force section.

434. Are MSBs subject to AML/CFT laws and regulations beyond the registration requirement?

Yes. Specific AML/CFT laws and regulations for an MSB vary based on the activities that it is involved in, as well as whether it is performing as the agent or as the principal MSB (e.g., maintaining an AML Program, reporting suspicious activities). For further guidance, please refer to the Money Services Businesses section.

MSB Registrant Search Web Page

435. Where is the monthly MSB Registration List maintained?

The monthly MSB Registration List has been replaced by the MSB Registrant Search Web Page. The MSB Registrant Search Web Page is updated weekly. New RMSBs are added to the MSB Registrant Search Web Page within approximately two weeks of electronic filings and 60 days for paper filings.

436. Is inclusion on the MSB Registrant Search Web Page a recommendation or endorsement from FinCEN?

No. Inclusion on the MSB Registrant Search Web Page is not a recommendation or endorsement of the MSB from FinCEN or any other government agency. The MSB Registrant Search Web Page is intended only as general reference for the public.

437. Does inclusion on the MSB Registrant Search Web Page serve as evidence of an MSB's registration with FinCEN?

Yes. Since the implementation of the MSB Registrant Search Web Page, FinCEN will no longer be sending registration acknowledgement letters. The MSB Registrant Search Web Page will provide MSB Registration Numbers, as well as the name of the registrant, states where the registrant engages in MSB activities and the types of MSB activities provided.

Completing the RMSB

438. What information does an MSB have to include with respect to its agents on its RMSB?

An MSB needs to provide the following information on its agents:

- Number of agents authorised to conduct each money services activity (e.g., money order sales, check cashing, currency exchange) on behalf of the MSB
- Jurisdictions in which it is conducting business that include jurisdictions in which it has agents

439. Should each agent of an MSB register separately with FinCEN?

If a business is acting solely as an agent of an MSB and does not independently provide covered financial services, the agent is not required to register separately with FinCEN.

440. Should each branch of an MSB register separately with FinCEN?

No. An MSB should not register each branch separately with FinCEN.

441. What information must a provider of prepaid access provide when registering with FinCEN?

In addition to a complete and accurate RMSB, a prepaid access provider is, among other things, required to provide a complete list of the prepaid programs for which it serves as a provider.

442. Do MSBs need to indicate on the RMSB all states in which they originate transactions or only states in which the MSB maintains a physical presence?

When completing an RMSB, MSBs should only indicate states in which the MSB, its agents or branches have a physical presence.

443. What supporting information is an MSB required to maintain as it relates to its RMSBs?

An MSB is required to maintain the following supporting documentation:

- Copy of its registration form
- An annual estimate of the volume of the registrant's business in the coming year
- The name and address of owner(s) or individual(s) who control the business (i.e., any shareholder holding more than 5 percent of the registrant's stock, any general partner, any trustee, any director, any officer)
- An agent list

444. Should an MSB send this supporting information to FinCEN along with its RMSB?

No. The supporting documentation detailed above should not be sent to FinCEN but should be maintained at a location within the United States for five years.

Filing of RMSBs

445. How do MSBs submit RMSBs to FinCEN?

After March 31, 2013, MSBs must submit RMSBs through the BSA E-Filing System, a system developed by FinCEN to enable financial institutions to file FinCEN Reports electronically, through discrete or batch filings.

446. How can financial institutions file corrected, amended or renewed RMSBs through the BSA E-Filing System?

MSBs can file amended, corrected or renewed RMSBs by submitting a new RMSB in the BSA E-Filing System.

447. Since MSBs submit RMSBs to FinCEN through the BSA E-Filing System, are they still required to retain copies in accordance with AML/CFT laws and regulations?

Yes. The BSA E-Filing System is not a recordkeeping program. MSBs are required to retain RMSBs for a minimum of five years from the date of filing in accordance with AML/CFT laws and regulations.

BSA Recordkeeping Requirements

Recordkeeping Basics

448. What are the key recordkeeping requirements of the BSA for depository institutions?

The BSA requires the retention of all FinCEN Reports (e.g., SARs, CTRs, FBARs, CMIRs, Form 8300, DOEPs, RMSBs). Additionally, other required documentation must be retained, such as the following:

- Each check, draft or money order drawn on the bank or issued and payable by it, except those drawn for US$100 or less, or drawn on certain accounts that are expected to have at least 100 checks per month drawn on them over the course of a year
- Each item in excess of US$100, other than bank charges or periodic charges made per agreement with the customer, comprising a debit to the customer's deposit account unless exempted
- Each item, including checks, drafts or transfers of credit of more than US$10,000 received directly and not through a domestic financial institution, by letter, cable or any other means from a bank, broker or dealer in foreign exchange outside of the United States
- A record of each remittance or transfer of funds or of currency, other monetary instruments, checks, investment securities or credit of more than US$10,000 to a person, account or place outside of the United States
- Records prepared or received by a bank in the ordinary course of business needed to reconstruct a transaction account and to trace a check in excess of US$100 deposited in the account through its domestic processing system or to supply a description of a deposited check in excess of US$100

- A record containing the name, address and TIN, if available, of the purchaser of each certificate of deposit, as well as a description of the instrument, a note of the method of payment and the date of the transaction
- A record containing the name, address and TIN, if available, of any person presenting a certificate of deposit for payment and a description of the instrument and date of the transaction
- A record of the statement and purpose of each loan over US$10,000, except if secured by real property
- Each piece of advice, request or instruction received regarding a transaction that results in the transfer of funds, currency, checks, investment securities, other monetary instruments or credit of more than US$10,000 to a person or account outside of the United States
- Each piece of advice, request or instruction given to another financial institution or person located within or outside of the United States regarding a transaction intended to result in a transfer of funds, currency, checks, investment securities, other monetary instruments or credit of more than US$10,000 to a person or account outside of the United States
- Each payment order that a financial institution accepts as an originator's, intermediary's or beneficiary's bank with respect to a funds transfer in the amount of US$3,000 or more
- Each document granting signature authority over each deposit account
- Each statement, ledger card or other record of each deposit account showing each transaction involving the account
- Each document relating to a transaction of more than US$10,000 remitted or transferred to a person or account outside of the United States
- Each check or draft in an amount in excess of US$10,000 drawn on or issued by a foreign bank that the bank has paid or presented to a nonbank drawee for payment
- Each item relating to any transaction of more than US$10,000 received on any one occasion directly, and not through a domestic financial institution, from a bank, broker or dealer in foreign exchange outside of the United States
- Each deposit slip or credit ticket reflecting a transaction in excess of US$100 or the equivalent record for direct deposit or wire transfer deposit transactions that shall record the amount of currency involved
- Verifying information obtained about a customer at account opening, which must be retained for five years after the date the account is closed

The above requirements apply to depository institutions and are discussed in further detail under regulation 31 C.F.R. 1010.410 – Records to be Made and Retained by Financial Institutions and 31 C.F.R. 1010.430 – Nature of Records and Retention Period.

Two key recordkeeping requirements also include:

- Funds Transfer Recordkeeping Requirement and the Travel Rule

- Recordkeeping Requirement for the Purchase and Sale of Monetary Instruments

Further details of each are provided below.

The BSA also outlines additional requirements for other types of financial institutions (e.g., dealers in foreign exchange, broker-dealers, casinos). For further guidance on the additional recordkeeping requirements for other types of financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

449. How long are financial institutions required to retain records in accordance with the BSA?

Financial institutions are required to retain records for five years in accordance with the BSA.

Some states, as well as international jurisdictions in which U.S. financial institutions may operate, require longer retention periods.

450. What date should financial institutions use to comply with the five year record retention requirement?

The date depends on the type of product, service or transaction. For example, financial institutions must retain the identifying information obtained at account opening for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant.

When a loan is sold, the account is "closed" under the record retention provision, regardless of whether the financial institution retains the servicing rights to the loan. Thus, records of identifying information about a customer must be retained for five years after the date the loan is sold.

451. Does the BSA outline how records should be stored (e.g., electronically)?

No; however, records should be stored in a manner that allows for retrieval within a reasonable period of time.

452. What is a "reasonable period of time"?

There is no specific time frame prescribed. FinCEN, however, has indicated that records should be accessible within a reasonable period, considering the quantity of records requested, the nature and age of the records, and the amount and type of information provided by the law enforcement agency making the request, as well as the financial institution's transaction volume and capacity to retrieve the records.

Financial institutions are, however, required to retrieve records relating to foreign correspondent banking activity within 120 hours of a request made by a regulatory agency. For further guidance on the "120-Hour Rule," please refer to the Section 319(b) - Bank Records section.

453. What should a financial institution do if it is unable to retrieve requested records within 120 hours?

The financial institution should notify its regulator immediately if it anticipates any delays with an information request.

454. How do the BSA recordkeeping requirements correspond to FATF Recommendations?

The BSA recordkeeping requirements parallel that of FATF.

Recommendation 11 – Recordkeeping suggests financial institutions retain records for a minimum of five years in a manner that enables swift compliance with information requests and permits reconstruction of financial transaction details.

Recommendation 16 – Wire Transfers suggests that requests for information be completed within three business days of the request.

For further guidance on international standards, please refer to the Financial Action Task Force section.

Funds Transfer Recordkeeping Requirement and the Travel Rule

Basics

455. What is the Funds Transfer Recordkeeping Requirement?

The basic requirements of the Funds Transfer Recordkeeping Requirement vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution, beneficiary institution).

For each funds transfer of US$3,000 or more, the originating institution must obtain and retain the following information relating to the payment order:

- The name and address of the originator
- The amount of the payment order
- The execution date of the payment order
- Any payment instructions received from the originator with the payment order
- The identity of the beneficiary's bank
- As many of the following items as are received with the payment order:
    - The name of the beneficiary
    - The address of the beneficiary
    - The account number of the beneficiary
    - Any other specific identifier of the beneficiary

Nonbank financial institutions (NBFIs) also must retain any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

For each funds transfer of US$3,000 or more that the financial institution accepts as an intermediary or beneficiary institution, the institution must retain a record of the payment order (e.g., original record, microfilm).

This recordkeeping requirement for funds transfers and transmittals of funds is implemented under regulation 31 C.F.R. 1010.410 – Records to be Made and Retained by Financial Institutions.

456. What is the Travel Rule?

The Travel Rule refers to the requirement for financial institutions that participate in funds transfers of US$3,000 or more to pass along certain information about the funds transfer to the next financial institution involved in the funds transmittal.

The requirements of the Travel Rule vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution).

The originating financial institution must forward the following information to the next financial institution in the chain:

- The name of the originator
- The account number of the originator, if used
- The address of the originator
- The amount of the payment order
- The execution date of the payment order
- The identity of the recipient's financial institution
- As many of the following items as are received with the payment order:
    - Name of the recipient
    - Address of the recipient
    - Account number of the recipient
    - Any other specific identifier of the recipient
- Either the name and address or the numerical identifier of the originator's financial institution

A financial institution serving as an intermediary must pass on the required information listed above, if received from the preceding financial institution, to the next financial institution in the chain. The intermediary, however, has no obligation to obtain information not provided by the preceding financial institution.

457. What is the difference between the Funds Transfer Recordkeeping Requirement and the Travel Rule?

The Funds Transfer Recordkeeping Requirement requires each financial institution involved in funds transfers to collect and retain certain information in connection with funds transfers of US$3,000 or more.

At the same time, a companion rule, the Travel Rule, requires financial institutions to include certain information in payment orders for funds transfers of US$3,000 or more.

458. Which entities are required to comply with the Funds Transfer Recordkeeping Requirement and Travel Rule?

The rules apply to the following:

- Banks
- Broker-dealers in securities
- Casinos and card clubs that meet specified thresholds (e.g., annual gaming revenue)
- Money transmitters which meet specified thresholds
- Telegraph companies
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Any entity subject to supervision by any state or federal bank supervisory authority

459. Do the requirements imposed on nonbank financial institutions (NBFIs) differ from the requirements imposed on depository institutions?

Yes. The requirements are very similar, although the terminology differs for NBFIs. Rather than using the terms “originator,” “beneficiary” and “payment order,” the terminology for NBFIs is “transmitter,” “recipient” and “transmittal order,” respectively. NBFIs also are required to retain any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

460. What are the benefits of the Funds Transfer Recordkeeping Requirement and Travel Rule to law enforcement?

The Funds Transfer Recordkeeping Requirement and Travel Rule provide an audit trail regarding individuals and entities sending and receiving funds through the funds transfer system, helping law enforcement agencies detect, investigate and prosecute money laundering and other financial crimes.

461. How are “funds transfers” and “transmittal of funds” defined? What is the difference?

The term “funds transfer,” which includes wire transfers, is used to describe the following series of transactions as executed by banks. The BSA defines “funds transfers” as:

- The “series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by

the originator's bank or an intermediary bank intended to carry out the originator's payment order.

- A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order."

The term "transmittal of funds" is used to describe the following series of transactions as executed by NBFIs. The BSA defines "transmittals of funds" as:

- The "series of transactions beginning with the transmittor's transmittal order, made for the purpose of making payment to the recipient of the order. The term includes any transmittal order issued by the transmittor's financial institution or an intermediary financial institution intended to carry out the transmittor's transmittal order.
- A transmittal of funds is completed by acceptance by the recipient's financial institution of a transmittal order for the benefit of the recipient of the transmittor's transmittal order."

Other than the executing parties, there is no difference between the terms "funds transfers" and "transmittal of funds."

462. Are there any exemptions from the definitions of "funds transfer" or "transmittal of funds"?

Yes. The following transactions are exempt from the definition of "funds transfer" and "transmittal of funds":

- Electronic funds transfers (EFTs) defined in Section 903(7) of the Electronic Funds Transfer Act of 1978 (EFTA) (as amended) as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorise a financial institution to debit or credit an account."
- Any other funds transfers that are made through an automated clearing house (ACH), an automated teller machine (ATM), or a point-of-sale (POS) system.

463. Are all funds transfers subject to this recordkeeping requirement, regardless of the amount?

No. Only funds transfers (or transmittals of funds) as defined above, equal to or greater than US$3,000 are subject to the rule.

464. Are there instances in which recordkeeping requirements are required for funds transfers of less than US$3,000?

Yes. A Geographic Targeting Order (GTO) gives the U.S. Treasury Department, and in some instances states, the authority to require a financial institution or a group of financial institutions or businesses in a geographic area to file additional reports or maintain additional records above and beyond the ordinary requirements for funds transfers. GTOs are used to collect information on individuals/entities suspected of conducting transactions under a certain threshold (e.g., under US$3,000).

465. What types of funds transfers are not subject to the Funds Transfer Recordkeeping Requirement Rule?

Funds transfers where both the originator and the beneficiary are the same person and the originator's bank and the beneficiary's bank are the same bank are excluded. Additionally, exceptions are provided from the recordkeeping requirements for funds transfers where the originator and beneficiary (or transmitter and recipient) are:

- A domestic bank
- A wholly owned domestic subsidiary of a bank chartered in the United States
- A domestic broker or dealer in securities or a wholly owned domestic subsidiary of a broker or dealer in securities
- An FCM or IB in commodities or a wholly owned domestic subsidiary of an FCM or IB in commodities
- U.S., state or local government
- A federal, state or local government agency or instrumentality
- A mutual fund

466. Do the obligations of a financial institution differ for funds transfers involving noncustomers?

Yes. A financial institution must consider three factors when assessing its obligations:

- Whether the financial institution is the sending/receiving institution;
- If the payment order/proceeds are not made/delivered in person; and
- Whether the funds are sent or received by an agent of the originator/beneficiary.

The requirements imposed on the financial institution vary from collecting information about the originator, beneficiary and agent (where applicable) and include name and address, type and number of identification reviewed, TIN, and copy or record of the method of payment. Additionally, the financial institution must verify identity under certain circumstances.

467. Do the Funds Transfer Recordkeeping Requirement and Travel Rule require reporting to the government of any information?

No. However, if a funds transfer or transmittal of funds appears to be suspicious, then a Suspicious Activity Report (SAR) is required, if the financial institution is subject to the suspicious activity reporting requirement.

In 2010, FinCEN issued a proposed rule that would impose additional reporting requirements of transmittal orders associated with "cross-border electronic transmittals of funds" (CBETFs). For further guidance, please refer to the Cross-Border Electronic Transmittal of Funds section.

468. What other AML/CFT requirements are required for funds transfers?

Financial institutions are also required to monitor for potentially suspicious activity and screen transactions for possible OFAC Sanctions violations. For additional guidance, please refer to the sections Office of Foreign Assets Control and International Sanctions Programs and Blocking and Rejecting Transactions.

In instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

For additional guidance on the AML/CFT risks of funds transfers, please refer to the Funds Transfers section.

469. Does the CFPB's Remittance Transfer Rule impose additional AML/CFT-related requirements on financial institutions?

No. Pursuant to Section 1073 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB's Remittance Transfer Rule, which amends the Electronic Funds Transfer Act of 1978 (EFTA) implemented under Regulation E, is intended to protect consumers who send money electronically to foreign countries by providing more information about the costs of remittances. The rules apply to most international remittances regardless of their purpose, including, but not limited to funds transfers and automated clearing house (ACH) transactions. Specifically, they would require the following:

- Disclosures in English including:
  - A prepayment disclosure at the time the person initiates that lists the following:
    - The exchange rate;
    - Fees and taxes collected by the companies;
    - Fees charged by the companies' agents abroad and intermediary institutions;
    - The amount of money expected to be delivered abroad, not including certain fees to be charged to the recipient or foreign taxes; and
    - If appropriate, a disclaimer that additional fees and foreign taxes may apply.
  - A receipt disclosure which must be provided to the sender once the payment has been made.
- A provision that consumers can cancel a transfer within 30 minutes (and sometimes more) of originating it;
- Requirements that companies must investigate problems consumers report about transfers and provide standards for error resolutions (e.g., refund, resending of transfer free of charge);
- Companies are made responsible for mistakes made by certain people who work for them; and
- Provisions relating to transfers pre-scheduled on a regular basis.

The rule is applicable to banks, thrifts, credit unions, money transmitters and broker-dealers that consistently execute 100 or more remittance transfers per calendar year and applies to remittance transfers that are more than US$15, made by a consumer in the United States, and sent to a person or company in a foreign country.

The Remittance Transfer Rule became effective on October 28, 2013. The CFPB has provided model forms as well as an International Funds Transfer Small Entity Compliance Guide; these and other information related to the rules can be found on the CFPB's website at www.consumerfinance.gov.

470. How do the Funds Transfer Recordkeeping Requirement and Travel Rule correspond to FATF Recommendations?

The Funds Transfer Recordkeeping Requirement and Travel Rule generally parallel FATF **Recommendation 16 – Wire Transfers.** Recommendation 16 advises financial institutions to require and retain information about domestic and cross-border wire transfers (e.g., originator information, beneficiary information, account number), including cover payments, and pass along the information to the next financial institution involved in the payment chain. A de minimis threshold no higher than US/EUR 1,000 was recommended for cross-border wire transfers. Requests for information about wire transfers should be completed within three business days of the request.

The Funds Transfer Recordkeeping Requirement and Travel Rule apply to funds transfers equal to or greater than US$3,000. A reporting requirement was proposed in 2010 for transmittal orders associated with cross-border electronic transmittals of funds (CBETF) for all amounts for banks and for amounts greater than US$1,000 for money transmitters.

The Funds Transfer Recordkeeping Requirement does not prescribe a time frame for responding to information requests.

Recommendation 16 also requires financial institutions to monitor wire transfers for suspicious activity and to implement mechanisms to enable screening, and when appropriate, freezing or rejecting wire transfers involving designated (or sanctioned) persons (e.g., terrorists). For further guidance, please refer to the Suspicious Activity Reports, Wire Transfer Red Flags and the Office of Foreign Assets Control and International Sanctions Programs sections.

Addresses and Abbreviations

471. What type of address may the originator or beneficiary provide?

The Funds Transfer Recordkeeping Requirement requires the financial institution to collect and maintain the originator's or beneficiary's street address. The Travel Rule allows the address of the originator or beneficiary to be the street address or a mailing address so long as the street address is available in the originating financial institution's customer information file and it is retrievable upon law enforcement's request.

It is recommended that both the street address and mailing address be included in screenings so that Office of Foreign Assets Control (OFAC) checks can be conducted properly.

472. If a customer arranges to have his or her mail held at the financial institution, can the customer use the financial institution's address as his or her address in the funds transfer transmittal?

No. The financial institution should use the customer's address in the funds transfer transmittal.

473. Does the use of abbreviated names and mailing addresses violate the Travel Rule?

The Travel Rule does not consider the use of abbreviated trade names (e.g., ABC Company versus Alpha Bravo Charlie Company), names reflecting different accounts of a corporation (e.g., ABC Company Payroll Account) and assumed names (i.e., doing business as [DBA]) or the names of unincorporated divisions or departments of the business as violations. The Funds Transfer Recordkeeping Requirement does not consider the use of a mailing address, including a post office box, as a violation either, so long as the street address is available upon law enforcement's request.

474. Can a financial institution use coded customer names and addresses within funds transmittals?

No. Financial institutions need to ensure they do not use coded customer names and addresses in funds transmittals. The uncoded name and address of the customer must be forwarded to the next financial institution in the chain to comply with the funds transfers recordkeeping requirement rule.

Verification of Identity

475. What requirements are imposed on financial institutions regarding verification of identity for established customers?

There is no verification of identity requirement for established customers. An established customer is a person with an account at a financial institution or a person for whom the financial institution has obtained or maintains on file the person's name, address and TIN. Verification is, however, required for noncustomers.

476. What types of documentation can the financial institution use to verify identity for noncustomers?

Where verification is required, the financial institution should verify a person's identity by examining a document (other than a bank signature card) that contains the person's name, address and, preferably, photograph. The documentation used to verify the identity should be the type normally acceptable by financial institutions as a means of identification when cashing checks for a person other than an established customer.

Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States may be made by passport, alien identification card, or other official document evidencing nationality or residence (e.g., a foreign driver's license with indication of home address).

Joint Party Transmittals and Aggregation

477. How should joint party transmittals of funds be treated?

When a transmittal of funds is sent to more than one recipient, the originator's financial institution may select one recipient as the person whose information must be passed which should be the account holder who ordered the transmittal of funds (in the case of joint accounts). In all other instances where more than one originator sends funds, the financial institution may choose one person whose information must be passed on. However, records on all parties must be kept.

478. How should aggregated transmittals of funds be treated?

A financial institution becomes the originator when it aggregates separate originators from separate transmittals of funds. Similarly, a financial institution becomes the recipient when it combines separate recipients from separate payment orders. However, records on all parties must be kept.

479. If a corporation has one or several individuals who are authorised by the corporation to order funds transfers through the corporation's account, who is the originator in such a transfer?

The corporation, and not the individual(s) authorised to issue the order on behalf of the corporation, is the originator. Accordingly, the information must be retrievable by the name of the corporation, not by the name of the individual ordering the funds transfer.

480. Who is the originator in a transaction where a trustee initiates a funds transfer on behalf of the trust?

The trust is the originator of the funds transfer, and not the trustee initiating the funds transfer. The trustee is merely the person authorised to act on behalf of the trust, a separate legal entity, similar to authorised signers on a corporate account.

Retrievability

481. What are the retrievability requirements of the Funds Transfer Recordkeeping Requirement?

The information a financial institution must obtain and retain, as required, should be retrievable by the name of the originator or beneficiary. The information also should be retrievable by account number if the originator/beneficiary is an established customer of the financial institution and has an account used for funds transfers.

482. Are financial institutions required to maintain records in a specific format?

No. Financial institutions can decide on the format, so long as the financial institution can retrieve the information required in a reasonable period of time.

483. What is the time frame allotted for retrieving records?

There is no specific time frame prescribed with respect to the Funds Transfer Recordkeeping Requirement. FinCEN, however, has indicated that records should be accessible within a reasonable period, considering the quantity of records requested, the nature and age of the records, and the amount and type of information provided by the law enforcement agency making the request, as well as the financial institution's transaction volume and capacity to retrieve the records.

Financial institutions are, however, required to retrieve records relating to correspondent banking activity within 120 hours of a request made by a regulatory agency and within seven days for a law enforcement inquiry. For further guidance on the "120-Hour Rule," please refer to the Section 319(b) – Bank Records section.

Cover Payments and SWIFT

484. What are cover payments?

"Cover payments" are used in correspondent banking as a cost effective method of sending international transactions on behalf of customers. A cover payment involves several actions by financial institutions:

- Obtaining a payment order from the customer;
- Sending of a credit transfer message for an aggregate amount through a messaging network (e.g., Society for Worldwide Interbank Financial Telecommunication [SWIFT]) that travels a direct route from the originating bank to the ultimate beneficiary's bank;
- Execution of a funds transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message; and
- Disbursement of funds to the ultimate beneficiary in accordance with the credit transfer message.

485. What challenges have cover payments posed?

Previous messaging standards did not include information on the ultimate originators and beneficiaries of cover payments. The lack of information posed a challenge for recordkeeping, suspicious activity monitoring and sanctions screening.

486. What is SWIFT's role in the international payments system?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the infrastructure supporting both global correspondent banking and most domestic payment systems and Real-Time Gross Settlement (RTGS) networks involving over 11,000 financial institutions (e.g., banks, broker-dealers, investment managers) in more than 200 countries and territories. Participants also include corporate as well as market infrastructures (settlement and clearing organisations) in payments, securities, treasury and trade.

Message types (MTs) are used to transmit financial information and instructions from one participating financial institution to another, also referred to as SWIFT FIN messages.

Oversight is provided by central banks including the National Bank of Belgium, the Bank of England, the Bank of Japan and the U.S. Federal Reserve.

487. What is the purpose of SWIFT?

SWIFT is used to advise on funds transfers. The actual funds movements (payments) are completed through correspondent banking relationships.

In addition to customer and bank funds transfers, SWIFT is used to transmit foreign exchange confirmations, debit and credit entry confirmations, statements, collections, and documentary credits.

488. Is SWIFT a financial institution or a payment system?

SWIFT is neither a financial institution nor a payment system: SWIFT is solely a message service.

489. What types of messages can be sent through SWIFT's network?

Nine types of preformatted messages, called message types (MT), currently exist for different types of financial transactions. Examples include, but are not limited to, the following:

- **MT 1nn** – Customer Payments:
  - **MT 101** – Request for Transfer – Requests to debit a customer's account held at another institution
  - **MT 102** – Multiple Customer Credit Transfer – Conveys multiple payment instructions between financial institutions
  - **MT 103** – Single Customer Transfer Credit – Instructs a funds transfer
- **MT 2nn** – Financial Institution Payments (e.g., bank-to-bank transactions):
  - **MT 200** – Financial Institution Transfer for its Own Account – Requests the movement of the sender's funds to its account at another financial institution
  - **MT 201** – Multiple Financial Institution Transfer for its Own Account – Multiple MT 200s
  - **MT 202** – General Financial Institution Transfer – Requests the movement of funds between financial institutions
  - **MT 202 COV** – General Financial Institution Transfer – Used to order the movement of funds to an underlying customer credit transfer sent as a cover payment.
- **MT3nn** – Treasury Markets, Foreign Exchange, Money Markets, Derivatives:
  - **MT 300** – Foreign Exchange Confirmation – Confirms information agreed to in the buying/selling of two currencies
  - **MT 304** - Advice/Instruction of a Third Party Deal – Advises of or instructs settlement of a third party foreign exchange deal

- Additional message types include:
  - **MT 9n** – System messages applicable to all message types
  - **MT 4nn** – Collection and Cash Letters
  - **MT 5nn** – Securities Markets
  - **MT 6nn** – Treasury Markets, Precious Metals
  - **MT 7nn** – Treasury Markets – Documentary Credits and Guarantees
  - **MT 8nn** – Travellers' Checks
  - **MT 9nn** – Cash Management and Customer Status

490. How are financial institutions identified within SWIFT MT messages?

The Bank Identifier Code (BIC) is a unique address which, in telecommunication messages, identifies precisely the financial institutions involved in financial transactions.

A BIC code can be either 8 or 11 digits long; an 8 digit code would refer to a primary office of a bank, while an 11 digit code would refer to a specific branch location. The first four digits in the code specify the bank, the next two the country, the following two the specific location (such as city), and the last three, if present, the specific branch. For example, the BIC code for UBS Zurich is: UBSWCHZH80A (UBSW for the bank, CH for Switzerland, ZH for Zurich and 80A for the branch).

491. What information is included in a SWIFT MT message?

A SWIFT MT message has two main parts:

- The **header** contains the sender, the message type and the receiver.
- The **message text** contains the payment instructions.

The remaining lines contain the payment instructions. Each line contains a colon followed by a number that represents a tag or field description. Tags include, but are not limited to, the following:

- **Tag 20** – Sender's Reference
- **Tag 23B** – Bank Operation Code
- **Tag 32A** – Value Date/Currency/Interbank Settled Amount
- **Tag 33B** – Currency/Instructed Amount
- **Tag 50K** – Ordering Customer
- **Tag 59** – Beneficiary Customer
- **Tag 71A** – Details of Charges

492. What enhancements were made to SWIFT's messaging with regard to cover payments?

MT 202s were often used in lieu of the MT 103s, in part, because MT 202s were more cost-effective. Regardless of the reason, however, the substitution of an MT 202 for an MT 103 in a commercial transaction masked the underlying parties to a transaction, thereby frustrating attempts to comply with recordkeeping, monitoring and sanctions requirements.

To address this lack of transparency, in 2009, SWIFT developed a variant of the MT 202 payment message type, MT 202 COV, which allows all information contained in certain fields (e.g., originator and beneficiary information) of the MT 103 to be transmitted in the MT 202 COV and is to be used for cover payments in lieu of MT 202s. The MT 202 COV provides intermediary banks with additional originator and beneficiary information to perform sanctions screening and suspicious activity monitoring.

To further improve efficiency and transparency of cross-border payments, SWIFT developed a global payments innovation (GPI) (expected to go live in 2017), a cloud-based payments tracking service that allows correspondents to see payments end-to-end throughout all legs of the transaction and meet regulatory requirements (e.g., KYC rules, sanctions screening, audit requests).

493. How can SWIFT messages be used to support sanctions screening?

SWIFT messages contain payment information such as originators, intermediate beneficiaries, ultimate beneficiaries and multiple banks involved in the transfers. It is important that these fields be screened against government sanctions lists (e.g., OFAC Sanctions Listings, U.N. Consolidated Lists).

For further guidance on screening software, please refer to the AML/CFT Technology section. For further guidance on sanctions screening, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

494. Do all SWIFT messages need to be screened as part of a sanctions program?

When implementing a risk-based sanctions compliance program, financial institutions may elect to include only SWIFT messages that constitute payment instructions. For example, the message MT 950 – Statement Message provides balance and transaction details of an account to the account owner and is widely used for account reconciliation within a bank, but does not constitute a payment instruction.

The decision to limit SWIFT messages may be restricted by the type of screening system used by a financial institution. For example, some systems have the ability to screen all messages, while others can only screen those messages that constitute a payment instruction.

495. How can SWIFT messages be used to support suspicious transaction monitoring efforts?

Many SWIFT message types can be converted to a format for import into an AML/CFT suspicious transaction monitoring system.

For those SWIFT message types that cannot be converted, a manual review by AML/CFT investigators may be implemented to support investigations into potentially suspicious activity. For example, in the

case of transactions related to letters of credit (LCs), it is imperative that the AML/CFT investigators compare the transfer amount (listed in an analysable SWIFT message type) to the terms listed in the LC to determine whether the transaction(s) is/are potentially suspicious.

For further guidance on suspicious activity monitoring, please refer to the Transaction Monitoring, Investigations and Red Flags section.

496. How are SWIFT messages used by the U.S. Department of Treasury to combat terrorist financing?

Following the terrorist activity on September 11, 2001, the U.S. Department of Treasury established the Terrorist Finance Tracking Program (TFTP) to identify, track and pursue terrorists by conducting targeted searches on data provided by SWIFT. The U.S. Department of Treasury submits subpoenas to the U.S. and European operating centres of SWIFT for financial messaging data related to specific terrorism investigations.

For further guidance on counter-terrorism efforts, please refer to the Counter Terrorism Sanctions Program section.

497. Is the TFTP limited to SWIFT messages from U.S. financial institutions?

No. In 2010, the United States and the European Union signed an international agreement authorising the transfer of financial messaging data from SWIFT's European operating centre to the U.S. Department of Treasury specifically for counter-terrorism efforts.

498. Are all SWIFT messages made available to the TFTP?

No. SWIFT provides messages requested through a subpoena from the U.S. Department of Treasury.

However, in 2010, FinCEN issued a proposed rule that would impose additional reporting requirements of transmittal orders (e.g., SWIFT messages) associated with "cross-border electronic transmittals of funds" (CBETFs). For further guidance, please refer to the Cross-Border Electronic Transmittals of Funds section below.

Cross-Border Electronic Transmittals of Funds

499. Are any additional reporting requirements under consideration with regard to funds transfers?

Yes. In September 2010, FinCEN issued Notice of Proposed Rulemaking, "Cross-Border Electronic Transmittals of Funds." The proposed rule would require banks and money transmitters to report transmittal orders associated with cross-border electronic transmittal of funds (CBETFs) within five business days following the day when the reporting financial institution issued or received the respective transmittal order. Banks would be required to report transmittal orders on all CBETFs; money transmitters would be limited to reporting on CBETFs greater than or equal to US$1,000, or the equivalent in other currencies.

Additionally, all banks would be required to submit an annual report to FinCEN that provides the number of the account that was credited or debited to originate or receive a CBETF and the U.S. taxpayer identification number (TIN) of the respective account holder by April 15 of the year following the transaction date.

At the time of this publication, no final rule has been issued.

500. How are CBETFs defined by the proposed rule?

The proposed rule defines CBETFs as transmittals of funds where either the transmittal order (e.g., payment instruction) or the advice (e.g., notification that a credit to an account has been made in relation to a CBETF) is:

- Communicated through electronic means; and
- Sent or received by either a first-in or last-out financial institution.

501. What are "first-in" and "last-out" financial institutions?

A first-in financial institution is "the first financial institution with respect to a transmittal of funds that receives a transmittal order or advice from a foreign financial institution" (for incoming CBETFs). A last-out financial institution is "the last financial institution with respect to a transmittal of funds that sends a transmittal order or advice to a foreign financial institution" (for outgoing CBETFs).

First-in/last-out financial institutions are viewed by FinCEN as consistently having more complete information about the CBETF than other U.S. financial institutions involved in the transmittal of funds.

502. Are financial institutions required to report on CBETFs where settlement never occurred?

Yes. The proposed CBETF rule is focused on the evidence of the payment represented by the transmittal order, and not the actual payment itself.

503. What information does the proposal indicate would need to be reported on CBETFs?

As proposed, the following information would be required to be reported to FinCEN on CBETFs:

- Unique transaction identifier number
- Either the name and address or the unique identifier of the transmitter's financial institution
- Name and address of the transmitter
- The account number of the transmitter (if applicable)
- The amount and currency of the transmittal of funds
- The execution date of the transmittal of funds
- The identity of the recipient's financial institution
- The name and address of the recipient

- The account number of the recipient (if applicable)
- Any other specific identifiers of the recipient or transaction
- For transactions of US$3,000 or more, reporting money transmitters shall also include the U.S. taxpayer identification number of the transmitter or recipient (as applicable) or, if none, the alien identification number or passport number and country of issuance

504. How would financial institutions submit the required information to FinCEN?

If a final rule is adopted, financial institutions would submit electronic copies of funds transmittal orders to FinCEN to fulfil reporting requirements.

505. When would reporting be required?

Reports would be required to be filed within five business days following the day the bank or money transmitter sent or received the transmittal order.

Additionally, all banks would be required to submit an annual report to FinCEN that provides the number of the account that was credited or debited to originate or receive a CBETF and the U.S. taxpayer identification number (TIN) of the respective account holder by April 15 of the year following the transaction date.

506. Can reports be submitted by a third party?

Yes. Third-party "centralised repositories" of CBETF information, such as SWIFT, can report CBETF information directly to FinCEN at the direction of a financial institution.

507. Are there any exceptions to the proposed rule?

The following electronic transmittals would be exempt from the proposed rule:

- Cross-border electronic transmittals of funds where either the transmitter is a bank and the recipient is a foreign bank, or the transmitter is a foreign bank and the recipient is a bank and, in each case, there is no third-party customer to the transaction; or
- The transmittal order and advice of the transmittal order are communicated solely through systems proprietary to a bank.

508. What would the impact of the proposed rule be?

FinCEN estimates suggest that based on geographic factors and proposed reporting thresholds, approximately 300 banks and 700 MSBs would be affected by the proposed rule resulting in some 500 to 700 million reports per year.

509. What would be the value of the proposed CBETF rule?

Per FinCEN, the proposed CBETF rule would enhance law enforcement's ability to detect, investigate and prosecute ML and TF offenses by creating a centralised database of CBETF information that could be proactively queried to detect patterns of potentially suspicious activity that was not previously

available. In particular, the proposed rule would potentially assist in detecting criminal activity related to terrorist financing (e.g., low dollar wire transfers) and tax evasion (e.g., wire transfers to offshore tax havens).

Recordkeeping Requirement for the Purchase and Sale of Monetary Instruments

510. What records are required for purchases and sales of monetary instruments for currency?

A financial institution that issues or sells for currency a monetary instrument (i.e., bank check or draft, foreign draft, cashier's check, money order, traveller's check) for amounts between US$3,000 and US$10,000 inclusive must first obtain the following information if the individual has a deposit account at the institution:

- The name of the purchaser
- The date of the purchase
- The type(s) of instrument(s) purchased
- The serial number(s) of each instrument(s) purchased
- The amount in dollars of each of the instrument(s) purchased

If the individual does not have a deposit account at the institution, in addition to the above, the following information must be obtained:

- Address of the purchaser
- SSN of the purchaser (or alien identification number if the purchaser is not a U.S. person)
- Date of birth (DOB) of the purchaser

This recordkeeping requirement is implemented under 31 C.F.R. 1010.415 – Purchases of Bank Checks and Drafts, Cashier's Checks, Money Orders and Traveller's Checks.

511. What additional steps must the financial institution take to comply with the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments?

In the case of deposit account holders, the financial institution also must verify that the individual is a deposit account holder (if verification of identity was previously conducted) or must verify the individual's identity. In the case of nondeposit account holders, the financial institution must verify the purchaser's name and address. Verification must be conducted in the following manner:

- Use of a signature card or other file or record at the financial institution, provided that the deposit account holder's name and address were verified previously and that information was recorded on the signature card or other file or record
- By examination of a document that is normally acceptable within the banking community as a means of identification when cashing checks

512. What is the value of the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments rule to law enforcement?

By proactively requiring financial institutions to maintain complete records on the purchase and sale of monetary instruments for currency, law enforcement will have sufficient information available to investigate potentially suspicious transactions (e.g., identification of transaction counterparties) quickly.

513. How are monetary instruments defined for the purpose of recordkeeping requirements for the purchases and sales of these instruments?

A monetary instrument is defined as follows:

- Bank check or draft
- Foreign draft
- Cashier's check
- Money order
- Traveller's check

514. Are prepaid access devices considered monetary instruments for the purpose of recordkeeping requirements for the purchases and sales of these instruments?

No. Prepaid access devices are not considered monetary instruments for the purposes of the recordkeeping requirements for the purchase and sale of monetary instruments. However, in October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on Reports of International Transportation of Currency or Monetary Instruments (CMIRs). No final rule on this proposed change has yet been issued. Section 13 of the proposed bill Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017, introduced by the U.S. Senate in May 2017, proposed amending the definition of monetary instrument to include funds stored in a digital format (e.g., prepaid access devices, virtual currency). Whether this bill will ever be passed into law is unclear.

For further guidance on prepaid access, please refer to the Prepaid Access and Stored-Value section. For further guidance on CMIRs, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

515. Do the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments apply to transactions in excess of US$10,000?

No. If the transaction exceeds US$10,000, Currency Transaction Report (CTR) filing requirements become applicable. For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

516. Do sales of monetary instruments for currency need to be aggregated for the documentation requirements above?

The recordkeeping requirements are applicable for multiple sales of the same or different types of monetary instruments totalling US$3,000 or more in one business day if the financial institution has knowledge that these sales have occurred.

517. If the purchaser of the monetary instrument is a customer of the financial institution, is the financial institution still obligated to collect the required information?

Yes. All purchases of monetary instruments for currency between US$3,000 and US$10,000 inclusive must be recorded, regardless of the purchaser's status as a customer of the institution. The only difference between the treatment of a customer and a noncustomer may be that the financial institution already has the required information on the customer and need only confirm its accuracy.

518. If the purchaser of the monetary instrument deposits the currency into his or her account prior to purchasing the instrument, is the financial institution still obligated to collect the required information?

Yes. The financial institution must still record the purchase of the monetary instrument for currency despite the fact that the customer deposits the currency into his or her account prior to the purchase. Depositing the currency into an account does create a paper trail; however, the purpose of the requirement is to document that currency was used to make the purchase.

519. How can a financial institution evidence its compliance with the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments?

Though it is no longer required, financial institutions often maintain the required information in "Money Order Logs" or, more generally, "Logs of Negotiable Instruments." Maintaining electronic logs (e.g., spreadsheets, databases) as opposed to paper logs will assist with performing queries for internal investigations, 314(a) inquiries, or OFAC screenings.

520. How long should a financial institution maintain documentation supporting Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments?

Documentation must be retained for a minimum of five years.

521. What other recordkeeping and reporting requirements are required for monetary instruments?

Monetary instruments are also subject to the following recordkeeping and reporting requirements:

- **Form 8300:** Form 8300 should be completed and then submitted to the IRS if a person engaged in trade or business, in the course of that trade or business, receives more than US$10,000 in single or multiple related transactions in:
  - Cash, or

- Covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

For additional guidance, please refer to the Form 8300 section.

- **Report of International Transportation of Currency or Monetary Instruments (CMIR)**: The CMIR is required to be filed by:
  - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
  - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding US$10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States. For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a **Suspicious Activity Report (SAR)**. For further guidance, please refer to the Suspicious Activity Reports section.

For additional guidance on the AML/CFT risks of monetary instruments, please refer to the Monetary Instruments section.

522. Is the definition of "monetary instruments" for this recordkeeping requirement the same for other BSA reporting requirements?

The term "monetary instrument" is defined separately for each BSA requirement. Form 8300 utilises the same definition as the Recordkeeping Requirement for the Purchase and Sale of Monetary Instruments (e.g., a cashier's check [by whatever name called, including treasurer's check and bank check], bank draft, traveller's check, or money order).

For CMIRs, the definition of monetary instruments also includes bearer shares.

523. How are "monetary instruments" defined by FATF?

FATF uses the term "bearer negotiable instruments (BNI)" to describe monetary instruments. BNIs are defined as "monetary instruments in bearer form such as: traveller's checks negotiable instruments (including checks, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including checks, promissory notes and money orders) signed, but with the payee's name omitted."

For further guidance on international standards, please refer to the Financial Action Task Force section.

USA PATRIOT ACT

USA PATRIOT Act Basics

524. What is the USA PATRIOT Act?

Following the terrorist activity of September 11, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was signed into law by President George W. Bush on October 26, 2001, significantly amending the Bank Secrecy Act (BSA). The USA PATRIOT Act has 10 titles:

- **Title I: Enhancing Domestic Security Against Terrorism**
- **Title II: Enhanced Surveillance Procedures**
- **Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001**
- **Title IV: Protecting the Border**
- **Title V: Removing Obstacles to Investigating Terrorism**
- **Title VI: Providing for Victims of Terrorism, Public Safety Officers and Their Families**
- **Title VII: Increased Information Sharing for Critical Infrastructure Protection**
- **Title VIII: Strengthening the Criminal Laws Against Terrorism**
- **Title IX: Improved Intelligence**
- **Title X: Miscellaneous**

Title III, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, deals with money laundering and terrorist financing. Title III made significant changes to U.S. money laundering regulations, imposed enhanced requirements for AML Programs, and significantly expanded the scope of coverage to nonbank financial institutions (NBFIs). It requires financial institutions to establish AML Programs that include policies, procedures and controls, designation of a compliance officer, training and independent review. In addition, it requires certain financial institutions to have customer identification procedures for new accounts and enhanced due diligence (EDD) for correspondent and private banking accounts maintained by non-U.S. persons.

The USA PATRIOT Act Improvement and Reauthorisation Act of 2005 made permanent certain temporary provisions of the USA PATRIOT Act; increased civil and criminal penalties for terrorist financing and terrorist attacks on mass transportation systems and seaports (e.g., enhancements to death penalty procedures); included laundering through informal value transfer systems (IVTSs) (e.g., hawalas) within the federal definition of money laundering; implemented safeguards to protect civil liberties related to various provisions of the USA PATRIOT Act (e.g., National Security Letters [NSLs],

roving surveillance orders, access to business records); and imposed additional measures to combat the trafficking of methamphetamine.

525. What are the key provisions of the USA PATRIOT Act?

The following is a summary of the key provisions of the USA PATRIOT Act:

- **Section 311 – Special Measures for Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern**
  - Section 311 provides the U.S. Department of the Treasury broad regulatory authority to impose one or more of five Special Measures against foreign jurisdictions, foreign financial institutions, and types of transactions and accounts that involve such foreign jurisdictions or financial institutions, if it determines that such jurisdictions, financial institutions, types of transactions or accounts are of primary money laundering concern. For additional guidance, please refer to Section 311 – Special Measures section.
- **Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts**
  - Section 312 requires special due diligence for correspondent accounts, private banking accounts maintained for non-U.S. persons and senior foreign political figures, also known as politically exposed persons (PEPs). Section 312 creates EDD standards for correspondent accounts maintained for a foreign bank operating (a) under an offshore banking license, (b) under a license issued by a country that has been designated as being non-cooperative with international AML/CFT principles or procedures by an intergovernmental group or organisation with which the United States agrees, or (c) under a license issued by a country subject to a Special Measure order as authorised by Section 311. Section 312 creates EDD standards for private banking customers defined as (a) accounts with a minimum aggregate deposit of funds or assets of not less than US$1 million, (b) established for or on behalf of non-U.S. persons, and (c) are administered or managed by an officer or employee acting as a liaison between the financial institution and the direct or beneficial owner of the account(s). Additionally, covered financial institutions are required to obtain beneficial ownership information under certain circumstances for correspondent banking and private banking customers. For additional guidance, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Senior Foreign Political Figures.
- **Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks**
  - Section 313 prevents financial institutions from establishing, maintaining, administering or managing correspondent accounts in the United States for foreign shell banks (i.e., a foreign bank that does not have a physical presence in any country or jurisdiction). Additionally, this section requires financial institutions to take reasonable steps to ensure that any correspondent accounts provided to a foreign

respondent are not being used by that foreign respondent to provide banking services indirectly to a foreign shell bank. Foreign shell banks affiliated with the following type of institution are exempt from this prohibition: banks that maintain a physical presence and are subject to banking authorities in their respective countries. For additional guidance, please refer to Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks section.

- **Section 314 – Cooperative Efforts to Deter Money Laundering**
  - Sections 314(a) and 314(b) establish procedures that encourage information sharing between governmental authorities and financial institutions, and among financial institutions, respectively. Section 314(a) establishes a mechanism for law enforcement agencies to communicate the names of suspected money launderers and terrorists to financial institutions in return for securing the ability to locate accounts and transactions involving those suspects promptly. Similarly, Section 314(b) enables financial institutions to share information relating to suspected money launderers and/or terrorists among themselves. For additional guidance, please refer to Section 314 – Cooperative Efforts to Deter Money Laundering section.
- **Section 315 – Inclusion of Foreign Corruption Offenses as Money Laundering Crimes**
  - Section 315 includes multiple offenses such as money laundering crimes, including, but not limited to, the following:
    - Bribery of a public official or the misappropriation, theft or embezzlement of public funds by or for the benefit of the public official;
    - Smuggling or export control violations related to certain goods (e.g., items on the U.S. Munitions list pursuant to the Arms Export Control Act of 1976 (AECA);
    - Any felony violations of the Foreign Corrupt Practices Act of 1977 (FCPA);
    - Any felony violations of Foreign Agents Registration Act of 1938 (FARA);
    - An offense with respect to multilateral treaties in which the United States would be obligated to extradite the offender or submit the case for prosecution if the offender were found in the United States.
  - For further guidance, please refer to the sections: Senior Foreign Political Figure, Anti-Bribery and Corruption Compliance Programs and Foreign Corrupt Practices Act.
- **Section 317 – Long-arm Jurisdiction Over Foreign Money Launderers**
  - Section 317 outlines the jurisdiction of the United States over foreign persons if:
    - The offense involves a financial transaction that occurred (in whole or in part) in the United States;

        - The foreign person converts property in which the United States has an ownership interest by an order of forfeiture by a U.S. court; or
        - The foreign person maintains a correspondent account in the United States.

- **Section 318 – Laundering Through a Foreign Bank**
    - Section 318 amends "financial institution" to include "foreign bank" as defined by the International Banking Act of 1978 (IBA).
- **Section 319 – Forfeiture of Funds in U.S. Interbank Accounts**
    - Section 319(a) provides for seizure by U.S. authorities of funds in U.S. interbank accounts. If funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a U.S. bank, broker-dealer or branch or agency of that foreign bank, the funds are deemed to have been deposited in the U.S. interbank account and are potentially subject to seizure. There is no requirement that the funds deposited in the U.S. interbank account be traceable to the funds deposited in the foreign bank.
    - Section 319(b) requires that financial institutions reply to a request for information from a U.S. regulator relating to AML/CFT compliance within 120 hours of such a request. Upon receipt of a written request from a federal law enforcement officer for information required to be maintained under Section 319(b), that information must be provided within seven days. Section 319(b) also requires U.S. depository institutions and securities broker-dealers that have correspondent accounts in the United States for foreign respondents to maintain records identifying the owners of the foreign respondent, and to maintain the name and address of a person who resides in the United States and is authorised to accept service of legal process for records regarding the correspondent account.
    - Section 319(d) outlines the authority of the United States to order convicted criminals to return property located abroad (e.g., forfeiture of substitute property, return of property to the jurisdiction of the court, repatriate and deposit forfeited or seized property/funds). Failure to comply may result in enhanced sentencing (e.g., under the obstruction of justice provision).
    - For additional guidance, please refer to Section 319 - Forfeiture of Funds in United States Interbank Accounts, 120-Hour Rule and Foreign Bank Certifications sections.
- **Section 320 – Proceeds of Foreign Crimes**
    - Section 320 amends U.S. forfeiture law to include property "constituting, derived from, or traceable to" proceeds from an offense (1) against a foreign nation or (2) involves a controlled substance (e.g., as defined by the Controlled Substances Act of 1970 [CSA]), which would be punishable within the foreign jurisdiction by death or imprisonment of one year or more, and would be punishable under the laws of the

United States by imprisonment of one year or more if the offense occurred in the United States.

- **Section 323 – Enforcement of Foreign Judgments**
  - Section 323 amends U.S. forfeiture law by including violations of foreign law that also would be a violation under U.S. law for which property could be forfeited. It also outlines conditions in which a U.S. court may issue a restraining order to preserve forfeited property at the request of a foreign government.
- **Section 325 – Concentration Accounts at Financial Institutions**
  - Section 325 authorises the Secretary of the U.S. Department of the Treasury to issue regulations concerning the maintenance of concentration accounts by U.S. depository institutions, with the purpose of preventing an institution's customers from anonymously directing funds into or through such accounts. (While the U.S. Department of the Treasury is authorised to issue such regulations, it is not required to do so, and has not done so at this time.) For additional guidance, please refer to Section 325 – Concentration Accounts at Financial Institutions.
- **Section 326 – Verification of Identification**
  - Section 326 requires the U.S. Department of the Treasury, along with each federal functional regulator, to prescribe a Customer Identification Program (CIP) with minimum standards for (a) verifying the identity of any person opening an account, (b) maintaining records of the information used to verify the person's identity, and (c) determining whether the person appears on any list of known or suspected terrorists or terrorist organisations. The requirement to establish a CIP is applicable only to certain types of financial institutions, as explained in the section on CIP. For additional guidance on CIP requirements, please refer to Section 326 – Verification of Identification section. For additional guidance on lists of suspected terrorists, please refer to the Counter Terrorism Sanctions Program section.
- **Section 328 – International Cooperation on Identification of Originators of Wire Transfers**
  - Section 328 requires the Secretary of the U.S. Department of the Treasury, in consultation with the U.S. Attorney General and the Secretary of the State Department, to encourage foreign governments to require (1) the inclusion of the name of the originator in wire transfers and (2) that information travels with the wire transfer until the point of disbursement. For further guidance on recordkeeping requirements for funds transfers, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.
- **Section 330 – International Cooperation in Investigations of Money Laundering, Financial Crimes and the Finances of Terrorist Groups**

- Section 330 directs the Secretary of the U.S. State Department, the U.S. Attorney General, the Secretary of the U.S. Department of the Treasury, and as appropriate, the Board of Governors of the Federal Reserve System to develop cooperative mechanisms (e.g., voluntary information exchange, letters rogatory, mutual legal assistance treaties) with foreign countries in the international effort to combat money laundering, terrorist financing and other financial crimes. For further guidance, please refer to the International Perspectives and Initiatives section.

- **Section 351 – Amendments Relating to Reporting of Suspicious Activities**
  - Section 351 clarifies the terms of the Safe Harbor from civil liability for financial institutions filing Suspicious Activity Reports (SARs). This protection does not apply if an action against an institution is brought by a government entity nor when a SAR is filed maliciously. Additionally, a bank, and any director, officer, employee or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency with jurisdiction, including a disclosure made jointly with another institution involved in the same transaction, shall be protected under the Safe Harbor provision. For additional guidance, please refer to the Safe Harbor section.

- **Section 352 – Anti-Money Laundering Programs**
  - Section 352 requires financial institutions to establish AML Programs and grants the Secretary of the U.S. Department of the Treasury authority to set minimum standards for such programs. Current minimum standards for AML Programs include:
    - Development of internal AML policies, procedures and controls
    - Designation of an AML Compliance Officer
    - An ongoing employee AML Training Program
    - Independent testing of AML Programs

  For additional guidance, please refer to Section 352 – AML Program.

- **Section 353 – Penalties for Violations of Geographic Targeting Orders and Certain Recordkeeping Requirements, and Lengthening Effective Period of Geographic Targeting Orders**
  - Section 353 clarifies that penalties for violation of the BSA and its implementing regulations also apply to violations of Geographic Targeting Orders (GTOs) issued by the U.S. Department of the Treasury and to certain recordkeeping requirements relating to funds transfers. For additional guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.

- **Section 355 – Authorisation to Include Suspicions of Illegal Activity in Written Employment References**

- Section 355 permits, but does not require, an insured depository institution to include information about the possible involvement of a current or former institution-affiliated party in potentially unlawful activity in response to a request for an employment reference by a second insured depository institution. If, however, such disclosure is done maliciously, there is no shield from liability.

- **Section 356 – Reporting of Suspicious Activities by Securities Brokers and Dealers; Investment Company Study**
  - Section 356(a) directs the Secretary of the U.S. Department of the Treasury to publish regulations requiring broker-dealers to file SARs. For additional guidance, please refer to the Suspicious Activity Reports and Broker-Dealers in Securities sections.

- **Section 358 – Bank Secrecy Provisions and Activities of United States Intelligence Agencies to Fight International Terrorism**
  - Section 358 expands the purpose and use of BSA information to include combating acts of international terrorism and permits disclosures of BSA information to governmental agencies for counterterrorism purposes.

- **Section 359 – Reporting of Suspicious Activities by Underground Banking Systems**
  - Section 359 amends the BSA definition of money transmitter to include underground banking systems or informal value transfer systems (IVTSs) in the definition of financial institution and thus subject to AML/CFT laws and regulations. For additional guidance on underground banking systems, please refer to the Informal Value Transfers Systems section.

- **Section 360 – Use of Authority of the United States Executive Directors**
  - Section 360 outlines the authority of the President to instruct the U.S. Executive Directors of international financial institutions (e.g., multilateral institutions such as the International Monetary Fund [IMF], the International Bank for Reconstruction and Development [IBRD], and the European Bank for Reconstruction and Development [EBRD]) to use its "voice and vote" to provide support in combating acts of international terrorism (e.g., provision of loans or utilisation of funds to combat international terrorism, auditing of disbursements to ensure funds are not used to pay persons committing or supporting terrorism).

- **Section 361 – Financial Crimes Enforcement Network**
  - Section 361 outlines the duty and powers of the Financial Crimes Enforcement Network (FinCEN). For further guidance, please refer to the Financial Crimes Enforcement Network section.

- **Section 362: Establishment of a Highly Secure Network**

- Section 362 requires the establishment of a secure network to facilitate information sharing and communication between FinCEN and financial institutions (e.g., filing required reports electronically, broadcasting industry alerts).

- **Section 363 – Increase in Civil and Criminal Penalties for Money Laundering**
  - Section 363 increases from US$100,000 to US$1 million, the maximum civil and criminal penalties for a violation of provisions added to the BSA, which was adjusted for inflation by the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Inflation Adjustment Act) from US$133,842 to US$1,338,420, with adjustments scheduled to occur every five years.

- **Section 365 – Reports Relating to Coins and Currency Received in Nonfinancial Trade or Business**
  - Section 365 amends the requirement for businesses that receive more than US$10,000 in coins or currency from a customer, in one transaction or two or more related transactions in the course of that person's nonfinancial trade or business, to file a report (Form 8300) with respect to such transaction with FinCEN. Previously, nonfinancial businesses were required to report to the IRS; they now are required to report to both FinCEN and the Internal Revenue Service (IRS). Section 365 also expands the scope of Form 8300 to include foreign currency and monetary instruments as prescribed by the secretary of the Treasury Department. For additional guidance, please refer to Form 8300 section.

- **Section 371 – Bulk Cash Smuggling into or out of the United States**
  - Section 371 includes bulk cash smuggling as a criminal offense and authorises forfeiture of any cash or instruments of the smuggling offense. For further guidance, please refer to the Bulk Shipments of Currency and Bulk Cash Smuggling section.

- **Section 372 – Forfeiture in Currency Reporting Cases**
  - Section 372 authorises the seizure of all property (e.g. currency) involved in violations of currency reporting requirements (e.g., Currency Transaction Reports [CTRs], Reports of International Transportation of Currency or Monetary Instruments [CMIRs]).

- **Section 373 – Illegal Money Transmitting Businesses**
  - Section 373 prohibits the operation of an unlicensed money transmitter. For additional guidance, please refer to the Money Services Businesses section.

- **Section 505 – Miscellaneous National Security Authorities**
  - Section 505 expanded the use of National Security Letters (NSLs), allowing their use in scrutiny of U.S. residents, visitors and U.S. citizens who are not suspects in any criminal investigation. For additional guidance, please refer to Section 505 - Miscellaneous National Security Authorities.

526. Do all financial institutions have to comply with all provisions of the USA PATRIOT Act?

No. Not all provisions of the USA PATRIOT Act apply to all financial institutions. Requirements are generally determined by the type of financial institution and the nature of the services (e.g., products, transactions) it provides.

For further guidance, please refer to each USA PATRIOT Act section outlined above and the Nonbank Financial Institutions and Nonfinancial Businesses section.

527. Are foreign financial institutions subject to the requirements of the USA PATRIOT Act?

The requirements of the USA PATRIOT Act apply to the U.S. operations of foreign financial institutions (FFIs) in the same manner that they apply to domestic financial services companies. As a practical matter, however, non-U.S. offices of FFIs will find that they are directly and indirectly affected by USA PATRIOT Act requirements in their efforts to support the AML/CFT Compliance Programs of their U.S.-based operations, especially through correspondent banking relationships.

528. What is the applicability of the USA PATRIOT Act to foreign subsidiaries and branches of U.S. financial institutions?

Foreign subsidiaries and branches of U.S. financial institutions must comply with some, but not all, U.S. AML/CFT laws and regulations (e.g., Section 326). In addition, a foreign subsidiary or branch also must comply with the AML/CFT laws and regulations of the jurisdictions in which it operates. U.S. financial institutions with international operations, therefore, need to be aware of AML/CFT laws and regulations globally to ensure subsidiaries and branches operating outside of the United States are in compliance with host country AML/CFT regulations, as well as U.S. AML/CFT requirements.

529. Does the USA PATRIOT Act in any way impact non-U.S. financial institutions without a U.S. presence?

Even though the specific requirements of the USA PATRIOT Act are not applicable to FFIs that operate exclusively outside of the United States, the USA PATRIOT Act, nonetheless, has a significant impact on financial institutions across the globe.

Specifically, Sections 311, 312, 313, 314, 319, 323, 326, 328, 330 and 352 of the USA PATRIOT Act can have significant effects on non-U.S. financial institutions. Many of these sections are discussed in further detail below. In summary, these requirements could result in the following:

- Additional information requests about the financial institution itself and its customers if their transactions are processed through a U.S. financial institution
- Seizures of a financial institution's funds maintained in an account in the United States
- Sanctions against either the financial institution itself or the country from which it operates

These measures are far-reaching; global financial institutions must be aware of their potentially significant impact.

USA PATRIOT Act – Analysis of Key Sections

Section 311 – Special Measures

530. What requirements does Section 311, Special Measures, impose on financial institutions?

Section 311 provides the U.S. Department of the Treasury broad authority to impose one or more of five Special Measures against foreign jurisdictions, foreign financial institutions (FFIs), classes of international transactions or types of accounts, if it determines that such jurisdictions, financial institutions, transactions or accounts are of primary money laundering concern. These Special Measures require a range of responses, from information requirements to outright prohibitions. They are as follows:

- **First Measure**: Additional recordkeeping and reporting of certain financial transactions
- **Second Measure**: The collection of information relating to beneficial ownership of accounts
- **Third Measure**: The collection of information relating to certain payable-through accounts (PTAs)
- **Fourth Measure**: The collection of information relating to certain correspondent accounts
- **Fifth Measure**: The prohibition or imposition of conditions on opening or maintaining correspondent or payable-through accounts (PTAs) and notifying foreign respondents of applicable restrictions

Section 311 is implemented for depository institutions under 31 C.F.R. 1010.650 – Special Measures under Section 311 of the USA PATRIOT Act and Law Enforcement Access to Foreign Bank Records.

531. What companies are required to comply with Special Measures orders?

Domestic financial institutions and domestic financial agencies and branches are required to comply with Special Measures orders, unless exempted by the order. Offices of foreign financial institutions operating in the United States are required to comply with Special Measures orders as with all domestic financial institutions.

532. Who imposes a Special Measures order, and what is the process?

The U.S. Department of the Treasury must follow a formal rulemaking process (a) before concluding that foreign jurisdictions, foreign financial institutions, classes of international transactions or types of accounts are of primary money laundering concern, and (b) when selecting the specific measures to be imposed against the foreign jurisdictions, foreign financial institutions, classes of international transactions or types of accounts.

FinCEN collects and disseminates information relating to Section 311 and serves as the main point of contact for inquiries.

533. What factors must the U.S. Department of the Treasury consider before making a Special Measure designation?

The Secretary of the U.S. Department of the Treasury is required to consult with appropriate federal agencies and consider the following specific factors:

- Whether similar action has been or is being taken by other nations or multilateral groups;
- Whether the imposition of any particular special measures would create a significant competitive disadvantage, including any undue cost or burden associated with compliance, for financial institutions organised or licensed in the United States;
- The extent to which the action or timing of the action would have a significant adverse system impact on the international payment, clearance and settlement system, or on legitimate business activities involving the jurisdiction; and
- The effect of the action on the national security and foreign policy of the United States.

Where concerns extend beyond money laundering and involve terrorist financing and weapons proliferation, the secretary of the U.S. Department of the Treasury is required to consider the following additional factors:

- Evidence that organised criminal groups, international terrorists, or entities involved in the proliferation of weapons of mass destruction (WMDs) or missiles, have transacted business in the jurisdiction;
- The extent to which that jurisdiction or financial institutions operating in that jurisdiction offer bank secrecy or special regulatory advantages to non-residents or nondomiciliaries of the jurisdiction;
- The substance and quality of administration of the bank supervisory and counter money laundering laws of the jurisdiction;
- The relationship between the volume of financial transactions occurring in that jurisdiction and the size of the economy of the jurisdiction;
- The extent to which that jurisdiction is characterised as an offshore banking or secrecy haven by credible international organisations or multilateral groups;
- Whether the United States has a mutual legal assistance treaty with that jurisdiction, and the experience of U.S. law enforcement officials and regulatory officials in obtaining information about transactions originating in or routed through or to such jurisdiction; and
- The extent to which that jurisdiction is characterised by high levels of official or institutional corruption.

534. Are Special Measures designations permanent?

Special Measures orders requiring information gathering and/or recordkeeping (e.g., collection of information relating to beneficial ownership of accounts) may not remain in effect for more than 120

days unless imposed by a regulation. In addition, the U.S. Department of the Treasury may rescind Special Measures orders (both information gathering/recordkeeping and prohibitions) if it determines that circumstances supporting the designation as primary money laundering concern no longer exist. At the time of this publication, the U.S. Department of the Treasury has, in fact, rescinded at least seven Special Measures orders.

535. How can a financial institution obtain the most current listing of Special Measure orders?

The U.S. Department of the Treasury's proposed and final Special Measures orders can be found at https://www.fincen.gov.

536. How can a financial institution screen its customer base and transactions for foreign jurisdictions or foreign financial institutions that are the subject of a Special Measures order?

Many financial institutions add subjects of Special Measures orders to their sanction interdiction software to automate the screening process for both customers and transactions.

To enlist respondents in this countermeasure, financial institutions are required to contact their correspondent account holders to inform them of Special Measures orders to screen for Special Measures subjects to prevent direct/indirect use of their correspondent accounts.

For additional guidance on interdiction software, please refer to the Customer and Transaction List Screening section.

537. Should a financial institution terminate its correspondent relationship with an entity that is the subject of a proposed Special Measure order?

A financial institution is not obligated to terminate a correspondent relationship with an entity that is the subject of a proposed Special Measures order, unless required by the specific Fifth Measure. Regardless, financial institutions may wish to conduct due diligence on the entity and determine if they want to continue the relationship even before a final rule imposing the Special Measures order is issued.

538. What should a financial institution do if a match to a subject of a Special Measures order is confirmed?

Financial institutions should consult the final order on the entity and follow the instructions exactly as written; requirements differ among final orders. A financial institution also may contact the FinCEN hotline with questions.

539. What are some examples of recordkeeping and reporting requirements under the First Measure?

Under the First Measure, financial institutions may be required to maintain records and file reports on transactions involving Special Measures designees that include the following information:

- Transaction details (e.g., amount, type, participants in transaction(s))
- Legal capacity of Special Measures designee in the transaction (e.g., by or on behalf of the beneficiary)
- Purpose of transaction(s)

540. Does the independent filing of a SAR satisfy the reporting requirements under the First Measure?

If an independently filed SAR includes the required information as outlined in the First Measure, it satisfies the reporting requirement of the First Measure. For further guidance on SARs, please refer to the Suspicious Activity Reports section.

541. If no reportable activity occurs under SAR filing requirements, are financial institutions still obligated to file SARs to report information pursuant to Special Measures information requests?

If no reportable activity (e.g., lack of suspicious activity, under reportable monetary threshold) occurred under SAR filing requirements, a financial institution is not obligated to file a SAR pursuant to Special Measures information requests.

542. Beyond termination, what other actions must financial institutions take to comply with the Fifth Measure?

To block a Special Measures designee's ability to gain indirect access to the U.S. financial system through a third-party correspondent banking relationship, a financial institution is required to notify its other respondents of its obligations to restrict access to the designee in their own accounts.

543. Do the notification requirements apply to U.S. offices of foreign banks?

No. U.S. offices of foreign banks are considered U.S. institutions whose notice is provided by the issuance of the Special Measures designation.

544. Are Special Measures orders imposed frequently?

Since 2002, the Treasury Department has invoked Special Measures fewer than 25 times, and subsequently rescinded several orders. Proposed and final Special Measures orders can be found at www.fincen.gov/resources/statutes-and-regulations/311-special-measures.

545. Has there been litigation with respect to implemented Special Measures orders?

Yes. In 2015, FBME Bank Ltd., formerly known as the Federal Bank of the Middle East Ltd., filed a lawsuit and ultimately won, alleging that FinCEN's Special Measures issued against FBME Bank Ltd. in 2014 violated the U.S. Administrative Procedures Act (APA). FBME alleged the following:

- FBME Bank Ltd. did not receive ample notice of the pending Special Measures order;
- Information leading to the ultimate imposition of the Special Measures was not disclosed;

- Information that could have proved that the Special Measures order was not warranted was not considered; and
- Other, less punitive actions were not considered as an alternative to the fifth Special Measures order.

Ultimately, FinCEN reopened comments on its 2014 Special Measures order against FBME Bank Ltd. to correct procedural deficiencies and reissued the final order in March 2016.

546. Is FinCEN required to disclose its reasoning behind the issuance of a Special Measures order?

FinCEN is not required to disclose classified information used to make the determination to issue a Special Measures order. However, under the APA, FinCEN is required to disclose non-classified non-privileged information supporting its rulemaking to allow for targeted financial institutions to respond before the issuance of the final rule.

547. Are Special Measures orders similar to sanctions administered by the Office of Foreign Assets Control (OFAC)?

The OFAC Sanctions Programs invoke stronger measures to reject and block the property and interests of designees. While some Special Measures may require the termination of a correspondent banking relationship with a designee, in general, there are no rejecting or blocking provisions, only recordkeeping and reporting requirements, unless explicitly required by the specific Special Measure. Designations under Section 311 can be incorporated into the existing screening process of an OFAC Sanctions Compliance Program, however, the required actions of financial institutions differ on confirmed matches.

The choice to use Special Measures versus the stronger OFAC sanctions is primarily dependent upon the perceived threat of the target and the internal decision making processes of the authority enacting the action. Sometimes the decision to use one tool over the other is not clear to members outside of the decision making process. For example, the fifth Special Measure was ordered and required U.S. financial institutions to deny North Korean financial institutions access to the U.S. financial system by requiring U.S. institutions to do the following:

- Conduct due diligence on their correspondent accounts to prevent indirect access by North Korean financial institutions, and
- Notify their foreign respondents of the prohibition on providing North Korean financial institutions access to their correspondent accounts.

To some, the effort to deny North Korean financial institutions access to the U.S. financial system could have been achieved more effectively by designating the targets subject to OFAC blocking/rejecting sanctions. The primary objective of the current North Korean Sanctions Program is to restrict and eliminate the existence and risk of the proliferation of weapons of mass destruction (WMDs) and weapons-usable fissile material on the Korean Peninsula by sanctioning the following types of targets:

- Importers/exporters of arms or related materials that contribute to the manufacturing, delivery or proliferation of WMDs;
- North Korean Government agencies and officials; and
- Worker's Party of Korea officials.

One reason the Fifth Special Measure may have been used on North Korean financial institutions over sanctions is their extensive use of aliases and front companies. Aliases and front companies would make it difficult to maintain accurate lists of designees and render interdiction software used to screen for these names ineffective. In June 2017, the Fifth Special Measure was applied to China's Bank of Dandong for alleged illicit financial ties to North Korea. For further guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts

Overview

548. What are the key provisions of Section 312, Special Due Diligence for Correspondent Accounts and Private Banking Accounts?

Section 312 requires special due diligence for correspondent accounts, private banking accounts maintained for non-U.S. persons and senior foreign political figures, also known as politically exposed persons (PEPs). Section 312 creates EDD standards for correspondent accounts maintained for a foreign bank operating (a) under an offshore banking license, (b) under a license issued by a country that has been designated as being non-cooperative with international AML/CFT principles or procedures by an intergovernmental group or organisation with which the United States agrees, or (c) under a license issued by a country subject to a Special Measure order as authorised by Section 311.

Section 312 creates EDD standards for private banking customers defined as (a) accounts with a minimum aggregate deposit of funds or assets of not less than US$1 million, (b) established for or on behalf of non-U.S. persons, and (c) are administered or managed by an officer or employee acting as a liaison between the financial institution and the direct or beneficial owner of the account(s).

Additionally, covered financial institutions are required to obtain beneficial ownership information under certain circumstances for correspondent banking and private banking customers.

549. What does the term "correspondent account" mean for Section 312 purposes?

The term "correspondent account" is defined broadly for banking organisations to include any account or formal relationship established by a financial institution to receive deposits from, make payments to or other disbursements on behalf of a foreign financial institution, or to handle other financial transactions related to the foreign financial institution.

Section 312's correspondent banking due diligence requirements for depository institutions are implemented under 31 C.F.R. 1010.610 – Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions. The regulation defines "correspondent account" as follows:

- "An account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution; or
- An account established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank."

In the case of securities broker-dealers, FCMs and IBs in commodities, and mutual funds, a correspondent account would include, but not be limited to, any account or formal relationship that permits the foreign financial institution to engage in regular services, including, but not limited to, those established to engage in trading or other transactions in securities and commodity futures or options, funds transfers or other types of financial transactions.

550. What is a correspondent clearing account? Does it fall under the USA PATRIOT Act's definition of a correspondent account?

Though the terms often seem to be used as synonyms, correspondent clearing accounts and correspondent accounts are not the same. A correspondent clearing account is one type of correspondent account and, as such, it does fall under the USA PATRIOT Act's definition of correspondent account. Correspondent clearing accounts are accounts maintained on behalf of another financial institution through which that financial institution processes or clears transactions on behalf of third parties. One example of a correspondent clearing account is a U.S. dollar clearing account maintained in the U.S. on behalf of an affiliated or third party FFI.

551. What is the purpose of correspondent banking?

Correspondent banking allows institutions to conduct business and provide services to their customers without the expense of a physical presence in a jurisdiction. It also allows institutions to expand their portfolio of products and services by offering the products and services of the correspondent to the respondent's customers.

552. What is the heightened money laundering and terrorist financing risk of correspondent accounts?

Correspondent banking relationships may expose the U.S. financial system to heightened money laundering and terrorist financing risk if they are established for foreign financial institutions (FFIs) located in jurisdictions with non-existent or weak AML/CFT laws and regulations. Additionally, correspondent banking involves high-volume, international transactions involving multiple parties in which no one institution may have a direct relationship with all parties involved nor have a complete view of the entire transaction.

553. Which financial institutions must comply with Section 312, Special Due Diligence for Correspondent Accounts and Private Banking Accounts?

The following financial institutions must comply with the correspondent banking, private banking and senior foreign financial official provisions of Section 312, including the requirement to obtain

beneficial ownership information on correspondent banking and private banking accounts under certain circumstances:

- Banks (including U.S. branches and agencies of foreign banks)
- Broker-dealers in securities
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Mutual funds
- Uninsured trust banks or trust funds that are federally regulated and subject to AML Program requirements
- Certain other entities

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM), "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator," that would expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to, the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations
- State-chartered non-depository trust companies
- International banking entities

554. What does the term "regular" mean for Section 312 purposes?

The term "regular" is not defined in the regulation; however, it suggests an arrangement for providing ongoing services and generally would exclude infrequent or occasional transactions. Some institutions use a standard of more than one transaction per quarter.

555. What is the difference between a correspondent bank and a respondent bank?

A "correspondent bank" (correspondent) is the financial institution providing the banking services. A "respondent bank" (respondent) is the financial institution utilising these account services, whether foreign or domestic. A "correspondent account" generally refers to the account held by the respondent bank at a correspondent bank. "Correspondent banking services" generally refers to the many types of financial services correspondent banks offer to respondent banks.

556. Are accounts with domestic financial institutions included in the USA PATRIOT Act's definition of a correspondent account?

No. The money laundering and terrorist financing risk associated with these relationships is not considered as high as those associated with foreign respondents because the domestic financial

institutions are subject to the same regulatory regime. Financial institutions should, however, have appropriate risk-based policies, procedures and controls to manage the money laundering and terrorist financing risks involved with their domestic respondents.

557. Do accounts maintained for foreign affiliates fall under the definition of correspondent accounts?

Yes. Accounts maintained by a financial institution's non-U.S. branches or offices fall under the definition of a correspondent account. Regardless of affiliation, the monitoring of activity and other due diligence procedures should be applied consistently to affiliate and non-affiliate financial institutions.

558. What types of services fall under the definition of correspondent banking services?

Correspondent banking services include, but are not limited to:

- Cash management services, including deposit accounts
- Payable-through accounts (PTAs)
- Check clearing services
- Foreign exchange services
- International funds transfers
- Pouch activities (or cash letters)
- Bulk cash activities
- U.S. Dollar drafts
- Trade finance services (e.g., letters of credit [confirmed/advised])
- Credit services (e.g., syndicating or agenting loans)
- Investment management (e.g., investment advisers, overnight investment accounts [sweep accounts])

Correspondent accounts for broker-dealers include, but are not limited to, the following:

- Accounts to purchase, sell or lend securities (e.g., securities repurchase agreements)
- Prime brokerage accounts
- Accounts trading foreign currency
- Over-the-counter derivatives contracts
- Custody accounts holding settled securities as collateral

To the extent that FCMs, IBs and mutual funds maintain correspondent accounts, they are required to comply with Section 312.

559. As customers, do all correspondent banking customers pose the same degree of risk?

No. The risks of each correspondent banking customer should be assessed based on a variety of factors, including, but not limited to, the following:

- The nature of, and markets served by, the foreign respondent's business
- The type, purpose and anticipated activity of the foreign respondent's account
- The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
- The owners and senior management of the respondent are identified as politically exposed persons (PEPs) or as close associates of PEPs
- The AML/CFT and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent
- The AML/CFT and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available)
- Information known or reasonably available about the foreign respondent's AML/CFT record

Evaluating the risks of correspondent banking customers in this manner will result in different risk ratings (e.g., low, moderate, high).

560. What does the term "payable-through account" (PTA) mean for Section 312 purposes?

A PTA, also known as a "pass through" or "pass-by" account, is an account maintained for a respondent that permits the respondent's customers to engage, either directly or through a subaccount, in banking activities (e.g., check writing, making deposits) usually in the United States. For additional guidance, please refer to the Payable-Through Accounts section.

561. What is the difference between PTAs and other correspondent clearing accounts?

In traditional correspondent clearing accounts, customers of respondents do not have the authority to transact through the respondent's account on their own. To send or receive funds through the respondent's account, the customer must send instructions to the respondent so the respondent can transact on behalf of the customer. In short, with PTAs, customers of the respondent have direct access to the account.

562. What are the heightened money laundering and terrorist financing risks of PTAs?

PTAs do provide legitimate business benefits, but the operational aspects of the accounts make them particularly vulnerable to abuse as a mechanism to launder money as multiple individuals can have signatory authority over a single correspondent account and, therefore, can conduct transactions anonymously. Often, PTA arrangements are with financial institutions and customers in less-regulated financial markets. Unless a financial institution is able to identify adequately and understand the transactions of the ultimate users of the respondent bank's account, there is a significant potential money laundering and terrorist financing risk.

563. When should financial institutions consider terminating PTAs?

Because they present a heightened risk of money laundering and terrorist financing, financial institutions that offer PTAs must have adequate resources and controls in place to manage the risks.

Financial institutions should consider terminating PTAs in situations including, but not limited to, the following:

- Adequate information about the ultimate users of the PTAs cannot be obtained
- Weak AML/CFT regulations and controls regarding customer identification and transaction monitoring exist in the jurisdiction of the foreign bank itself
- Ongoing suspicious and unusual activities occur in the PTA
- The financial institution is unable to conclude that PTAs are not being used for illicit purposes

564. How is the term "pouch activity" defined?

Pouch activity, also known as "pouch services" or "cash letters," entails the use of a courier to transport currency, monetary instruments, loan payments and other financial documents to a financial institution.

Pouches can be sent by another financial institution or by an individual and are commonly offered in conjunction with correspondent banking services. For additional guidance, please refer to the Pouch Activity section.

565. Is the term "pouch activity" limited to the transport of financial documents from a foreign country to a financial institution in the United States?

No. Pouch activity can be offered to domestic and foreign individuals and institutions. The risk is heightened for pouches received from countries with lax or deficient AML/CFT regimes.

566. What are bulk cash activities?

Bulk cash activities entail the use of common, independent or U.S. Postal Service carriers to transport large volumes of currency or bank notes (U.S. or foreign) from sources inside or outside the United States to a bank in the United States. For further guidance, please refer to the section Bulk Shipments of Currency and Bulk Cash Smuggling.

567. Are there other specific AML/CFT requirements for correspondent banking and PTAs beyond those required by Section 312?

Yes. In addition to Section 312, financial institutions may be required to comply with the following:

- Under Section 311, the Fifth Measure restricts or prohibits the provision of correspondent banking and PTA services to financial institutions designated as a money laundering concern. For further guidance, please refer to the Section 311 – Special Measures section.

- Section 313 prohibits U.S. financial institutions from establishing correspondent banking relationships with foreign shell banks. For further guidance, please refer to Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks.
- Section 319 outlines circumstances in which funds can be seized from a U.S. interbank account; requirements to retrieve bank records of foreign respondents within "120 hours"; and "foreign bank certification" requirements of foreign respondents (e.g., certifies physical presence, regulated status, prohibition of indirect use of correspondent accounts by foreign shell banks). For further guidance, please refer to Section 319 – Forfeiture of Funds in U.S. Interbank Accounts.
- Although regulations have not been issued, Section 325 outlines restrictions on the use of concentration accounts to prevent abuse similar to that conducted through correspondent banking accounts. For further guidance, please refer to Section 325 – Concentration Accounts at Financial Institutions.
- Some OFAC Sanctions Programs restrict or prohibit the provision of correspondent banking and PTA services to designated entities (e.g., Iranian-linked financial institutions, financial institutions providing services to persons on the Specially Designated Nationals and Blocked Persons List [SDN List]). For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

568. How do Section 312 requirements for correspondent banking and PTAs correspond to FATF Recommendations?

FATF addresses correspondent banking and PTAs in the following recommendations:

- **Recommendation 13 – Correspondent Banking** – FATF recommends financial institutions implement measures to mitigate the risks of cross-border correspondent banking and PTAs, including, but not limited to, the following:
  - Risk-based due diligence program to understand the nature of the respondent's business; the respondent's AML/CFT Compliance Program, especially as it relates to PTAs; and the respondent's public history of money laundering or terrorist financing investigations or regulatory actions;
  - Requiring senior management approval for new correspondent banking relationships; and
  - Prohibiting establishing correspondent banking relationships with shell banks.
- **Recommendation 19 – Higher Risk Countries** – FATF recommends financial institutions implement enhanced measures for correspondent banking relationships in high-risk countries (e.g., more frequent monitoring, termination).

As outlined above, U.S. AML/CFT requirements for correspondent banking and PTAs are comprehensive and consistent with FATF Recommendations.

For further guidance on international standards, please refer to the Financial Action Task Force section.

569. What international efforts have been made to collect and share due diligence information on correspondent banks?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) has developed a KYC Registry that collects correspondent banking due diligence information and documentation submitted by financial institutions in accordance with international best practices (e.g., Wolfsberg AML Principles for Correspondent Banking). The KYC Registry aims to create a global standard from a single validated source to ease the complex and often inconsistent due diligence standards for correspondent banking. Examples of due diligence and documents maintained by the KYC Registry include, but are not limited to, the following:

- Banking licenses
- Corporate governance documents (e.g., bylaws, articles of incorporation)
- Foreign bank certifications as required by Section 319 of the USA PATRIOT Act
- AML/CFT Policies and Procedures related to correspondent banking services

Participation in the registry is voluntary.

570. What guidance and information have been issued on correspondent banking?

Among the key guidance and information issued on correspondent banking are the following:

- **Correspondent Banking – Overview (Domestic and Foreign)** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 13: Correspondent Banking** (2012) by the Financial Action Task Force (FATF)
- **Wolfsberg AML Principles for Correspondent Banking** (2014) by the Wolfsberg Group of Banks (Wolfsberg Group).
- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2014) by the Wolfsberg Group
- **Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking (Exposure Draft**) (2014) by The Clearing House
- **Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism** (2017) (includes revisions to Annex II – Correspondent Banking and Annex IV – General Guide to Account Opening) by the Basel Committee on Banking Supervision
- **Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking** (2002) by The Clearing House
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payment Messages** (2009) by the Wolfsberg Group

- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** (2009) by the International Finance Corporation (IFC), the private sector arm of the World Bank Group
- **Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment** (2008) by Financial Crimes Enforcement Network (FinCEN)
- **Application of the Correspondent Account Rule to Executing Dealers Operating in Over-the-Counter Foreign Exchange and Derivatives Markets Pursuant to Prime Brokerage Arrangements** (2007) by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** (2006) by FinCEN
- **Application of the Regulations regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts** (2006) by FinCEN
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers** (2008) by the Basel Committee on Banking Supervision of the Bank of International Settlements (BIS)
- **U.S. Senate Hearing on the Role of U.S. Correspondent Banking in International Money Laundering** (2001)
- **Senate Permanent Subcommittee Hearing on "U.S. Vulnerabilities to Money Laundering and Terrorist Financing: HSBC Case History"** (2012)

For additional guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks, Section 319 – Forfeiture of Funds in U.S. Interbank Accounts, Foreign Bank Certifications, and Section 311 – Special Measures.

Due Diligence for Correspondent Accounts

571. What types of foreign respondents are subject to the correspondent account due diligence requirements outlined in Section 312?

Section 312 applies to correspondent accounts maintained at the following:

- Foreign banks
- Foreign branch(es) of a U.S. bank
- Businesses organised under a foreign law that, if located in the United States, would be:
  - Broker-dealers in securities
  - Futures commission merchants (FCMs)
  - Introducing brokers (IBs) in commodities

- Mutual funds
- Money transmitters or dealers in foreign exchange

572. What are the general correspondent account due diligence requirements outlined in Section 312?

As part of its AML Program, a domestic correspondent must establish a due diligence program that includes appropriate, specific, risk-based and, where necessary, enhanced policies, procedures and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any correspondent account established, maintained, administered or managed in the United States for a foreign financial institution.

At minimum, the due diligence program must:

- Determine whether the account is subject to enhanced due diligence (EDD) under Section 312
- Assess the money laundering and terrorist financing risk posed, based on a consideration of relevant risk factors
- Apply risk-based policies, procedures and controls to each such respondent reasonably designed to detect and report known or suspected money laundering or terrorist financing activity. Controls should include a periodic review of the respondent's account activity to determine consistency with information obtained about the type, purpose and anticipated activity of the account

573. Can financial institutions rely upon a third party's due diligence for their correspondent banking relationships?

In instances where the parent company has effective control, financial institutions may be able to rely on due diligence conducted on the ultimate parent company in lieu of conducting individual assessments of each foreign branch, subsidiary or affiliate. However, financial institutions must consider unique factors of each branch, subsidiary or affiliate when determining if reliance is appropriate.

574. What steps should a financial institution take if it cannot perform the appropriate due diligence?

Section 312 states that a financial institution's due diligence program should include procedures to be followed in circumstances where due diligence cannot be performed. These procedures should detail the circumstances when the financial institution should file a Suspicious Activity Report (SAR), and when it should refuse to open the account, suspend transaction activity and close the account.

575. Does Section 312 provide guidance as to what relevant risk factors should be considered when assessing the money laundering and terrorist financing risks of foreign respondents?

Yes. Section 312 provides the following factors that should be considered:

- The nature of, and markets served by, the foreign respondent's business

- The type, purpose and anticipated activity of the foreign respondent's account
- The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
- The AML/CFT and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent
- The AML/CFT and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available)
- Information known or reasonably available about the foreign respondent's AML/CFT record

576. Are there any particular challenges to monitoring correspondent clearing activity?

One of the most difficult challenges to effective monitoring of correspondent clearing activity is determining the reasonableness of transactions conducted by customers of the respondent. This requires understanding the nature of the services provided by the respondent and the customer base of the respondent and determining what additional research or information is necessary for the adequate review of activity.

577. Do the new obligations of the "Customer Due Diligence Requirements for Financial Institutions" rule impact Section 312?

No. The Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule) requires covered financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership or significant control of legal entity customers.

Section 312 already required covered financial institutions to collect and verify beneficial owners for private banking customers and correspondent accounts for certain foreign financial institutions (FFIs) but at 10 percent or greater ownership or control.

For further guidance on the proposed rule, please refer to the Beneficial Owners section.

578. What are cover payments and how are they a challenge to monitoring correspondent clearing activity?

"Cover payments" are used in correspondent banking as a cost effective method of sending international transactions on behalf of customers. A cover payment involves several actions by financial institutions:

- Obtaining a payment order from the customer;
- Sending of a credit transfer message for an aggregate amount through a messaging network (e.g., Society for Worldwide Interbank Financial Telecommunication [SWIFT]) that travels a direct route from the originating bank to the ultimate beneficiary's bank;
- Execution of a funds transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message; and

- Disbursement of funds to the ultimate beneficiary in accordance with the credit transfer message.

Previous messaging standards did not include information on the ultimate originators and beneficiaries of cover payments. The lack of information posed a challenge for recordkeeping, suspicious activity monitoring and sanctions screening.

579. What is SWIFT's role in the international payments system?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the infrastructure supporting both global correspondent banking and most domestic payment systems and Real-Time Gross Settlement (RTGS) networks involving over 11,000 financial institutions (e.g., banks, broker-dealers, investment managers) in more than 200 countries and territories. Participants also include corporate as well as market infrastructures (settlement and clearing organisations) in payments, securities, treasury and trade.

Message types (MTs) are used to transmit financial information and instructions from one participating financial institution to another, also referred to as SWIFT FIN messages.

Oversight is provided by central banks, including the National Bank of Belgium, the Bank of England, the Bank of Japan and the U.S. Federal Reserve.

580. What enhancements were made to SWIFT's messaging with regard to cover payments?

MT 202s were occasionally used in lieu of the MT 103s, in part, because MT 202s were more cost-effective. Regardless of the reason, the substitution of a MT 202 for a MT 103 in a commercial transaction masked the underlying parties to a transaction, thereby frustrating attempts to comply with recordkeeping, monitoring and sanctions requirements.

To address this lack of transparency, in 2009, SWIFT developed a variant of the MT 202 payment message type, MT 202 COV, which allows all information contained in certain fields (e.g., originator and beneficiary information) of the MT 103 to be transmitted in the MT 202 COV and is to be used for cover payments in lieu of MT 202s. The MT 202 COV provides intermediary banks with additional originator and beneficiary information to perform sanctions screening and suspicious activity monitoring.

To further improve efficiency and transparency of cross-border payments, SWIFT developed a global payments innovation (GPI), a cloud-based payments tracking service that allows correspondents to see payments end-to-end throughout all legs of the transaction and meet regulatory requirements (e.g., KYC rules, sanctions screening, audit requests).

581. How can SWIFT messages be used to support suspicious transaction monitoring efforts?

Many SWIFT message types can be converted to a format for import into an AML/CFT suspicious transaction monitoring system.

For those SWIFT message types that cannot be converted, a manual review by AML/CFT investigators may be implemented to support investigations into potentially suspicious activity. For example, in the

case of transactions related to letters of credit (LCs), it is imperative that the AML/CFT investigators compare the transfer amount (listed in an analysable SWIFT message type) to the terms listed in the LC to determine whether the transaction(s) is/are potentially suspicious.

For further guidance on suspicious activity monitoring, please refer to the Transaction Monitoring, Investigations and Red Flags section.

582. How can SWIFT messages be used to support sanctions screening?

SWIFT messages contain payment information such as originators, intermediate beneficiaries, ultimate beneficiaries and multiple banks involved in the transfers. It is important that these fields be screened against government sanction lists (e.g., OFAC Sanctions Listings, U.N. Consolidated Lists).

For further guidance on screening software, please refer to the AML/CFT Technology section. For further guidance on sanctions programs, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

For further guidance on cover payments and SWIFT messages, please refer to the Cover Payments and SWIFT section.

Enhanced Due Diligence for Correspondent Accounts

583. Which types of accounts are subject to the enhanced correspondent account due diligence requirements outlined in Section 312?

Section 312 applies to correspondent accounts maintained for the following foreign financial institutions:

- Foreign banks operating under an offshore banking license
- Foreign banks under a license issued by a country that has been designated as being non-cooperative with international AML/CFT principles or procedures by an intergovernmental group or organisation of which the United States is a member and with which designation the U.S. representative to the group or organisation concurs
- Foreign banks operating under a license issued by a country designated by the U.S. Treasury Department as warranting Special Measures due to money laundering concerns (as defined in Section 311)

584. What are the heightened money laundering and terrorist financing risks of financial institutions operating under an offshore banking license?

Financial institutions operating under offshore banking licenses are prohibited from conducting business with the residents of their licensing jurisdiction or in their local currency, but have the authority to transact business "offshore" with the citizens of other countries. Because they have no negative effect upon local citizens and are often lucrative profit centres for the licensing jurisdiction, local government regulators have less incentive to engage in appropriate oversight of offshore banking institutions.

585. Do all financial institutions operating under an offshore banking license pose the same risk?

No. Offshore banks affiliated with well-established onshore parent financial institutions may not pose as high a risk as unaffiliated offshore banks; however, affiliated status is no guarantee against anti-money laundering deficiencies. Financial institutions should consider conducting their own due diligence to understand the risks of affiliated offshore banks and not automatically assume their AML Program is the same or as strong as the reputable affiliate.

586. What is the difference between a Class A and a Class B offshore banking license?

Simply put, Class A licenses allow an institution to provide services to customers within and outside of the jurisdiction granting the license, while Class B licenses restrict institutions to conduct only offshore banking activities.

587. What are the enhanced due diligence (EDD) requirements for correspondent accounts outlined in Section 312?

Applicable U.S. financial institutions must, at minimum:

- Conduct enhanced scrutiny to guard against money laundering and terrorist financing and to identify and report any suspicious transactions, including:
  - Obtaining and considering information relating to the respondent's AML/CFT Compliance Program
  - Monitoring transactions to, from or through the account
  - Obtaining information from the foreign bank about the identity of any person with authority to direct transactions through any correspondent account that is a payable-through account (PTA), and the sources and beneficial owner of funds or other assets in the PTA
- Determine whether the respondent for which the account is established or maintained in turn maintains correspondent accounts for other foreign institutions that use the account established or maintained by the U.S. financial institution, and take reasonable steps to obtain information relevant to assess and mitigate money laundering and terrorist financing risks associated with the respondent's correspondent accounts for other foreign financial institutions, including, as appropriate, the identity of such foreign institutions
- Determine, for any respondent whose shares are not publicly traded, the identity of each owner of the foreign institution and the nature of and extent of the ownership interest

Due Diligence for Private Banking Accounts

588. What are the due diligence requirements for private banking accounts outlined in Section 312?

Requirements include the establishment of a due diligence program that includes policies, procedures and controls that are reasonably designed to detect and report known or suspected money laundering activity conducted through or involving any private banking account established, maintained, administered or managed in the United States by the financial institution for a non-U.S. person.

At minimum, the due diligence program must:

- Identify the nominal (i.e., named) and beneficial owners of a private banking account
- Determine if any of the nominal and beneficial owners of the of the private banking account are politically exposed persons (PEPs)
- Identify the private banking account's source of funds, purpose and expected use
- Review the private banking account activity to ensure it is consistent with the information obtained about the customer's source of funds, stated purpose and expected use of the account
- Report, as appropriate, known or suspected money laundering or suspicious activity conducted to, from or through the private banking account

Section 312's private banking due diligence requirements for depository institutions are implemented under 31 C.F.R. 1010.620 – Due Diligence Programs for Private Banking Accounts.

589. What does the term "private banking account" mean for Section 312 purposes?

A private banking account is defined as an account (or combination of accounts) maintained at a financial institution that meets the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of not less than US$1 million
- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account
- Is assigned to, or is administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account

590. What are typical products/services offered to private banking customers?

Private banking services may include, but are not limited to:

- Cash management (e.g., checking accounts, bill-paying services, overnight sweeps, overdraft privileges)
- Asset management (e.g., trust advisory, investment management, custodial and brokerage services)

- Lending services
- Financial and estate planning
- Facilitation of offshore entities (e.g., private investment companies [PICs], trusts)

591. What is the heightened money laundering and terrorist financing risk of private banking accounts?

Private banking can be vulnerable to money laundering schemes for the following reasons:

- Strict privacy and confidentiality culture of private bankers
- Powerful clientele (e.g., politically exposed persons [PEPs])
- Use of trusts, private investment companies (PICs) and other types of nominee companies
- Increased frequency of international transactions

592. What are private investment companies and their heightened money laundering and terrorist financing risks?

A private investment company (PIC) generally refers to a company formed by an individual(s) to own and manage his or her assets. Often established in offshore financial centres (OFCs) for tax reasons, PICs provide confidentiality and anonymity to the beneficial owners of the funds because the management of the PIC often rests with a third party not readily associated with the beneficial owner. It is because the ownership of a PIC is not transparent that PICs may pose heightened money laundering risk.

593. What are offshore financial centres?

Offshore financial centres (OFCs) are jurisdictions that have a relatively large number of financial institutions engaged primarily in business with non-residents. OFCs are generally known for their favourable tax climate and bank secrecy laws. Some examples of OFCs include Bermuda, the British Virgin Islands, the Cayman Islands, Cyprus, the Isle of Man and Panama. Additional information, including assessments of OFCs, can be found on the International Monetary Fund's (IMF) website: www.imf.org.

594. Should an account be subject to the enhanced due diligence requirements of a private banking account if it satisfies the regulation's definition of a private banking account with the exception that the financial institution does not require a minimum balance of US$1 million?

Financial institutions have taken varying stances regarding their interpretation of the definition of a private banking account. Some financial institutions have taken the position that if the financial institution does not require a minimum balance of US$1 million to qualify for additional private banking services, then the financial institution does not have private banking accounts. Others classify any account(s) with more than US$1 million in assets as a private banking account. A financial institution should clearly outline its definition of a private banking account within its policies and

procedures. Regardless of a financial institution's definition, a risk-based approach should be used when selecting accounts for additional due diligence.

595. What does the term "beneficial owner" mean for Section 312 purposes?

For Section 312 purposes, the term "beneficial owner" of an account is defined as an "individual who has a level of control over, or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account." 31 C.F.R. 1010.605 further states that "the ability to fund the account or the entitlement to the funds of the account alone, however, without any corresponding authority to control, manage or direct the account (such as in the case of a minor child beneficiary), does not cause the individual to be a beneficial owner."

Covered financial institutions are required to identify all beneficial owners with at least 10 percent control or entitlement to the private banking account. A different definition of beneficial owners with a higher threshold was recently established for a broader rule to identify beneficial owners, as described below.

596. How does FinCEN define "beneficial owner" in the final rule "Customer Due Diligence Requirements for Financial Institutions"?

FinCEN issued the final rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) in 2016, which requires financial institutions currently subject to Customer Identification Program (CIP) requirements to identify and verify the identity of beneficial owners with 25 percent or greater ownership or significant control of legal entity customers. However, the Beneficial Ownership Rule does not change Section 312 requirements.

The Beneficial Ownership Rule uses a two-prong concept – ownership and effective control – by defining a "beneficial owner" as a natural person, not another legal entity, who meets the following criteria:

- **Ownership prong** – Each individual, up to four, who owns, directly or indirectly, 25 percent or more of the equity interest in a legal entity customer; and
- **Control prong** – At least one individual who exercises significant responsibility to control, manage or direct (e.g., a C-suite Executive, Managing Member, General Partner, President, Treasurer) the legal entity.

In cases where an individual is both a 25 percent owner and meets the control definition, that same individual can be defined as a beneficial owner under both prongs. From an industry perspective, the second prong improves upon the definition in the advanced notice of proposed rulemaking (ANPR) issued in 2012. The earlier definition would have required the identification of the individual who had "greater responsibility than any other individual."

For further guidance, please refer to the Beneficial Owners section.

597. If an individual is entitled to the funds in the account, but does not have any authority to control, manage or direct the account, would the individual be considered a "beneficial owner"?

No. The ability to fund the account or the entitlement to the funds in the account alone does not cause the individual to be a beneficial owner.

598. Can a financial institution rely on the due diligence conducted by well-regulated foreign intermediaries that open private banking accounts on behalf of their clients?

No. Financial institutions cannot rely on foreign intermediaries to satisfy a financial institution's Section 312 obligations.

599. How do Section 312 requirements for private banking correspond to FATF Recommendations?

In **Recommendation 10 – Customer Due Diligence**, FATF recommends financial institutions implement enhanced measures for higher risk customers, geographies, products, services, transactions and delivery channels, including private banking.

Section 312 outlines enhanced due diligence (EDD) for private banking, including, but not limited to the identification of beneficial owners and politically exposed persons (PEPs).

For further guidance on international standards, please refer to the Financial Action Task Force section. For further guidance on customer due diligence, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence sections.

600. What are the enhanced due diligence (EDD) requirements for private banking accounts outlined in Section 312?

A private banking due diligence program should include reasonable steps to detect and report transactions that may involve the proceeds of foreign corruption. This is in addition to the other requirements for private banking accounts as detailed in the Due Diligence for Private Banking Accounts section.

601. What does the term "proceeds of foreign corruption" mean for purposes of Section 312?

"Proceeds of foreign corruption" are defined as assets or properties that are acquired by, through or on behalf of a senior foreign political figure through the following:

- Misappropriation, theft or embezzlement of public funds;
- The unlawful conversion of property of a foreign government; or
- Acts of bribery or extortion.

Properties into which any such assets have been transformed or converted also are covered under this definition.

602. What guidance has been issued on private banking?

The following are examples of key guidance that has been issued on private banking:

- **Private Banking Due Diligence Program (Non-U.S. Persons)** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Wolfsberg Anti-Money Laundering Principles for Private Banking** (2012) by the Wolfsberg Group of Banks (Wolfsberg Group)
- **Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities** (2001) by the U.S. Senate (Hearing)

Additional topics related to private banking include beneficial ownership and politically exposed persons (PEPs). For further guidance, please refer to the sections: Beneficial Owners, Politically Exposed Persons and Senior Foreign Political Figures.

Senior Foreign Political Figure

603. What does the term "senior foreign political figure" mean for Section 312 purposes?

A "senior foreign political figure," also known as a politically exposed person (PEP), is defined as:

- A current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not);
- A senior official of a major foreign political party;
- A senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual;
- An immediate family member of such an individual; or
- Any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual.

"Immediate family member" means an individual's spouse, parents, siblings, children and spouse's parents or siblings. "Senior official" or "senior executive" means an individual with substantial authority over policy, operations or the use of government-owned resources.

604. How do Section 312 requirements for PEPs correspond to FATF Recommendations?

FATF's definition of PEP, developed to be consistent with the United Nation's Convention Against Corruption (UNCAC), includes the following:

- **Foreign PEPs** are defined as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).

- **Domestic PEPs** are individuals who are, or have been, entrusted domestically with prominent public functions (e.g., heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).
- **International organisation PEPs** are individuals who are, or have been, entrusted with prominent functions by an international organisation (e.g., senior management, directors, board members).

Family members (e.g., direct relatives, through marriage) and close associates (e.g., social, professional) of PEPs are also included in FATF's definition.

FATF Recommendation 12 – Politically Exposed Persons recommends financial institutions implement risk-based measures to mitigate the money laundering risks of PEPs including, but not limited to, the following:

- Identification of foreign PEPs (and family members or close associates) in the customer population (or as beneficial owners);
- Establishing the source of wealth/funds of PEPs;
- Conducting ongoing monitoring of PEP relationships; and
- Requiring senior management approval to provide services to PEPs (e.g., opening an account, paying out on a life insurance policy).

If other high-risk factors are present (e.g., high-risk nature of business, high-risk country of operation), enhanced measures should be applied to domestic PEPs as well.

The USA PATRIOT Act's definition of PEP is consistent with FATF's definition of foreign PEP. While Section 312 of the USA PATRIOT Act outlines enhanced due diligence measures for "senior foreign political figures," many U.S. financial institutions have voluntarily applied due diligence measures to domestic PEPs as well.

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

605. What is the heightened money laundering risk of PEPs?

Access to government funds may increase the potential for corruption and bribery. **Section 315 – Inclusion of Foreign Corruption Offenses as Money Laundering Crimes** includes multiple offenses as money laundering crimes, including, but not limited to, the following:

- Bribery of a public official or the misappropriation, theft, or embezzlement of public funds by or for the benefit of the public official
- Any felony violations of the Foreign Corrupt Practices Act of 1977 (FCPA)
- An offense with respect to multilateral treaties in which the United States would be obligated to extradite the offender or submit the case for prosecution if the offender were found in the United States

For additional guidance on corruption, please refer to Anti-Bribery and Corruption Compliance Program and Foreign Corrupt Practices Act sections.

606. Is the definition of a PEP limited to "foreign" senior officials?

Many financial institutions extend the definition of PEP to include domestic senior political figures, as well, though this is not required by Section 312.

Other jurisdictions (e.g., European Union) have explicitly expanded their definition to include domestic senior political figures as PEPs. Some multinational financial institutions may modify their definition of PEPs to include senior foreign political figures of all countries, irrespective of where each bank/branch is based. Additionally, they may utilise a risk-based approach and only include PEPs from countries with lax AML/CFT laws and regulations or a high index of corruption.

607. Is the definition of a PEP limited to private banking customers?

No. Status as a PEP is not dependent on the types of products and services utilised by the PEP.

608. Is someone who was a PEP always a PEP?

The most conservative approach would be "once a PEP, always a PEP." A moderate approach, endorsed by the Wolfsberg Group and outlined in the European Union's Fourth Anti-Money Laundering Directive, would be for a financial institution to remove the individual from the institution's PEP list one year after the individual is no longer in a political function. However, if derogatory information or suspicious activity is detected, a financial institution should continue to categorise the customer as high risk.

609. Is the definition of PEP limited to natural persons? Are there instances when corporations are considered PEPs?

If a legal entity (e.g., corporation) has been formed by or for the benefit of a PEP, the entity itself would be a PEP-associated entity and subject to similar enhanced due diligence as a PEP.

610. Should an entity controlled by a PEP be subject to similar measures as the PEP itself?

Yes. The same enhanced due diligence should be applied to entities owned or controlled by PEPs.

Criminals, such as corrupt foreign officials, may use legal entities such as private investment companies (PICs) to obscure their identity and disguise their illicit activities. While Section 312 requires the collection and verification of beneficial ownership information for private banking customers, not all PEPs fall under the definition of private banking customers.

To address this vulnerability, FinCEN issued the notice of proposed rulemaking (NPRM), "Customer Due Diligence Requirements for Financial Institutions" in 2014, which would require financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers.

For further guidance, please refer to the following sections: Beneficial Owners, Business Entities: Shell Companies, Private Investment Companies and Anti-Bribery and Corruption Compliance Programs.

611. Do embassy and foreign consulate accounts fall within the definition of a PEP?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status. For further guidance on embassy accounts, please refer to the Foreign Embassy and Consulates section.

612. Do all PEPs pose the same degree of risk?

No. Not all PEPs pose the same degree of risk. A financial institution may consider, for example, the country of domicile, level of office, negative history/media on the PEP and the degree of affiliation to the PEP (in the case of family members and close associates) when assessing the degree of risk.

613. What guidance has been issued with respect to PEPs and embassy banking?

The following key guidance has been issued on PEPs, embassy banking and related topics:

- **Politically Exposed Persons – Overview** (2010) and **Embassy and Foreign Consulate Accounts – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)** (2013) by the Financial Action Task Force (FATF)
- **Best Practices Paper: The Use of FATF Recommendations to Combat Corruption** (2013) by FATF
- **Corruption: A Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight against Corruption** (2012) by FATF
- **Interagency Advisory: Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions** (2011) by the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), FinCEN, National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** (2008) by FinCEN
- **Wolfsberg FAQs on Politically Exposed Persons** (2008) by the Wolfsberg Group of Banks (Wolfsberg Group)
- **Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption** (2001) by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Department of State

- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** (2010) by the World Bank (WB)
- **Stolen Asset Recovery: Guide on Non-Conviction Based (NCB) Asset Forfeiture** (2009) by the WB
- **Interagency Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions** (2011) by FinCEN
- **Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies and Foreign Political Figures** (2004) by FinCEN
- **Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the PATRIOT Act: Case Study Involving Riggs Bank Report** (2004) by the United States Senate Permanent Subcommittee on Investigations

For further guidance on foreign embassies, corruption and beneficial ownership, please refer to the sections: Foreign Embassy and Consulates, Anti-Bribery and Corruption Compliance Programs and Beneficial Owners.

Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks

614. Which financial institutions are required to comply with Section 313, Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks?

The following financial institutions must comply with Section 313:

- An insured bank
- A commercial bank or trust company
- A private banker
- An agency or branch of a foreign bank in the United States
- A credit union
- A savings association
- A corporation acting under section 25A of the Federal Reserve Act (12 U.S.C. 611 et seq.)
- A registered (or required to be registered) broker or dealer in securities, with limited exceptions

Section 313's shell bank requirements are implemented under 31 C.F.R. 1021.630 – Prohibition on Correspondent Accounts for Foreign Shell Banks, Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process.

615. What does the term "foreign shell bank" mean for Section 313 purposes?

The term "foreign shell bank" is a foreign bank without a physical presence in any country.

616. What does the term "physical presence" mean for Section 313 purposes?

Physical presence means a place of business that:

- Is maintained by a foreign bank
- Is located at a fixed address (other than solely an electronic address or a P.O. box) in a country in which the foreign bank is authorised to conduct banking activities, at which location the foreign bank:
  - Employs one or more individuals on a full-time basis
  - Maintains operating records related to its banking activities
  - Is subject to inspection by the banking authority that licensed the foreign bank to conduct banking activities

617. Why would a legitimate banking organisation establish a shell bank?

A legitimate banking organisation may create a foreign shell bank for a variety of reasons including, but not limited to, the following:

- Cost-effective method of expanding into foreign jurisdictions
- Legally avoid domestic restrictions
- Minimisation of tax liabilities
- Reduced regulatory burden

618. What are the requirements imposed on financial institutions outlined in Section 313?

Financial institutions are prohibited from establishing, maintaining, administering or managing a correspondent account in the United States for, or on behalf of, a foreign shell bank.

619. Are there exceptions to the requirements outlined in Section 313?

Yes. A financial institution can maintain a correspondent account for a foreign shell bank that is a regulated affiliate of a bank with a physical presence.

620. What steps should a financial institution take to ensure that one or more of its correspondent relationships do not involve a foreign shell bank?

Beyond complying with Section 313, the financial institution should conduct due diligence on its correspondent relationships to (a) gain a better understanding of the respondent, and (b) develop an understanding of the respondent's customer base. The correspondent should perform transaction monitoring to identify, among other things, potential nested relationships.

Additionally, Section 319(b) requires financial institutions to obtain foreign bank certifications, also referred to as USA PATRIOT Act certifications, in which foreign respondents state in writing that the use of correspondent accounts by foreign shell banks is prohibited. For further guidance, please refer to the Foreign Bank Certifications section.

621. What does the term "nested relationship" mean for Section 313 purposes?

Foreign banks may use correspondent accounts of other foreign banks rather than maintaining their own correspondent account with a U.S. financial institution to gain access to the U.S. financial system. These are nested relationships also referred to as "downstream correspondents." A nested bank gains the advantages of a correspondent status often without being subject to the correspondent's customer acceptance standards and perhaps without the correspondent's awareness.

622. What should a correspondent do when a former respondent is nesting through a current respondent relationship?

When a correspondent closes an account due to the identification of suspicious activity, the respondent usually is added to a watch list in order to ensure the respondent does not open another account a few months later. Monitoring against this list would enable a correspondent to find nested relationships that were closed due to suspicious activity. Where a correspondent has terminated a relationship with a respondent and subsequently finds nesting, it may inform its respondent that it is not comfortable doing business with the nested respondent (if it can do so without tipping the respondent off to the fact it has filed a SAR) or it may decide to file a SAR(s) on the nested activity if it deems it suspicious.

623. What should a correspondent do when a foreign shell bank is nesting through a current respondent relationship?

In addition to the investigation and SAR filing procedures detailed above, the correspondent should close all accounts with the respondent within a commercially reasonable amount of time. Reopening of such accounts can occur only under special circumstances (e.g., respondent implements satisfactory measures to guard against the provision of services to foreign shell banks).

624. How do Section 313 requirements for foreign shell banks correspond to FATF Recommendations?

FATF Recommendation 13 – Correspondent Banking recommends prohibiting the establishment of correspondent banking relationships with shell banks.

Section 314 – Cooperative Efforts to Deter Money Laundering

625. How does Section 314 facilitate cooperative efforts to deter money laundering and terrorist financing?

Section 314 establishes two mechanisms to facilitate information sharing and collaboration to deter money laundering and terrorist financing:

- Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities
- Section 314(b) – Cooperation among Financial Institutions

Details of both information sharing mechanisms are provided below.

626. Which financial institutions are eligible to participate in Section 314 information sharing?

All financial institutions required to establish AML Programs under Section 352 are eligible to participate in Section 314(a) and (b) information sharing. At the time of this publication, this includes the following:

- Depository institutions (e.g., insured banks, commercial banks, private banks, credit unions, thrifts and savings institutions)
- Broker-dealers
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Money services businesses (MSBs) (e.g., check cashers, money transmitters, providers of prepaid access)
- Casinos and card clubs
- Mutual funds
- Insurance companies
- Dealers in precious metals, precious stones or jewels
- Operators of credit card systems
- Loan or finance companies (e.g., nonbank residential mortgage lenders and originators [RMLO])
- Housing Government-Sponsored Enterprises (GSE)

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM), "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator," that will expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to, the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations
- State-chartered non-depository trust companies
- International banking entities

627. How does Section 314 correspond to FATF Recommendations?

Several FATF Recommendations provide guidance on information sharing:

- **Recommendation 2 – National Cooperation and Coordination** – FATF recommends the implementation of a mechanism to enable policy-makers, FIUs, law enforcement, regulatory

authorities and other relevant authorities to cooperate and coordinate the development and implementation of policies and activities to deter money laundering, terrorist financing and the proliferation of weapons of mass destruction (WMDs).

The following recommendations also address information sharing across an enterprise and with relevant international authorities:

- **Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries –** FATF recommends the implementation of an enterprisewide AML/CFT Compliance Program that includes policies on information sharing across the group.
- **International Cooperation (Recommendations 36 – 40) –** Countries are encouraged to ratify international conventions/treaties and develop a legal basis (e.g., sign treaties, enter a Memorandum of Understanding [MOU]) to provide mutual legal assistance (e.g., information sharing, freezing of assets, extraditions) to other countries (e.g., financial institutions, FIUs, supervisors, law enforcement) in relation to money laundering and terrorist financing proceedings.

For further guidance on international standards, please refer to the Financial Action Task Force section.

Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities

628. How does Section 314(a), Cooperation Among Financial Institutions, Regulatory Authorities, and Law Enforcement Authorities, facilitate the sharing of information?

Section 314(a) of the USA PATRIOT Act establishes a mechanism for law enforcement agencies to communicate the names of persons engaged in or suspected to be engaged in terrorism and money laundering to financial institutions in return for securing the ability to locate accounts and transactions involving those suspects promptly. Currently, FinCEN can reach more than 44,000 points of contact in over 22,000 financial institutions.

Section 314(a) is implemented for depository institutions under 31 C.F.R. 1010.520 – Information Sharing between Government Agencies and Financial Institutions.

629. Are financial institutions obligated to share information under Section 314(a)?

All financial institutions required to establish an AML Program under Section 352 are obligated to comply with 314(a) information requests. Unlike Section 314(b), participation is not voluntary.

630. What are the protocols for issuing 314(a) requests prior to distribution to financial institutions?

Every 314(a) request is certified and vetted through the appropriate channels within each law enforcement agency to ensure that the information requested from financial institutions is related to a valid and significant money laundering/terrorist investigation. FinCEN also requires documentation showing the size or impact of the case, the seriousness of the underlying criminal activity, the

importance of the case to major agencies, and the exhaustion of traditional or alternative means of investigation prior to the submittal of requests to financial institutions by FinCEN.

631. What law enforcement agencies are able to participate in issuing 314(a) requests?

Since the inception of 314(a) information sharing, all federal domestic law enforcement agencies have been permitted to participate in providing requests to FinCEN to be submitted to the participating financial institutions.

On February 10, 2010, FinCEN issued a final rule expanding participation privileges to foreign law enforcement agencies as well as domestic state and local agencies. Further, the final rule grants FinCEN the ability to initiate 314(a) inquiries on its own behalf, and on behalf of other areas of the U.S. Department of the Treasury.

632. How often do financial institutions receive information requests under Section 314(a)?

Batched information requests are sent by FinCEN every two weeks. However, an ad hoc information request may be sent to a financial institution in an urgent situation.

633. How are 314(a) requests distributed to financial institutions?

In March 2005, FinCEN began distributing 314(a) subject lists through its secure website, Secure Information Sharing System (SISS). Every two weeks, or more often if an emergency request is transmitted, the financial institution's designated point of contact can download the current 314(a) subject list, as well as the preceding list, in various formats for searching.

Financial institutions previously were able to receive the 314(a) subject lists via facsimile transmission; however, this option is no longer available. Institutions may no longer elect to receive 314(a) transmissions via fax, as FinCEN now requires all participants to obtain 314(a) subject lists through SISS. FinCEN may still elect to send facsimile transmissions of the list; however, this may not be relied upon by financial institutions.

634. What information is included in 314(a) requests?

The requests contain subject and business names, addresses and as much identifying data as possible to assist the financial institutions with searching their records.

635. How does a financial institution change its point-of-contact information on FinCEN's distribution list for receiving 314(a) information requests?

A financial institution should contact its primary federal regulator or self-regulatory organisation (SRO) to change its point of contact. Financial institutions also should provide information for Section 314(a) points of contact on the financial institution's quarterly call or Thrift Financial Report (for financial institutions subject to supervision by one of the five federal banking regulators). Contact information can be found at www.fincen.gov.

636. Within what time frame are financial institutions required to complete their 314(a) searches?

Financial institutions are required to complete their searches and respond to FinCEN with any matches within two weeks of receiving the request.

637. What records are financial institutions required to search under 314(a)?

Financial institutions are required to search the following records if maintained in a searchable electronic format:

- Deposit account records
- Funds transfer records
- Records for the sale of monetary instruments
- Loan records
- Trust department account records
- Records of accounts to purchase, sell, lend, hold or maintain custody of securities
- Commodity futures, options or other derivatives
- Safe deposit box records

638. Does the "Customer Due Diligence Requirements for Financial Institutions" final rule create new obligations for covered financial institutions with regard to Section 314(a)?

No. The Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule) does not create new obligations for covered financial institutions; however, if a match with identifying information provided in the 314(a) request is made, including with beneficial owners, covered financial institutions are required to report this.

639. How can technology be used to facilitate 314(a) searches?

Some institutions use technology solutions to facilitate searching. Interdiction software, also known as filtering or screening software, is a tool that facilitates the comparison of separate sets of data (e.g., a customer database, list of individuals/businesses linked to illicit activity) for possible hits. For further guidance, please refer to the AML/CFT Technology and Interdiction Software sections.

640. If a financial institution scans and saves checks onto its systems as images, should these also be searched?

No. Electronic media that is searchable (e.g., databases, delimited text files) should be included in 314(a) searches, but images and other electronic media that do not support search technology are excluded from the scope of 314(a) searches.

641. Is a financial institution obligated to report a possible match with a noncustomer of the institution (e.g., beneficiary of a funds transfer originated by its own customer)?

Yes, any match should be reported. 314(a) searches apply not only to accounts, but also to transactions conducted at or through the financial institution; therefore, a transaction counterparty, who may be a noncustomer, could result in a possible match.

642. Are there records that financial institutions are not required to search for possible 314(a) matches?

Financial institutions are not required to search the following records unless the information is readily searchable (e.g., databases, delimited text files):

- Checks processed through an account to determine whether a named subject was a payee of a check
- Monetary instruments (e.g., cashier's checks, money orders, traveller's checks, drafts) issued by the institution to determine whether a named subject was a payee of such an instrument
- Signature cards to determine whether a named subject is a signatory to an account (unless such a search is the only method to confirm whether a named subject maintains an account, as described above)

643. For what periods are financial institutions required to search their records under Section 314(a)?

Unless otherwise noted in the 314(a) information request, financial institutions must search their records for the preceding 12 months for account parties (e.g., account holders, signers), and for the preceding six months for transactions.

644. Should financial institutions receiving information requests from FinCEN under Section 314(a) search their records on a continuing basis?

Unless otherwise noted on the information request, 314(a) requests require a one-time search only. Financial institutions do not need to continue to search their records in the future, unless specified on the information request.

645. What action should a financial institution take if it does not identify a match to a 314(a) request?

If the search does not yield any results, a financial institution should not reply to the 314(a) request. It should document the completion of the search and the results, and protect the confidentiality of the 314(a) list.

646. What action should a financial institution take if it identifies a potential match to a 314(a) request?

In the event of a possible match, a financial institution should conduct an investigation to the extent necessary to determine whether the information represents a true match, or is a false positive. In the

event of a true match, the designated point of contact should notify FinCEN via the website that it has a match, as well as provide the individual's contact information to enable the requesting law enforcement agency to contact the institution to obtain further information regarding the match. The financial institution must provide FinCEN with the name and account number of each individual, entity or organisation for which a match was found, as well as any taxpayer identification number (TIN), date of birth (DOB) or other similar identifying information provided by such person at the account opening or when the transaction(s) was conducted.

647. Is 314(a) information sharing an acceptable substitute for complying with a subpoena or National Security Letter?

No. Section 314(a) provides lead information only. It is not a substitute for a subpoena or other legal process. To obtain documents from a financial institution that has a reported match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool it chose to use to obtain the documents.

648. What documentation should a financial institution maintain relating to its 314(a) searches?

Some financial institutions choose to maintain copies of the cover page of the request, with sign-off from appropriate personnel indicating the date the search was completed, and the results (i.e., positive, negative). For positive matches, many financial institutions also maintain the correspondence with FinCEN. Other financial institutions maintain the entire 314(a) request, including subjects searched. Regardless of the documentation maintained, a financial institution must maintain procedures to protect the security and confidentiality of 314(a) requests.

649. Should financial institutions automatically file a SAR on a positive 314(a) match?

No. FinCEN strongly discourages financial institutions from using the results of a 314(a) search as the sole factor in reaching a decision to file a SAR unless the request specifically states otherwise. A 314(a) match may serve to initiate an investigation; however, the decision to file a Suspicious Activity Report (SAR) should be based on the institution's investigation of the activity involved.

650. Has FinCEN issued statistics relating to the usefulness of 314(a) requests?

Yes. FinCEN issues a 314(a) Fact Sheet annually that outlines a number of statistics relating to 314(a) requests including the following:

- Total number of processed requests
- Number of cases related to terrorism
- Number of cases related to money laundering
- Number of "subjects of interest"
- Number of positive confirmations

Approximately 80 percent of cases are related to money laundering. The law enforcement requesters who provided FinCEN with feedback indicated that because of the 314(a) system, 95 percent of the confirmations contributed to arrests and indictments.

651. Beyond Section 314(a), what other mechanisms are used by law enforcement to obtain information from financial institutions?

Other mechanisms used by law enforcement to obtain information from financial institutions include, but are not limited to, the following:

- **Subpoenas** – Law enforcement has the ability to request certain specific information by the use of subpoenas, which must comply with applicable laws, such as the Right to Financial Privacy Act.
- **National Security Letters (NSLs)** – Written investigative demands may be issued by the local Federal Bureau of Investigation (FBI) field office and other federal government authorities in counterintelligence and counterterrorism investigations to obtain telephone and electronic communications records from telephone companies and internet service providers, information from credit bureaus and financial records from financial institutions. NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. For further guidance on NSLs, please refer to Section 505 – Miscellaneous National Security Authorities.

Section 314(b) – Cooperation Among Financial Institutions

652. How does Section 314(b), Cooperation Among Financial Institutions, facilitate the sharing of information?

Section 314(b) enables financial institutions, or an association of financial institutions, to share information concerning suspected money laundering and terrorist activity with other financial institutions under a Safe Harbor from liability. To participate in information sharing with other financial institutions and financial institution associations, each participant must notify FinCEN of its intent to share information. Notification can be provided by completing a Financial Institution Notification Form that can be found on FinCEN's website. If the notification form is not provided to FinCEN, the Safe Harbor protection is not available.

Section 314(b) is implemented for depository institutions under 31 C.F.R. 1010.540 – Voluntary Information Sharing Among Financial Institutions.

653. Are "association of financial institutions" eligible for participation in Section 314(b) sharing?

Yes. An "association of financial institutions" comprised entirely of financial institutions as defined by the broad list of financial institutions listed in the USA PATRIOT Act is eligible to participate in sharing.

654. Are financial institutions obligated to share information under Section 314(b)?

No. Unlike Section 314(a), financial institutions are not obligated to share information under Section 314(b).

655. For what period does the notification form submitted to FinCEN allow a financial institution to share information?

Once the notification is filed, the filing institution may share information for one year, beginning on the execution date of the notification form. A financial institution does not need to wait for confirmation from FinCEN to begin sharing information.

656. Do financial institutions have any obligations beyond submitting notification forms in order to share information?

Yes. Financial institutions sharing information under Section 314(b) must have procedures in place to protect the security and confidentiality of shared information and to ensure the information is used only for authorised purposes.

Financial institutions also should take reasonable steps to ensure that any financial institution with which it shares information has submitted the requisite form as well. This can be done by confirming that the other financial institution appears on a list that FinCEN provides to financial institutions that have filed a notice, or by confirming directly with the other financial institution that the requisite notice has been filed.

657. Does the notification form need to be renewed?

To continue to share information after the expiration of the one-year period, a financial institution must submit a new notification form.

658. What are the consequences of failing to submit this notification form but continuing to share information?

A financial institution that fails to notify FinCEN of its intent to share information with other institutions will not be protected under the Safe Harbor provision.

659. Can SARs be shared as part of Section 314(b) sharing?

No. Section 314(b) sharing does not allow financial institutions to disclose the filing of SARs. However, the underlying transactional and customer information may be shared.

660. Are there any restrictions on what information is permitted to be shared under 314(b)?

Yes. To benefit from the protection afforded by the Safe Harbor provision associated with 314(b), financial institutions must adhere to guidelines established by FinCEN that cover the purpose of information permitted to be shared and the content:

- The purpose for sharing under the 314(b) rule is to identify and report activities that the financial institution(s) "suspects may involve possible terrorist activity or money laundering"
- "Permissible information" is limited to that which the financial institution(s) (both parties) feel is relevant to an investigation of only money laundering or terrorist financing activities and may not include the disclosure of a SAR filing

As of June 26, 2009, FinCEN extended the breadth of permissible information covered under the Safe Harbor provision to include information related to certain specified unlawful activities (SUA) including, but not limited to, the following:

- Manufacturing, import, sale or distribution of a controlled substance
- Murder, kidnapping, robbery, extortion, destruction of property by means of explosive or fire, or a crime of violence
- Fraud, or any scheme or attempt to defraud, by or against a foreign bank
- Bribery of a public official, or the misappropriation, theft or embezzlement of public funds by or for the benefit of a public official
- Smuggling or export control violations involving specified items outlined in the United States Munitions List and the Export Administration Regulations
- Trafficking in persons, selling or buying of children, sexual exploitation of children, or transporting, recruiting or harbouring a person, including a child, for commercial sex acts

A comprehensive listing of unlawful activities covered under the 314(b) Safe Harbor provision is documented in The Money Laundering Control Act of 1986 (MLCA), 18 U.S.C. Section 1956 and 1957. Financial institutions should consult with counsel on how best to handle the sharing of information under the 314(b) provision.

661. Are there any restrictions on how the shared information is permitted to be used under 314(b)?

Yes. Financial institutions can use the information for AML/CFT purposes only (e.g., supporting an investigation, determining whether to engage in activity/process a transaction, and determining whether to terminate a relationship).

Financial institutions must maintain policies and procedures to safeguard the security and confidentiality of shared information.

662. Does the sharing of information as permitted in Section 314(b) obviate the need for a financial institution to file a SAR or notify law enforcement?

No. Section 314(b) sharing does not obviate the need to file a SAR or notify law enforcement, if warranted. For further guidance on reporting potentially suspicious activity, please refer to the Suspicious Activity Reports section.

Section 319 – Forfeiture of Funds in United States Interbank Accounts

Basics

663. What are the key provisions of Section 319 – Forfeiture of Funds in United States Interbank Accounts?

Section 319 outlines circumstances in which funds can be seized from a U.S. interbank account; requirements to retrieve bank records of foreign respondents within "120 hours"; and "foreign bank certification" requirements of foreign respondents (e.g., certifies physical presence, regulated status, prohibition of indirect use of correspondent accounts by foreign shell banks) as required by Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks.

Section 319(a) – Forfeiture of Funds in United States Interbank Accounts

664. What does the term "interbank account" mean for the purposes of Section 319(a), Forfeiture from U.S. Interbank Accounts?

An "interbank account" is an account owned by a financial institution that is held with another financial institution for the primary purpose of facilitating customer transactions (e.g., correspondent accounts, payable-through accounts [PTAs], concentration accounts).

665. What are the implications of Section 319(a), Forfeiture from U.S. Interbank Accounts?

Section 319(a) addresses the circumstances in which funds can be seized from a U.S. interbank account. If a deposit with a financial institution outside of the United States is subject to forfeiture, and that foreign institution, in turn, deposits funds in the United States with a bank, broker-dealer, or branch or agency of a foreign bank, those funds are deemed to have been deposited in a U.S. interbank account and thus are subject to seizure under this rule. The funds do not have to be traceable to the funds originally deposited in the foreign financial institution (FFI) to be subject to seizure.

Section 319 is implemented for depository institutions under 31 C.F.R. 1010.670 – Summons or Subpoena of Foreign Bank Records, Termination of Correspondent Relationship.

666. Who has the authority to seize funds under Section 319(a)?

The U.S. Department of Justice (DOJ) has authority to seize funds under Section 319(a). Although the U.S. DOJ has used its authority to seize foreign bank funds in a number of interbank accounts at financial institutions in the United States, the seizure of funds in an interbank account is intended to be used as a last resort by law enforcement agencies.

667. Can foreign financial institutions contest the forfeiture of funds in interbank accounts?

Only the owner of the funds deposited into the account may contest the forfeiture. Foreign financial institutions are explicitly excluded from the definition of "owner."

668. What can a financial institution do to mitigate the risk of seizure of funds in its interbank accounts?

Financial institutions should ensure they complete thorough due diligence procedures on their interbank accounts and understand the other financial institution's customer base. However, funds subject to seizure do not need to be traceable to the original funds deposited at the foreign financial institution. Thus, although performing thorough due diligence reduces the risk of seizure, such risk cannot be eliminated altogether.

669. How does Section 319(a) correspond to FATF Recommendations?

Several FATF Recommendations provide guidance on the freezing and confiscation of assets derived from criminal activity.

- **Recommendation 4 – Confiscation and Provisional Measures** – FATF recommends the implementation of measures to freeze or seize proceeds from criminal activity (e.g., predicate offenses outlined by FATF), laundered funds, funds used to finance terrorism or support a terrorist act or organisation or property of corresponding value.
- **Recommendation 6 – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing** – FATF recommends compliance with various United Nations Security Council Resolutions (UNSCR) requiring the freezing of property of persons designated as terrorists or terrorist organisations by relevant authorities.
- **Recommendation 7 – Targeted Financial Sanctions Related to Proliferation** – FATF recommends compliance with various UNSCR requiring the freezing of property of persons designated as proliferators of weapons of mass destruction (WMDs) by relevant authorities.
- **Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation** – FATF recommends the implementation of international instruments to assist with foreign requests to identify, freeze and seize affected property.

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section. For additional guidance on asset seizure, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

670. What are some examples of cases of forfeiture of funds in interbank accounts?

In 2014, the Asset Forfeiture and Money Laundering Section of the Criminal Division of the Department of Justice (DOJ) sought the forfeiture of approximately US$1.5 million in funds traceable to the money laundering of bribery payments violating the Canadian Corruption of Foreign Public Officials Act and the U.S. Foreign Corrupt Practices Act (FCPA). These funds were held in several of the five U.S. interbank accounts held by Nedbank Ltd., a South African bank, and were therefore subject to seizure under Section 319.

In 2014, the DOJ sought the forfeiture of approximately US$70 million in funds traceable to fraudulent payments made to Hikatullah Shadman, his associates and his companies for the transport of U.S.

military supplies in Afghanistan. Shadman and associates bribed subcontractors and used fraudulent documents to win trucking contracts in violation of the FCPA.

These funds were held in U.S. interbank accounts held by multiple foreign banks, including Afghanistan International Bank (AIB) from Afghanistan, Bank Alfalah from Pakistan and Emirate National Bank from the United Arab Emirates (UAE), and were therefore subject to seizure under Section 319. Since the initial hearing, a portion of the funds has been seized and Shadman and AIB have filed complaints, contesting the seizure of the remaining funds on multiple grounds (e.g., innocence, international comity, funds "owned" by AIB, not Shadman).

Section 319(b) – Bank Records

120-Hour Rule

671. Does a U.S. regulatory agency have the authority to request information about a foreign financial institution's accounts, transactions or customers related to its correspondent account at a U.S. financial institution?

Yes. A foreign financial institution must reply to an information request regarding one or more of its accounts from a U.S. regulatory agency relating to AML/CFT compliance.

Section 319(b) is implemented under 31 C.F.R. 1021.670 – Summons or Subpoena of Foreign Bank Records, Termination of Correspondent Relationship.

672. What is the time frame allotted for retrieving records?

Financial institutions are required to retrieve records relating to foreign correspondent banking activity within 120 hours of a request made by a regulatory agency and within 7 days of a request made by law enforcement.

673. If a request for information about a respondent covered under the 120-Hour Rule is received at 5:00 p.m. on Friday, when must the financial institution respond?

The financial institution must reply by 5 p.m. the following Wednesday, within 120 hours of the request. Weekends and holidays are included in the time frame for submissions.

7-Day Rule

674. What is the time frame allotted for retrieving records requested by law enforcement?

Financial institutions are required to retrieve records relating to foreign correspondent banking activity within 7 days of a request made by law enforcement as outlined in Section 319 implementing regulation 31 C.F.R. 1021.670 – Summons or Subpoena of Foreign Bank Records, Termination of Correspondent Account.

Foreign Bank Records

675. Who has authority to request information from a foreign financial institution?

The Secretary of the U.S. Treasury Department or the Attorney General is authorised to subpoena records of a foreign financial institution relating to a U.S. correspondent account.

676. What will happen if a foreign bank does not comply with the information request?

If a foreign financial institution does not comply with or contest any such summons or subpoena within 10 calendar days of notification, U.S. depository institutions or broker-dealers that hold an account with the foreign bank are required to sever immediately their correspondent arrangements with the foreign bank.

677. Are financial institutions obligated to provide U.S. regulatory agencies and/or law enforcement agencies with records maintained outside of the United States?

If a transaction is conducted by or through a financial institution in the United States, records relating to that transaction can be requested by regulatory agencies and/or law enforcement agencies. The financial institution is obligated to provide those records.

Foreign Bank Certifications

678. What recordkeeping requirements does Section 319(b) impose on financial institutions?

A foreign respondent that maintains a correspondent account with any U.S. bank or U.S. broker-dealer in securities must certify the following in writing:

- Physical presence/regulated affiliated status
- Prohibition of indirect use of correspondent accounts by foreign shell banks
- Ownership status (for non-public institutions)

This "foreign bank certification," also referred to as a USA PATRIOT Act certification, must include the name and address of a person who resides in the United States and is authorised to accept service of legal process for records regarding the correspondent account.

Domestic correspondents are required to obtain a foreign bank certification from each foreign respondent.

Section 319(b)'s foreign bank certification requirements are implemented under 31 C.F.R. 1010.630 – Prohibition on Correspondent Accounts for Foreign Shell Banks; Records Concerning Owners of Foreign Banks and Agents for Service of Legal Process.

679. What is a foreign bank for purposes of certification?

A foreign bank is a bank organised under foreign law and located outside of the United States. A bank includes offices, branches, and agencies of commercial banks or trust companies, private banks,

national banks, thrift institutions, credit unions, and other organisations chartered under banking laws and supervised by banking supervisors.

680. Are financial institutions required to obtain foreign bank certifications for foreign MSBs?

In some cases, foreign MSBs are chartered under banking laws and supervised by banking supervisors and thus subject to foreign bank certification requirements.

681. Are there any exceptions from foreign bank certification requirements?

Foreign bank certifications are not required for nonbank financial institutions (including foreign broker-dealers), U.S. banks operating in the United States, or U.S. branches or subsidiaries of foreign banks.

682. Are U.S. financial institutions required to obtain foreign bank certifications for their foreign affiliates?

No. U.S. financial institutions may rely on their knowledge of their foreign affiliates' AML/CFT Compliance Program in lieu of obtaining foreign bank certifications; however, monitoring of activity and other due diligence procedures should be applied consistently to affiliate and non-affiliate financial institutions.

683. Do certifications have to be obtained from each branch, agency and subsidiary of a foreign respondent?

Single certifications covering multiple branches and offices outside of the United States are permitted provided that the certification includes the names, addresses and regulating body(ies) of all branches or offices to be covered under the single certification (e.g., all the branches and offices outside of the United States that maintain a correspondent account with the U.S. depository institution or securities broker-dealer).

684. Has FinCEN provided an example of a foreign bank certification?

Yes. A template foreign bank certification form issued by the Treasury Department is available on FinCEN's website at www.fincen.gov.

685. Are financial institutions afforded Safe Harbor if they use the foreign bank certification?

Yes. Financial institutions receive Safe Harbor if they use the foreign bank certification as prescribed by AML/CFT laws and regulations (i.e., obtained from each foreign bank every three years).

686. What does the term "owner" mean?

The term "owner" is any person who directly or indirectly owns, controls or has the power to vote 10 percent or more. Members of the same family shall be considered to be one person.

687. Is ownership information required for all foreign respondents?

No. Ownership information is not required for foreign respondents that are publicly traded on an exchange or organised in the over-the-counter market that is regulated by a foreign securities authority as defined by the Securities Exchange Act of 1934 or that have filed an Annual Report of Foreign Banking Organisations form with the Federal Reserve.

688. If a foreign respondent posts its foreign bank certification form on the internet, has it satisfied its 319(b) requirements?

Yes. Many financial institutions post foreign bank certifications on their websites to streamline the foreign bank certification process.

Additionally, the Wolfsberg Group, in partnership with a third-party vendor, has developed a subscription-based international due diligence repository that allows financial institutions to submit foreign bank certifications and other information about their institutions and their AML Programs to a central repository. Additional information about this repository is available at www.wolfsberg-principles.com.

689. How often must a foreign respondent update its foreign bank certification?

Foreign bank certifications are required to be renewed every three years.

690. What is required of a foreign respondent if facts and circumstances (e.g., change in ownership) have changed since the last certification?

A foreign respondent must notify each domestic correspondent relationship, within 30 days, of changes to its:

- Physical presence/regulated affiliated status
- Indirect use of correspondent accounts by foreign shell banks
- Ownership status (for non-public institutions)

691. If a foreign respondent makes corrections/amendments to its original foreign bank certification, should the recertification date be three years from the original certification date or from the execution of an amended/corrected certification date?

The recertification date should be three years from the execution of an amended/corrected certification date.

692. What steps should a domestic correspondent take if the foreign respondent does not provide the requested foreign bank certification?

If certification or recertification has not been obtained from the foreign respondent within 90 days of a request, the domestic correspondent is required to close all correspondent accounts with the foreign respondent within a commercially reasonable time. At that time, the foreign respondent is prohibited from establishing new accounts or conducting any transactions with the domestic correspondent other

than those necessary to close the account. Failure to terminate a correspondent relationship can result in civil penalties assessed per day until the relationship is terminated.

693. Can a domestic correspondent re-establish the correspondent account if the account was initially closed because the foreign respondent failed to provide a foreign bank certification?

Yes. Domestic correspondents may re-establish the account, or even open a new correspondent account, for the foreign respondent if the foreign respondent provides the required information.

694. What is the time frame for terminating a relationship with a foreign respondent when requested by regulators and/or governmental agencies?

A financial institution must terminate the relationship within 10 business days of the request.

695. What steps should a domestic correspondent take after receiving a foreign bank certification?

Domestic correspondents should have procedures in place to ensure the foreign bank certifications obtained are reviewed for reasonableness, completeness and consistency. This responsibility may be assigned to the correspondent bank group or to AML compliance personnel.

696. Does compliance with foreign bank certification requirements suggest the good standing of a financial institution's AML Program?

No. Obtaining the certification will help domestic correspondents ensure they are complying with requirements concerning correspondent accounts with foreign respondents and can provide Safe Harbor for purposes of complying with such requirements. However, due diligence still must be conducted to understand the AML/CFT laws in the country of domicile and incorporation of the foreign respondent, as well as the foreign respondent's AML Program.

697. Does the receipt of the foreign bank certification meet the due diligence requirements outlined in Section 312?

No. The foreign bank certification requirements outlined in Section 319(b) are, though related, distinct from the requirements outlined in Section 312.

698. How long should a domestic correspondent retain original foreign bank certifications?

The foreign bank certifications must be retained for a minimum of five years after the date that the domestic correspondent no longer maintains any correspondent accounts for the foreign respondent.

699. What is the time frame in which the domestic correspondents must respond to formal law enforcement requests regarding foreign bank certifications?

The domestic correspondent must provide a copy of the foreign bank certification within seven days upon written request from a federal law enforcement officer.

700. Are correspondents required to obtain certifications beyond the Foreign Bank Certification from their foreign respondents?

Pursuant to OFAC's Iranian Sanctions Program, upon receiving a written request from FinCEN, U.S. financial institutions are required to obtain a "Certification for Purposes of Section 104(e) of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA) and 31 C.F.R. 1060.300" (CISADA Certification) from specified foreign respondents. The CISADA Certification requires foreign respondents to provide information on whether they have maintained a correspondent account or processed transaction(s) other than through a correspondent account, directly or indirectly, for an Iranian-linked financial institution, Iran's Islamic Revolutionary Guard Corps (IGRC) or any of its agents or affiliates designated as a Specially Designated National (SDN). For each correspondent relationship/applicable transaction, U.S. financial institutions are required to provide the following details:

- Name of Iranian-linked financial institution/IGRC-linked person;
- Name on correspondent account;
- Correspondent account number(s);
- Approximate value in USD of transactions processed (through or outside of the correspondent account) within the preceding 90 calendar days; and
- Other applicable identifying information for the correspondent account or the transferred funds.

For further guidance on sanctions, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

701. What is the deadline for submitting CISADA Certifications?

The U.S. financial institution must report to FinCEN within 45 calendar days of the written request, regardless of the foreign respondent's response (e.g., positive, negative, incomplete, non-response). If information is received from the foreign respondent after the 45 calendar days, the U.S. financial institution is required to report this to FinCEN within 10 calendar days of receipt. U.S. financial institutions are also required to report to FinCEN when they do not maintain a correspondent account for the specified foreign respondent.

702. Are U.S. financial institutions required to obtain CISADA Certifications from all of their foreign respondents?

No. U.S. financial institutions are only required to submit a CISADA Certification, or a report with the same information, on foreign respondents specified in FinCEN's written request.

703. Should financial institutions automatically file a SAR on activity of confirmed foreign respondents specified in FinCEN's written request?

No. A financial institution should not automatically file a SAR upon receipt of FinCEN's written request. The decision to file a SAR should be based on the institution's own investigation into the activity of the party that/who is the subject of the law enforcement inquiry. FinCEN's written request

may be relevant to a financial institution's overall risk assessment of its customers and accounts. For further guidance on SARs, please refer to the Suspicious Activity Reports section.

704. Is the use of the CISADA Certification mandatory?

No. U.S. financial institutions are not required to use the CISADA Certification but are required to provide the same information when receiving a written request from FinCEN.

Section 325 – Concentration Accounts at Financial Institutions

705. How is the term "concentration account" defined for purposes of Section 325?

The USA PATRIOT Act introduces the possibility of future regulation relating to concentration accounts; however, it does not define this term. Within the industry, a concentration account is an account that a financial institution uses to aggregate funds from different customers' accounts. Concentration accounts are also known as collection, intraday, omnibus, settlement, special-use or sweep accounts.

706. What are financial institutions required to do with respect to concentration accounts under Section 325?

As previously noted, regulations relating to concentration accounts have not been issued by the U.S. Treasury Department. However, financial institutions are advised to recognise and take appropriate actions to control the risks of these accounts.

Section 325 mandates that if regulations are issued, they should:

- Prohibit financial institutions from allowing customers to direct transactions through a concentration account.
- Prohibit financial institutions and their employees from informing customers of the existence of the institution's concentration accounts.
- Require financial institutions to establish written procedures governing documentation of transactions involving concentration accounts.
- In the absence of finalised regulations related to concentration accounts, financial institutions should:
    - Ensure they understand the reasons and the extent to which they use concentration accounts.
    - Establish controls over the opening, maintenance and reconcilement of concentration accounts.
    - Subject concentration accounts to suspicious activity monitoring.

707. What is the heightened money laundering risk of concentration accounts?

Concentration accounts involve the commingling of different customers' funds and also can involve the commingling of customer funds with a financial institution's funds in a way that conceals the identity of underlying parties to a transaction.

Section 326 – Verification of Identification

CIP Basics

708. What are the requirements of Section 326 – Verification of Identification?

Section 326 requires each financial institution to maintain and develop a written Customer Identification Program (CIP). Specifically, financial institutions are required to:

- Collect the following information from new customers:
  - Name
  - Date of birth (DOB) for individuals
  - Address
  - Identification number
- Verify the identity of any person seeking to open an account
- Maintain records of the information used to verify a person's identity
- Consult lists of known or suspected terrorists or terrorist organisations to determine whether a person seeking to open an account appears on any such list

Section 326 is implemented for depository institutions under 31 C.F.R. 1020.220 – Customer Identification Programs for Banks, Savings Associations, Credit Unions and Certain Non-Federally Regulated Banks.

709. Does FinCEN's "Customer Due Diligence Requirements for Financial Institutions" amend Section 326 requirements?

No. CIP requirements are not impacted; however financial institutions subject to CIP have new obligations around identifying and verifying beneficial owners. Previously, covered financial institutions were required to obtain beneficial ownership only in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Customer Due Diligence Requirements for Financial Institutions rule (Beneficial Ownership Rule), finalised in July 2016, requires financial institutions currently subject to CIP requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants

[FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership and/or significant control of legal entity customers.

For further guidance on the Beneficial Ownership rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

710. When must the financial institution obtain and verify the information?

Depository institutions must obtain the information prior to opening the account. Some exceptions may apply to obtaining the taxpayer identification number (TIN). Financial institutions must apply a risk-based approach in verifying the information within a reasonable time of account opening. For additional guidance on verification, please refer to the Verification section. For additional guidance on Customer Identification Programs (CIPs) for other types of financial institutions, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

711. Which financial institutions must comply with Section 326 – Verification of Identification?

The following financial institutions must comply with Section 326:

- Banks (including U.S. branches and agencies of foreign banks)
- Savings associations
- Credit unions
- Securities broker-dealers
- Mutual funds
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities

In some instances, money services businesses (MSBs), prepaid access providers and casinos and card clubs are required to obtain and verify customer identification information, similar to the CIP requirement. For further guidance, please refer to the sections: Money Services Businesses, Providers and Sellers of Prepaid Access and Casinos and Card Clubs.

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM) "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator" that will expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations

- State-chartered non-depository trust companies
- International banking entities

712. Is Section 326 applicable to a financial institution's foreign subsidiaries?

No. Section 326 does not apply to any part of the financial institution located outside of the United States. Nevertheless, financial institutions should implement an effective AML Program (including Section 326 requirements) throughout their operations, including in their foreign offices, except to the extent that requirements of the rule would conflict with local law.

713. Should financial institutions collect information beyond what is required by Section 326's CIP?

Yes. As part of its KYC procedures, a financial institution should collect additional information that enables it to understand the nature of its customer's activities and assess the risks associated with that customer. Examples include, but are not limited to, the following:

- Occupation or nature of business
- Purpose of account
- Expected pattern of activity in the account in terms of transaction types, dollar volume and frequency
- Expected origination and destination of funds

For additional guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

714. How does Section 326 correspond to FATF Recommendations?

The CIP rule generally parallels the FATF Recommendations:

- **Recommendation 10 – Customer Due Diligence** recommends the implementation of a risk-based customer due diligence program that identifies and verifies customers; identifies and verifies beneficial owners; and obtains information on the purpose and intended nature of the account.
- **Recommendation 11 – Recordkeeping** recommends the maintenance of relevant records for a minimum of five years.
- **Recommendation 17 – Reliance on Third Parties** suggests specific criteria that should be met before relying upon a third party to perform elements of a CIP (or any part of its AML Program) (e.g., regulated institution, due diligence program of third party consistent with the program of the financial institution).

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

Customer Defined

715. What does the term "customer" mean for purposes of Section 326?

A "customer" is any person who opens a new account or enters into another formal relationship after October 1, 2003. "Person" in this context includes individuals, corporations, partnerships, trusts or estates, joint stock companies, joint ventures or other incorporated organisations or groups.

716. Are there exemptions from the definition of "customer"?

The following are exempt from the definition of customer:

- A financial institution regulated by a federal functional regulator or a bank regulated by a state bank regulator
- A department or agency of the United States, a state or political subdivision of a state
- An entity that exercises governmental authority on behalf of the United States, a state or political subdivision of a state
- An entity (other than a bank) whose common stock is traded on the New York Stock Exchange (NYSE) or the American Stock Exchange (Amex/ASE) or whose common stock has been designated as a National Association of Securities Dealers Automated Quotations (NASDAQ) National Market Security listed on the NASDAQ Stock Market (except stock listed under NASDAQ Small-Cap Issues)
- A person who has an account with the financial institution that existed before October 1, 2003, if the financial institution has a reasonable belief that it knows the true identity of the person

717. Does exemption indicate that a financial institution need not conduct any due diligence on a customer?

No. A financial institution's KYC procedures should, on a risk-assessed basis, address all customers, even those exempt from a financial institution's CIP.

718. Is a person who has an existing relationship with an affiliate considered exempt from the definition of a "customer"?

No. The relationship must have existed with the financial institution itself, not an affiliate, to be excluded from the definition of "customer."

719. Is a person with a previous relationship with the financial institution considered exempt from the definition of a "customer"?

Only customers with existing relationships are exempt. For example, a customer who had a loan with a financial institution, repaid it, and subsequently obtained a new loan would be a new customer.

720. Is a person who becomes co-owner of an existing deposit account or new borrower who is substituted for an existing borrower through an assumption of a loan considered a "customer"?

Yes. What qualifies a person as a "customer" is the new establishment of a formal relationship between that particular customer and the financial institution, even though the account itself previously existed.

721. Do the requirements apply to loans that are renewed or certificates of deposit that are rolled over for customers with accounts existing before October 1, 2003?

Each time a loan is renewed or a certificate of deposit is rolled over, the financial institution establishes new formal banking relationships. Because the CIP rule excludes persons with existing relationships from the definition of "customer," assuming that the financial institution has a reasonable belief that it knows the true identity of the person and there was no break in the relationship, the institution need not perform its CIP when a loan is renewed or certificate of deposit is rolled over.

722. Who is the "customer" with respect to a commercial entity?

Financial institutions are required to verify the identity of the commercial entity, not the signers on the commercial accounts. The Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule), finalised in July 2016, requires covered financial institutions to obtain CIP information on beneficial owners of select legal entity customers. For further guidance, please refer to the Beneficial Owners section.

723. Who is the "customer" for purposes of trust accounts?

The "customer" is the trust, not the beneficiary(ies) of the trust, whether or not the financial institution is the trustee for the trust. Similar to commercial accounts, based on the financial institution's risk assessment of new accounts opened by customers that are not individuals, the institution may want to conduct due diligence on the individuals with authority or control over such an account, including signatories, settlors, grantors, trustees or other persons with the authority to direct the trustee, in order to establish the true identity of the account holder.

It is important to distinguish between "trust" accounts as an account type versus account holders that are legal trusts.

724. Who is the "customer" when an account is opened by an individual who has power of attorney for the owner of an account?

When an account is opened by an individual who has power of attorney for a competent person, the "customer" is the owner of the account. In the situation where the owner of the account lacks legal capacity, the individual with power of attorney is the "customer." Similarly, if parents open accounts on behalf of their minor children, the parents are the "customers" of the financial institution, not the children.

725. Who is the "customer" for purposes of escrow accounts?

If a financial institution establishes an account in the name of a third party, such as a real estate agent or an attorney who is acting as an escrow agent, then the financial institution's customer will be the escrow agent. If the financial institution is the escrow agent, then the person who establishes the account is the customer.

726. Who is the "customer" when there are joint account holders?

All joint account holders are deemed to be customers. This includes persons opening accounts for minors and unincorporated entities. It does not include beneficiaries, authorised users, authorised signers on business accounts or other financial institutions.

Account Defined

727. What does the term "account" mean for purposes of Section 326?

An "account" is a formal relationship in which financial transactions or services are provided. Examples of products and services where a formal relationship would normally exist include deposit accounts and extensions of credit; a safe deposit box or other safekeeping services; or cash management, custodian or trust services.

728. Are there exemptions from the definition of "account"?

An "account" does not include:

- Products or services for which a formal banking relationship is not established with a person (e.g., check cashing, wire transfers, sales of money orders)
- An account that the bank acquires (as a result of acquisitions, mergers, purchase of assets)
- Accounts opened for the purpose of participating in an employee benefit plan established by an employer under the Employee Retirement Income Security Act of 1974 (ERISA). In such cases, the plan administrator and not the plan participant has control over the account, thus personal identification from each participant is not required

Such circumstances would not require the institution to implement its CIP. However, this does not exempt an institution from recordkeeping and reporting requirements. The institution still must obtain the minimum information required for reporting in regard to Currency Transaction Reports (CTRs), Suspicious Activity Reports (SARs) and recordkeeping requirements (e.g., Purchase and Sale of Monetary Instruments, Funds Transfer Recordkeeping Rule, the Travel Rule).

Verification

729. Are financial institutions required to confirm every element of customer identification information used to establish the identity of their customers?

Financial institutions need not confirm every element of customer identifying information; rather, they must verify enough information to form a reasonable belief that they know the true identity of their

customers. The CIP must include procedures for verifying the identity of customers and whether documentary methods, non-documentary methods or a combination thereof will be used and must require additional verification for customers that are non-individuals, based on the financial institution's risk assessment of the customer (e.g., verifying the identity of account signatories). It also must contain procedures for responding to circumstances in which the financial institution cannot form a reasonable belief that it knows the true identity of a customer.

730. What does the term "reasonable belief" mean for Section 326 purposes?

The regulation does not provide any guidance as to what constitutes a "reasonable belief."

Some financial institutions have established account opening requirements above and beyond the minimum requirements (e.g., salary/revenue, occupation/industry) that, if received, would provide a basis for a financial institution to decide it has reasonable belief that it knows the customer. Other financial institutions require the account officer to certify he or she has reasonable belief that he or she knows the identity of the customer. Regardless of the financial institution's definition, the financial institution should clearly define the term within its CIP.

731. What are the obligations or requirements for financial institutions to update customer identification information for existing customers?

Existing customers are exempt from the verification requirements on the condition that the financial institution has a reasonable belief that it knows the true identity of the customer. To a large extent, the acceptability of exempting existing customers from CIP requirements will depend on the strength of the financial institution's customer identification procedures prior to implementation of its CIP. Financial institutions that had strong customer identification procedures will have a better case for exempting customers.

732. What are some examples of documentary methods of verification?

Documentary verification may include physical proof of identity or incorporation (i.e., visual inspection of documents). Examples include, but are not limited to, an unexpired driver's license, passport, business license, certificate of good standing with the state, or documents showing the existence of the entity, such as articles of incorporation. These documents can be presented physically at the time of account opening, as well as virtually (e.g., opening an account with a financial institution online by providing a driver's license number in an electronic form).

733. What are some examples of non-documentary methods of verification?

Non-documentary verification may include positive, negative or logical verification of a customer's identity. Positive verification ensures that material information provided by customers matches information from third-party sources. Negative verification ensures that information provided is not linked to previous fraudulent activity. Logical verification ensures that the information is consistent (e.g., area code of the home number is within the ZIP code of the address provided by the customer).

Examples of non-documentary verification include phone calls; receipted mail; third-party research (e.g., internet or commercial databases); electronic credentials, such as digital certificates; and site

visits. Site visits should be conducted using a risk-based approach and should not be limited to account opening, but also conducted periodically for high-risk relationships such as foreign correspondent banking relationships.

Regardless of the type of non-documentary verification used, a financial institution must be able to form a reasonable belief that it knows the true identity of the customer.

734. What resources are currently available to financial institutions to assist in the verification process?

Various public record search engines and commercial databases allow financial institutions to conduct ID matches (e.g., determining that a customer's TIN is consistent with his or her DOB and place of issue) and to check for prior fraudulent activity. For further guidance, please refer to the AML/CFT Technology, KYC Process and Customer and Transaction List Screening sections.

735. Can a financial institution open an account for a customer even if it cannot form a reasonable belief that it knows the customer's true identity?

Although a financial institution may allow a customer under certain circumstances to use an account while the financial institution attempts to verify the customer's identity, the financial institution's CIP procedures should identify the terms under which this will occur, when the financial institution should close an account after attempts to verify the customer's identity have failed and when the financial institution should file a SAR.

736. Should financial institutions conduct verification for individuals with authority or control over a business account (e.g., authorised signers, grantors)?

Based on its risk assessment, a financial institution may require identifying information for individuals with authority or control over a business account for certain customers or product lines.

737. Should subsidiaries of financial institutions implement a CIP?

The federal banking agencies take the position that implementation of a CIP by subsidiaries is appropriate as a matter of safety and soundness and protection from reputation risks.

738. What types of addresses can financial institutions accept as identifying information?

For an individual, Section 326 requires that a residential or business street address be obtained. If an individual does not have a residential or business street address, the following can be accepted:

- An Army Post Office (APO) box number, Fleet Post Office (FPO) box number
- Rural route number
- The residential or business street address of next of kin or of another contact individual

For companies, a principal place of business, local office or other physical location must be obtained.

739. Can a financial institution accept a rural route number?

Yes. A rural route number is a description of the approximate area where the customer is located. These types of addresses are commonly used in rural areas and are acceptable for a customer who, living in a rural area, does not have a residential or business address.

740. What type of identification number can financial institutions accept?

A taxpayer identification number (TIN) should always be obtained for U.S. persons. For non-U.S. persons, one or more of the following should be obtained:

- TIN
- Passport number and country of issuance
- Alien identification card number
- Number and issuing country of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

The identification obtained must be government-issued and unexpired. Although Section 326 does not prescribe that the form of identification bear a photograph in all cases, many financial institutions make this a requirement.

741. What steps should a financial institution take if the customer has applied for, but has not yet received, a TIN?

The financial institution's CIP should include procedures for opening an account for a customer who has applied for, but has not yet received, a TIN. The financial institution's CIP must include procedures to confirm that the TIN application was filed before the customer opens the account. Additionally, the financial institution must take measures to ensure it has received the TIN in a reasonable amount of time.

742. Can a financial institution open an account for a U.S. person who does not have a TIN?

Though the financial institution does not need to have the TIN at account opening for new customers, the financial institution must receive the TIN in a reasonable amount of time. Financial institutions, however, are able to open additional accounts for existing customers without TINs if they have a reasonable belief that they know the identity of the customer. The financial institution should have procedures in place to track compliance with this requirement and close accounts, as appropriate.

743. Can financial institutions rely on other types of identification cards other than a passport?

The decision as to whether to rely on other forms of identification (e.g., Matricula Consular IDs) must be made by the financial institution. Regardless of this decision, the financial institution must be able to form a reasonable belief that it knows the true identity of its customers.

Updating CIP for Existing Customers and on an Ongoing Basis

744. What are the obligations of financial institutions to update CIP information for existing customers?

Financial institutions are exempt from performing CIP on existing clients so long as the institution has a "reasonable belief" that it knows the true identity of the customer. The regulation does not provide any guidance as to what constitutes "reasonable belief."

To a large extent, the acceptability of exempting existing customers from CIP requirements inevitably will depend on the strength of the financial institutions' customer identification procedures prior to implementation of its CIP. Financial institutions that had strong customer identification procedures will have a better case for exempting customers.

745. What are the obligations of financial institutions to update customer information beyond CIP for existing customers?

A customer's information should be updated if there are significant changes to the customer's transaction activity or the risk level to the customer's account. Financial institutions should consider a risk-based approach to updating customer information beyond CIP, such as nature of business/occupation and expected activity.

The Customer Due Diligence Requirements for Financial Institutions final rule (Beneficial Ownership Rule), issued in May 2016, clarified the obligations of covered financial institutions with regard to updating customer information (e.g., CDD/EDD, customer risk profile) on an ongoing basis. While the expectation to update customer information is not a categorical requirement, the frequency and nature of this review should be based on the customer's risk rating and results of suspicious activity monitoring, consistent with existing AML/CFT laws and regulations.

For additional guidance on obtaining and updating customer information beyond CIP, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

Record Retention

746. Should copies of identifying information be made and retained?

Section 326 does not require a financial institution to make copies of identifying information. However, Section 326 does require a financial institution to retain records of the method of identification and the identification number. For example, if an individual's passport was reviewed as identifying information, the financial institution should note the fact that the passport was seen, and should document and retain the passport number and issuing country. While it is not required that identification be copied and retained, financial institutions may choose to adopt this procedure as a leading practice, although they also must be mindful of the implications of maintaining copies of identification in light of fair lending and other anti-discrimination laws.

747. How long must original account opening information be maintained?

Section 326 requires that a financial institution retain the identifying information obtained at account opening for five years after the date the account is closed or, in the case of credit card accounts, five years after the account is closed or becomes dormant.

748. How does the record retention period apply to a customer that opens multiple accounts in a financial institution?

If several accounts are opened for a customer, all identifying information about a customer obtained under Section 326 must be retained for five years after the last account is closed or, in the case of credit card accounts, five years after the last account is closed or becomes dormant.

749. How does the record retention period apply to a situation where a financial institution sells a loan but retains the servicing rights to the loan?

When a loan is sold, the account is "closed" under the record retention provision, regardless of whether the financial institution retains the servicing rights to the loan. Thus, records of identifying information about a customer must be retained for five years after the date the loan is sold.

750. If the financial institution requires customers to provide more identifying information than the minimum required by Section 326 at account opening, is it required to keep this information for five years?

Yes. If the financial institution obtains other identifying information at account opening in addition to the minimum required, such as the customer's phone number, then this information must be retained for the same period as the required information.

List Matching

751. What requirements does Section 326 impose on financial institutions regarding list matching?

Financial institutions also are required to screen their customers against government sanctions lists to determine whether the individual/entity appears on any list of known or suspected terrorists or terrorist organisations. For additional guidance on government sanctions, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

Customer Notice

752. What notification requirements does Section 326 impose?

A financial institution is obligated to notify its customers that it is requesting information to verify identity. Many financial institutions have incorporated the notification language into their account opening documentation in order to ensure that the notice is properly delivered to both primary and joint account holders.

753. Should notifications be provided to all owners of a joint account?

Yes. Notice must be provided to all owners of a joint account. However, a financial institution may satisfy this requirement by directly providing the notice to any account holder of a joint account for delivery to the other owners of the account.

754. Must this notification to customers be provided in writing?

Section 326 does not require that the notification be in writing, but it must be provided in a manner reasonably designed to ensure that a customer is able to view the requirement or is given it before opening the account.

Third-Party Reliance

755. Can a financial institution rely upon a third party to conduct all or part of the financial institution's CIP?

Yes. A financial institution may rely on other federally regulated institutions to conduct all or part of the financial institution's Customer Identification Program (CIP) when the following conditions are met:

- Such reliance is reasonable
- The other financial institution is regulated by a federal functional regulator
- The other financial institution is subject to a general Bank Secrecy Act (BSA) compliance program requirement
- The other financial institution shares the customer with the financial institution
- The two institutions enter into a reliance contract that contains certain provisions

756. What obligations does Section 326 impose on third-party financial institutions conducting part or all of the financial institution's CIP?

The third-party financial institution must provide an annual certification that it has implemented its AML Program and that it will perform (or its agent will perform) the specified requirements of the financial institution's CIP.

757. How does Section 326's third-party reliance provision correspond to FATF Recommendations?

FATF Recommendation 17 – Reliance on Third Parties suggests the following criteria should be met before relying upon a third party to perform elements of a CIP (or any part of its AML Program):

- Ability to obtain copies of identification data and related information from the third party without delay

- Third party has implemented a customer due diligence and recordkeeping program consistent with the financial institution
- Third party is regulated
- Enhanced measures for third parties located in high-risk jurisdictions

For further guidance on international standards, please refer to the Financial Action Task Force section.

758. What guidance has been issued on third-party service providers (TPSP)?

The following are examples of guidance that has been issued on third-party service providers:

- **Third-Party Payment Processors – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 17: Reliance on Third Parties** (2012) by the Financial Action Task Force (FATF)
- **Retail Payment Systems** and **Wholesale Payment Systems Booklet** (2004) within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Third-Party Senders and the ACH Network: An Implementation Guide** (2012) by The Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)
- **Bank Use of Foreign-Based Third-Party Service Providers** (2002) by the Office of the Comptroller of the Currency (OCC)
- **Risk Management Principles for Third-Party Relationships** (2001) by the OCC
- **Payment Processor Relationships** (2012) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance on Managing Third-Party Risk** (2008) by the FDIC

Section 352 – AML Program

Program Basics

759. What are key elements of an effective AML Program as required by Section 352 of the USA PATRIOT Act?

At a minimum, Section 352 requires financial institutions to establish AML Programs, which previously included the following "four pillars":

- Development of written internal policies, procedures and controls
- Designation of an AML compliance officer

- Ongoing AML employee-training program
- Independent testing of the AML Program

Since FinCEN issued the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) in July 2016, a fifth pillar has been added to the AML Program:

- Ongoing risk-based monitoring of customer activity and information with updates as necessary

The Beneficial Ownership Rule did not add new AML/CFT requirements for financial institutions; it only served to make existing AML/CFT expectations explicit requirements for the sake of clarity and consistency. The fifth pillar emphasises the importance of current and complete customer due diligence to support the identification of suspicious activity.

Section 352 is implemented for depository institutions under 31 C.F.R. 1020.210 – Anti-Money Laundering Program Requirements for Financial Institutions Regulated Only by a Federal Functional Regulator, Including Banks, Savings Associations and Credit Unions.

760. Which types of financial institutions are required to maintain an AML Program as required by Section 352?

At the time of this publication, the following financial institutions were required to maintain an AML Program:

- Depository institutions (e.g., insured banks, commercial banks, private banks, credit unions, thrift and savings institutions)
- Money services businesses (MSBs) (e.g., issuers or sellers of money orders or traveller's checks, check cashers, dealers in foreign exchange, providers and sellers of prepaid access, money transmitters)
- Broker-dealers in securities
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Mutual funds
- Operators of credit card systems
- Insurance companies
- Dealers in precious metals, precious stones or jewels
- Loan or finance companies (nonbank residential mortgage lender or originator [RMLOs])
- Housing government-sponsored enterprises (GSEs)

Rules have been proposed for the following financial institutions but have yet to be finalised or were withdrawn:

- Persons involved in real estate settlements and closings
- Unregistered investment companies

- Investment advisers
- Commodity trading advisers

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM) "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator" that will expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to, the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations
- State-chartered non-depository trust companies
- International banking entities

761. Does FinCEN's "Customer Due Diligence Requirements for Financial Institutions" amend Section 352's AML Program requirement?

FinCEN's "Customer Due Diligence Requirements for Financial Institutions" final rule (Beneficial Ownership Rule), finalised in July 2016, does not amend what financial institutions must implement as part of an AML Program but it does seek to include ongoing due diligence and monitoring as the fifth pillar of the AML Program.

Previously, covered financial institutions were required to obtain beneficial ownership information in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule requires financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, FCMs and IBs) to identify and verify the identity of beneficial owners with 25 percent or greater ownership and/or significant control of legal entity customers.

For further guidance on the proposed rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

762. Should the AML Program be limited to the key elements above as required by Section 352 of the USA PATRIOT Act?

No. The AML Program should be customised to the institution and cover all aspects of the business. An effective AML/CFT Compliance Program begins with the establishment of a strong governance framework that clearly outlines the following:

- **Board of Director and Senior Management Support and Oversight**
- **Designation of an AML Compliance Officer and Well-Defined Roles and Responsibilities** – For further guidance, please refer to the Designation of AML Compliance Officer and the AML/CFT Compliance Organisation section.
- **Risk Assessments** – For further guidance, please refer to the Enterprisewide Risk Assessment, Line of Business/Legal Entity Risk Assessment, Horizontal Risk Assessment, Geographic Risk Assessment, Product/Service Risk Assessment, Customer Risk Assessment and OFAC/Sanctions Risk Assessment sections.
- **Customer Acceptance and Maintenance Program** – For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence, Section 326 – Verification of Identification, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Know Your Customer Types sections.
- **Large Currency Monitoring and Currency Transaction Report Filing Program** – For further guidance, please refer to the Currency Transaction Reports section.
- **Monitoring, Investigating and Suspicious Activity Report Filing Program** – For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Reports sections.
- **OFAC Sanctions Compliance Program** – For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.
- **Information Sharing** – For further guidance, please refer to Section 314(a) – Cooperation Among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities, Section 314(b) – Cooperation Among Financial Institutions and Section 505 – Miscellaneous National Security Authorities (National Security Letters [NSLs]) sections.
- **BSA Recordkeeping and Retention Program** – For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule, Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, Form 8300, Report of Foreign Bank and Financial Accounts, Report of International Transportation of Currency or Monetary Instruments and Registration of Money Services Businesses sections.
- **Independent Testing** – For further guidance, please refer to the Independent Testing section.
- **Training** – For further guidance, please refer to the AML Training section.

To distinguish the AML Program with "five pillars," this publication will use "AML/CFT Compliance Program" when referencing the expanded program.

It is important to note that not all types of financial institutions are required to have each of the key components listed above. For additional guidance on the AML/CFT requirements of nonbank financial institutions (NBFIs), please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

763. How often should the AML Program be reviewed and approved?

The AML Program should be updated on an ongoing basis to address changing risks facing the financial institution (e.g., new products and services, new target markets), as well as changing control structure throughout the organisation (e.g., upgrades to or implementation of new AML/CFT monitoring systems, added roles and responsibilities of compliance staff). At minimum, however, the AML Program should be approved by the board of directors and senior management on an annual basis or when material changes are made to the AML Program.

764. What are the key elements of an effective AML/CFT governance framework?

Among the keys to establishing and maintaining an effective AML/CFT governance framework are:

- Strong and evident support of the board of directors and executive management for a culture of compliance, which is reinforced, among other ways, through a clearly defined risk appetite statement, appropriate limits, and the institution's performance review and compensation decisioning processes.
- A designated AML compliance officer with the necessary skills, authority and support to manage the AML/CFT Compliance program across the entire organisation.
- An adequate number of dedicated skilled resources, which will be determined by factors such as the size, complexity and geographic reach of the institution as well as the extent to which the compliance effort is enabled by technology.
- Robust policies and procedures that contain clear delineation of roles and responsibilities of the first, second and third lines of defence including obligations for "credible challenge" or "effective challenge."
- Effective, dynamic processes for assessing money laundering/terrorist financing and sanctions risk.
- AML training, which is appropriately customised to different audiences within the institution.
- A strong working relationship among the AML/CFT compliance organisation and other groups within the organisation (such as Legal and Fraud) with which the AML/CFT compliance organisation would be expected to interact.
- Appropriately selected and maintained technology to support, as examples, transaction monitoring and sanction screening.
- Robust management reporting that includes the necessary metrics to measure and monitor risks and performance.
- Ongoing monitoring and periodic independent testing of the effectiveness of the program.

765. What is a culture of compliance?

A culture of compliance is one in which management and staff of an organisation do the right thing because they know it is what is expected, that the organisation will support them, and where they are not afraid to surface compliance issues for fear of retribution or retaliation. FinCEN recently stated, "[A] good compliance culture is one where doing the right thing is rewarded, and where 'looking the other way' has consequences."

766. How can financial institutions cultivate a strong culture of compliance?

In August 2014, FinCEN issued an advisory suggesting how financial institutions can cultivate a strong culture of compliance through:

- Efforts to manage and mitigate AML/CFT deficiencies and risks are not compromised by revenue interests;
- Implementation of an effective AML/CFT Compliance Program that is tested by independent and competent parties;
- Adequate human and technological resources dedicated to the AML/CFT compliance function;
- Active support and understanding of AML/CFT and sanctions compliance efforts by leadership and employees; and
- Strong information-sharing mechanisms in place between lines of business and AML/CFT compliance with a mutual understanding of how BSA reports and data further AML/CFT efforts.

767. How can a financial institution maintain an effective AML Program?

A key element of maintaining an effective AML Program is to emphasise the importance of AML/CFT compliance across all business lines, as well as to demonstrate the importance of the AML Program to customers. Building a compliance culture throughout the financial institution will lead to a stronger and more effective compliance program, as well as deter unwanted risks for the financial institution. Some common practices to encourage compliance throughout the financial institution include:

- Ensuring consistency between the practices of the institution and policies and procedures
- Embedding compliance requirements into business processes
- Ensuring timely communication between the compliance department and senior management on compliance matters
- Establishing roundtables or group forums around compliance matters
- Conducting customised compliance training sessions for lines of business
- Requiring attestation to a code of conduct as a condition of employment
- Communicating and enforcing specific and clear consequences for noncompliance
- Aligning compliance expectations and performance with incentive compensation programs and compensation decisions

- Developing key performance indicators (KPIs) for measuring the effectiveness of the compliance program

768. What are the most common gaps in the AML/CFT compliance efforts of financial institutions?

Often financial institutions do not recognise the breadth and applicability of the AML/CFT laws and regulations, and thus underestimate the resources and commitment required to achieve compliance with the regulations. This has commonly resulted in the following problems and issues:

- Lack of adequate board of director and senior management oversight
- AML compliance officer (as well as other employees) lacks sufficient experience and/or knowledge regarding AML/CFT policies, procedures and tools
- Insufficient/inadequate resources dedicated to AML/CFT compliance
- Lack of specific and customised training of employees with critical functions (e.g., account opening, transaction processing, risk management)
- Failure to conduct adequate risk assessments (e.g., enterprisewide risk assessment, horizontal risk assessment, line of business/legal entity risk assessment, customer risk assessment, OFAC/Sanctions risk assessment)
- Failure to incorporate risk assessments into a suspicious transaction monitoring program, customer acceptance standards, audits, testing or training
- Inadequate KYC (e.g., CIP, CDD and EDD procedures at or after account opening, including inadequate controls over required fields, inadequate methods of obtaining and/or maintaining current information, lack of reporting capabilities over missing information and lack of verification procedures)
- Poor documentation maintained for investigations that did not lead to SAR filings
- Poor follow-up on SAR actions (e.g., close, monitor)
- Lack of reporting of key SAR information to senior management/board of directors
- Inadequate tuning, validation and documentation of automated suspicious activity monitoring systems
- Overreliance on software to identify transactions for which CTRs and/or SARs must be filed without fully understanding how the software is designed and what information it does and does not capture
- Exclusion of certain products from transaction monitoring (e.g., loans, letters of credit, capital markets activities)
- Lack of timeliness when filing CTRs and SARs (e.g., reports are manually filed via certified mail, and the date postmarked is not noted)

- Lack of or inadequate independent testing of the AML Program
- Lack of or untimely corrective actions to prior examination or audit findings

In order to identify potential gaps in a financial institution's AML Program, regulatory enforcement actions for AML/CFT deficiencies against other (similar) financial institutions should be reviewed to identify the specific violations and related action steps. This enables financial institutions to recognise and correct any potential weaknesses of their own before their next regulatory examination.

769. How do Section 352 requirements correspond to FATF Recommendations?

Section 352 parallels FATF Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries. Recommendation 18 advises financial institutions to implement a risk-based enterprisewide AML Program that includes foreign branches and subsidiaries that are consistent with the AML/CFT measures with the home country of the parent institution, to the extent that host countries permit. At a minimum, the program should include the following:

- Development of written internal AML policies, procedures and controls
- Designation of an AML compliance officer
- Ongoing AML employee-training program
- Independent testing of the AML Program

For further guidance on international standards, please refer to the Financial Action Task Force section.

Policies and Procedures

770. What is required under Section 352 of the USA PATRIOT Act with regard to policies and procedures?

A financial institution is required to have written AML policies and procedures as part of its AML Program.

Written AML policies and procedures should incorporate the following:

- Definition of money laundering and terrorist financing
- Legislative and regulatory framework (federal, state and international, if applicable)
- Standards of knowledge
- AML/CFT-related roles and responsibilities (including reliance placed on any third parties)
- Principal products and service offerings, customer base and geographic reach
- Prohibited products and service offerings, industries and customers, geographies, as applicable
- AML/CFT risk assessment methodologies (e.g., enterprisewide risk assessments, horizontal risk assessments, line of business/legal entity risk assessment, geographic risk assessment, product/service risk assessment, customer risk assessment, OFAC/Sanctions risk assessment)

- Customer acceptance, maintenance and termination standards (sanctions and PEP screening, CIP, CDD, EDD, KYC, Beneficial Ownership)
- Confidentiality and safeguarding of information
- Investigation, reporting and recordkeeping requirements for suspicious activity
- Examples of suspicious activities specific to the financial institution
- AML training (e.g., type of training, frequency of training)
- Use of systems to support the compliance effort, especially maintenance, tuning and validation of automated transaction monitoring systems
- Internal testing, which includes details of the steps and frequency of testing for compliance with the policies and procedures and the requirements for communicating the results of the testing and following up on any deficiencies noted
- Independent testing of the AML Program

771. Can one set of policies and procedures be applied uniformly throughout an institution?

The AML/CFT policy should be developed and adopted at the corporate level. Because financial institutions have many different departments and service offerings, a "one-size-fits-all" approach to procedures implementing the corporate policy generally would not be adequate. It is essential that procedures be customised to different departments and product areas to mitigate the money laundering and terrorist financing risk to that particular department and the specific product offering concerned.

772. Should an institution separate its policies from its procedures?

Since changes in AML/CFT policy require approval by senior management and/or the board of directors, many companies separate policies from procedures to allow for prompt modifications to procedures to provide clarification to policies or address new regulatory requirements.

773. Where should the AML/CFT policies and procedures be stored?

In many cases, the compliance department maintains the most recent versions of the AML/CFT policies and procedures for ease of updating. Some financial institutions, however, have a dedicated department that is responsible for maintaining all of the financial institution's policies and procedures in a central location. Wherever the policies and procedures are stored, the financial institution should have a mechanism in place to ensure that the most recent (and approved) policies and procedures are available for both reference and submission to the financial institution's regulators upon request.

In addition, many financial institutions post AML/CFT policies on an internal website so that all employees can reference the documentation.

774. How can a financial institution ensure all of its employees are familiar with its AML/CFT policies and procedures?

Many financial institutions include a review of AML/CFT policies and procedures during new-hire training and third-party introductions to the institution (depending upon an employee's/third party's roles and responsibilities within the institution). Additionally, the ongoing AML training of employees, required by Section 352, commonly addresses the AML/CFT policies and procedures.

Also, many compliance departments develop and distribute AML/CFT publications to staff. These publications reiterate roles and responsibilities outlined within AML/CFT policies, as well as requirements of AML/CFT laws and regulations applicable to the institution. They commonly are posted on the institution's internal website for future reference.

Designation of AML Compliance Officer and the AML/CFT Compliance Organisation

775. What is required under Section 352 of the USA PATRIOT Act with regard to the AML compliance officer?

Section 352 requires the designation of an AML compliance officer by the board of directors.

776. What is the role of the AML compliance officer?

The AML compliance officer generally is responsible for developing and maintaining the AML Program, including policies and procedures; ensuring the timely and accurate filing of required reports; coordinating AML training (within the compliance department and with relevant employees); and acting as the liaison for AML/CFT-related matters with regulators. In addition, many AML compliance officers oversee the transaction monitoring function.

Beyond these general points, the role of the AML compliance officer will vary by institution depending on its size and the availability of resources. In some instances, the AML compliance officer is responsible for OFAC compliance; in larger institutions, an OFAC compliance officer is responsible for OFAC compliance. Accordingly, the role of the AML compliance officer should be documented clearly in a job description.

777. Are AML compliance officers personally liable for their AML Programs?

There is a movement toward making compliance officers and other management personally and criminally liable for their compliance programs. Outside of the AML/CFT space, there's a shift toward individual accountability for corporate misconduct and wrongdoing (e.g., Department of Justice [DOJ] Memorandum on "Individual Accountability for Corporate Wrongdoing" issued by former Deputy Attorney General Sally Quillian Yates [Yates Memo]). On a state level, in 2015, the New York Department of Financial Services (DFS) proposed regulations requiring compliance officers to certify annually that their suspicious activity monitoring and sanctions filtering programs are in compliance, thus making AML Compliance Officers [AMLCOs] personally liable for submitting "false or incorrect" certifications if it was shown that their AML Program was deficient/non-compliant.

778. Are AML compliance officers required to certify that their AML Programs are in compliance with AML/CFT laws and regulations?

Federal AML/CFT laws and regulations do not require "certifications." Due to identified serious shortcomings in AML/CFT programs, New York State Department of Financial Services (DFS) enacted a first of its kind rule in 2016 requiring annual certifications of transaction monitoring and filtering programs by the board of directors or senior official(s) responsible for the management, operations, compliance and/or risk management of a covered institution.

For more guidance, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications in the Appendix.

779. What is an example of an enforcement action emphasising individual accountability?

To date, the largest public civil AML enforcement action against an individual was a US$250,000 fine and a three-year injunction barring compliance employment with any money transmitter against former chief compliance officer (CCO) of MoneyGram International Inc. (MoneyGram), Thomas E. Haider, commonly referred to as "The Haider Settlement" (May 2017).

In December 2012, MoneyGram entered into a Deferred Prosecution Agreement (DPA) with the DOJ with a forfeiture of US$100 million for aiding and abetting wire fraud and failing to maintain an effective AML Program. Initially, Haider faced a personal fine of up to US$5 million for his "wilful inaction." According to FinCEN's press release, Haider ultimately settled for a lower amount after admitting, acknowledging and accepting responsibility for the following:

- "[F]ailing to terminate specific MoneyGram outlets after being presented with information that strongly indicated that the outlets were complicit in consumer fraud schemes;
- [F]ailing to implement a policy for terminating outlets that posed a high risk of fraud; and
- [S]tructuring MoneyGram's anti-money laundering (AML) program such that information that MoneyGram's Fraud Department had aggregated about outlets, including the number of reports of consumer fraud that particular outlets had accumulated over specific time periods, was not generally provided to the MoneyGram analysts who were responsible for filing suspicious activity reports with FinCEN."

For further details on MoneyGram's enforcement action, please refer to Key U.S. Enforcement Actions and Settlements in the Appendix.

780. What skills and experience are necessary for an AML compliance officer to be effective?

AML compliance officers need both technical skills and leadership skills. Necessary technical skills include: understanding of the business of the institution and its risks to money laundering and terrorist financing; knowledge of AML/CFT and sanctions laws and regulations; analytical and investigative skills; problem solving ability; and a solid understanding of the technology used to support compliance efforts. The leadership skills that are important for an effective AML compliance officer include: strong people and project management skills; strong communication skills (up and down the organisation) with demonstrated ability to influence and advocate; and confidence and

conviction to raise compliance issues with executive management and the board of directors, as applicable.

781. To whom within the organisation should the AML compliance officer report?

There is no right or wrong answer for the reporting line of an AML compliance officer, except that the AML compliance officer should be independent of the lines of business and business units. Acceptable reporting lines may include the chief compliance officer, the chief risk officer or another C-level executive who is not primarily responsible for running a line of business. What is important is that the reporting line provides adequate autonomy to the AML compliance officer and that the AML compliance officer is appropriately positioned within the organisation to indicate the importance placed on this role by the board of directors and executive management. The AML compliance officer should also have unfettered access to the audit committee, compliance committee, risk committee, or other appropriate board-level committee in order to voice any concerns he/she may have about the institution's compliance.

Outside the United States, regulatory authorities may have requirements or strong views on the reporting lines of AML compliance officers, which need to be considered in the design of a global AML organisation.

782. What is the role of the board of directors with respect to the AML Program?

The board of directors is responsible for ensuring that adequate resources are provided to promote and support an effective AML Program. In addition, the board of directors is responsible for designating the AML compliance officer, for approving AML/CFT policy and for reviewing periodically the status of the AML Program, often through periodic reporting made by the AML compliance officer.

783. What is the role of senior management, with respect to the AML Program?

Senior management, together with the board of directors, is responsible for continually reinforcing the importance of compliance to all personnel of the financial institution. This is accomplished through creating an environment where compliance is of the highest priority through, for example, considering compliance in all employee evaluations and ensuring that the AML/CFT compliance department has the support and cooperation of all business units. Senior management also should ensure that the financial institution has adequate resources to perform its AML/CFT compliance responsibilities effectively and ensure that such responsibilities are being carried out in accordance with approved policies and procedures.

784. Is the AML compliance officer for a financial institution required to receive the board of directors' approval to file a SAR?

No. The AML compliance officer should not seek approval from the board of directors or any business line for Suspicious Activity Report (SAR) filings. Though the compliance department may involve the business to aid in its investigation of unusual or potentially suspicious activity, the department must make its own determination as to whether the activity identified warrants a SAR filing. In many

instances, the AML compliance officer makes the final decision to file or not file a SAR. In some instances, a committee is established to review the case and decide to file or not file a SAR.

It is important to note, however, that the board of directors and senior management should be notified of SAR filings. Since regulations do not mandate a particular notification format, financial institutions have flexibility in structuring their format and may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification as opposed to providing actual copies of SARs.

785. In addition to SAR-related information, what information should be included in periodic reports to senior management and/or the board of directors?

Management reporting is a process through which management (and the board of directors) are provided, routinely and on an as-needed escalation basis, the information they need to manage the operations and risks of the organisation. Management reporting will vary depending on the type of financial institution, the nature of the products and services it offers, and the clients it serves. The following are non-exhaustive examples of key risks and key performance indicators and other information related to the AML/CFT Compliance Program that may be considered:

- **Suspicious Activity Reports (SARs) and significant investigations**
  - Number of SAR filings and associated volume of suspicious activity and deposit/lending balance of named subjects
  - Explanations for significant changes in volume of SAR filings
  - Volume of alerts, investigations
  - Aging of alerts and investigations
  - Alert-to-investigation ratio, investigation-to-SAR ratio
  - Summary of significant investigations (e.g., high volume of suspicious activity, uncovered weakness in monitoring program, investigations involving insiders, politically exposed persons [PEPs])
- **Currency Transaction Reports (CTRs)**
  - Overall volume of cash activity
  - Number of CTR filings and associated volume of cash activity
  - Explanations for significant changes in volume of cash activity/CTR filings
- **Office of Foreign Assets Control (OFAC) and other sanctions reporting**
  - Number of OFAC blocked/rejected report filings and associated volume of blocked/rejected activity and deposit/lending balance of named subjects
  - Aging of "hits"
  - Results of OFAC/Sanctions risk assessment
- **Information sharing**

  - Number of confirmed 314(a) matches and associated deposit/lending balance of named subjects
  - Number of incoming/outgoing 314(b) requests and associated deposit/lending balance of named subjects
  - Number of National Security Letters (NSLs)
  - Number of subpoenas and other information requests
- **Training**
  - Number of exceptions (e.g., employees who have not completed or who have failed training)
  - Summary of significant updates to the training program
- **Staffing**
  - Significant staff changes, turnover trends, approved and unfilled positions
- **Technology**
  - Major changes to the automated systems being used to support the company's AML/CFT Compliance Program and rationale for the changes
  - Status of any major technology implementations, upgrades or changes affecting the AML/CFT Compliance Program
  - Results of independent validations of supporting technology models
- **Third-party reliance**
  - Periodic discussion of any third parties on which the company relies for any part of its AML/CFT or sanctions compliance programs and actions taken by the company to satisfy itself with third parties' compliance efforts
- **Risk assessments**
  - Results of executed AML/CFT risk assessments (e.g., enterprisewide risk assessment, horizontal risk assessment, line of business/legal entity risk assessment, geographic risk assessment, product/services risk assessment, customer risk assessment, OFAC/Sanctions risk assessment), including inherent risk, ratings of controls/control environment and residual risk
  - Changes in the institution's risk profile and explanations for what is driving the change
  - Summary of significant changes to risk assessment methodologies
  - Number of high-risk customers and associated deposit/lending balances
  - New products/services/transaction types and associated risks
  - New target markets (e.g., customer type, geography) and associated risks

- **Examination/independent testing/self-testing findings**
  - Summary of findings and status of corrective actions
- **Changes in laws, regulations or regulatory expectations**
  - Summary of new requirements and their impact on the company
- **Current events**
  - Details of recently reported money laundering/terrorist financing schemes, to the extent that the company may, because of its products/services and customers, be subject to risk and discussion of controls in place to mitigate such risks
  - Summary of recent AML enforcement actions and relevance of the issues cited to the financial institution

The content, level of detail and frequency of reports should be tailored to the audience (e.g., business line management, compliance, risk management, senior management, or board of directors).

786. To what extent is it appropriate to delegate AML/CFT compliance responsibilities to individuals within the business?

The business plays a critical role in ensuring that the institution complies with applicable AML/CFT requirements and internal policies and procedures. The extent to which individuals within the business are charged with specific compliance-related or quality assurance responsibilities (such as reviewing adequacy of Know Your Customer (KYC) information for new clients, risk rating clients, or adjudicating potential OFAC hits) is often a function of the size and complexity of the organisation. Delegating certain responsibilities in a larger institution may be the only practical way to manage compliance. Where activities are delegated to individuals within the business, the centralised compliance function should have responsibility for:

- Determining that the individuals within the business assigned compliance responsibilities are competent to carry out their duties.
- Developing consistent enterprise standards to guide the activities of all businesses.
- Periodically monitoring that business line personnel are discharging their responsibilities in accordance with enterprise standards and expectations.
- Proving input into performance evaluations of business line personnel with compliance responsibilities.

787. Should the compliance department be involved in the decision to offer new products?

The compliance department should be aware of a financial institution's plans to offer new products and services and should work with relevant parties in the institution to ensure compliance risks are considered appropriately in advance of the launch of a new product or service. The ultimate decision to offer a new product or service, however, rests with the business; however, the compliance function

should be on record if it believes the product or service exposes the institution to undue or difficult to manage risks.

788. Should the compliance department be involved in the decision to enter into customer relationships?

Many financial institutions have developed customer acceptance committees that meet on a regular basis to discuss high-risk prospects (e.g., those customers posing increased credit risk, AML/CFT risk, reputation risk) wishing to enter into a relationship with the financial institution. The committee should be composed of members from each business line and the compliance function. While the compliance department can provide its view on the risks associated with the prospect, the decision to enter into a customer relationship rests with the business. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

789. Should the compliance department be involved in the decision to exit a customer relationship?

As with customer acceptance committees, many financial institutions have developed committees that meet on a regular basis to discuss high-risk customers (e.g., those customers who have defaulted on a number of credit products, customers subject to SARs). The committee should be composed of members from each business line and the compliance function. While the compliance department can provide its view on the risks associated with the customer, and regulators encourage the compliance function to challenge the business, the ultimate decision to exit a customer relationship usually rests with the business. For further guidance, please refer to the Monitoring and Terminating Relationships with SAR Subjects section.

790. Should multinational institutions organise their AML/CFT compliance functions the same way in every jurisdiction in which they operate?

To the extent feasible, there are advantages to having a consistently designed AML/CFT compliance function in every jurisdiction in which a financial institution operates. However, it is important to note that regulatory bodies in some jurisdictions have strong views on how compliance functions are organised and to whom the AML compliance officer reports; in these cases, it is important to make adjustments to respect the local requirements and expectations.

For further guidance on international AML/CFT standards, please refer to the International Perspectives and Initiatives section.

AML Training

791. What is required under Section 352 of the USA PATRIOT Act with regard to AML training?

Section 352 requires an ongoing AML training program for relevant employees.

792. What are the key components of an AML training program?

An AML training program needs to be customised to an institution. For institutions with many different departments and products, it may even need to be customised further for each different department or product.

A basic AML training program should incorporate the following:

- Background on money laundering and terrorist financing
- Summary of the key AML/CFT laws and regulatory requirements (federal, state and international, if applicable)
- Requirements of the AML/CFT policies and procedures of the financial institution
- Summary of how the AML/CFT laws and regulatory requirements impact the financial institution
- Roles and responsibilities of the employees in attendance
- Suspicious activity red flags and case studies
- Consequences of noncompliance

793. What form does the training typically take?

The form of AML training depends on a financial institution's preference (e.g., cost, level of interaction). Financial institutions have several methods of delivering AML training:

- Computer-based training (CBT) (e.g., delivered through the intranet, internet or downloaded/installed applications which may be internally developed or vendor-provided)
- Face-to-face training (either internally developed or vendor-provided)
- Third party certification programs

For additional guidance on how technology can support an AML training program, please refer to the Training Software section.

794. Should external training be included as part of a financial institution's AML training program?

Although not required, outside seminars and conferences may be appropriate for employees with overall responsibility for AML/CFT compliance efforts (e.g., AML compliance officer, internal audit director). Financial institutions can keep abreast of industry standards through their interactions with peer institutions.

795. How often should the AML training program be updated?

The AML training program should be reviewed and updated as necessary to reflect current developments in and changes to laws and regulations, money laundering and terrorist financing trends and developments, and internal policy. It also should be reviewed or updated based on areas of weakness as indicated by employee test scores (assuming quizzes are given as part of the training).

796. Should OFAC training be included as part of the AML training program?

Since the OFAC Sanctions Listings include alleged narcotics traffickers, terrorists and proliferators of weapons of mass destruction (WMDs), financial institutions often consider the OFAC Sanctions Compliance Program to be a subset of their overall AML/CFT Compliance Program. As a result, OFAC training is often included in the AML training program.

797. How can a financial institution measure the effectiveness of the training provided?

Some financial institutions choose to provide employees with a quiz at the end of the training session, as this often encourages employees to take the training seriously. It also provides the compliance department with an idea of employee understanding of AML/CFT requirements and isolates topics that need to be expanded to improve the overall AML training program.

798. Who should attend AML training?

Employees, permanent or temporary, who have direct or indirect contact with customers, open customer accounts, or process transactions or customer information should attend AML training.

In addition, employees in compliance, accounting and internal audit departments, as well as those personnel in management functions (including senior management and board members), should attend AML training.

799. Is it sufficient for the AML compliance officer to attend only internal AML training?

Regulators expect that AML compliance officers have broad knowledge of industry trends and peer practices. The best way to gain this perspective is to attend external training and networking events. Some recent regulatory enforcement actions, in fact, have mandated that the AML compliance officer attend external training.

800. Should nonemployees (e.g., vendors, agents) attend the AML training of an institution?

The vendor's roles and responsibilities should be taken into consideration when determining if nonemployees should be required to attend AML training.

801. How frequently should employees attend AML training?

While there is no formal requirement regarding the frequency of AML training, employees should attend AML refresher sessions on at least an annual basis. Financial institutions may also consider providing certain employees (such as those in account opening, transaction processing and compliance roles) with training on a more frequent basis (e.g., semi-annually). New employees should receive training upon commencement of employment and prior to assuming their duties.

802. What records should be retained to evidence AML training of employees?

It is important that financial institutions retain records evidencing that their employees have attended AML training. Maintaining not only the attendance list, but also the agenda, training materials and employees' quiz scores (if applicable), will assist in assessing the overall quality of the AML training during the independent testing/audit of a financial institution's AML training program.

Independent Testing

803. What is required under Section 352 of the USA PATRIOT Act with regard to independent testing?

Section 352 requires a periodic independent testing of the AML Program.

804. How does independent testing of the AML Program differ from the AML compliance monitoring function?

The AML compliance department is responsible for developing and implementing an organisation's overall AML Program, including AML policies and procedures. Individual departments are required to adhere to those policies by developing their own procedures to comply with the organisation's compliance policies. The compliance department may monitor business-unit adherence to policies and procedures in a number of ways, including reviewing business-unit self-assessments and conducting periodic reviews. Independent testing must be conducted by individuals independent of the compliance function and, in the same way as an internal audit, is intended to test compliance with legal and regulatory requirements and internal AML-related policies, procedures and controls. Regulators expect that independent tests will be risk-based.

805. What does the term "risk-based" mean for independent testing purposes?

For the purposes of independent testing, "risk-based" means that the scope and approach (e.g., determining sample selection methodology and sample sizes) are based on consideration of an organisation's ML/TF risk, as determined by its own risk assessment and/or a risk assessment performed by the independent reviewer. Put simply, in a risk-based examination, priority is given to areas of highest risk as well as areas that were previously criticised.

806. What should the independent testing incorporate?

The objective of the independent testing is to assess compliance with the institution's AML Program, with particular focus on specific USA PATRIOT Act Section 352 requirements, including the development and maintenance of written policies, procedures and controls; the designation of an AML compliance officer; and the design and implementation of an AML training program. The policies and procedures must be tested to confirm that they contain procedures for meeting regulatory requirements and are updated in a timely manner to meet any newly developed regulatory requirements. A comprehensive independent test will include, at minimum, coverage of the following:

- Role of the board of directors and senior management
- The AML compliance organisation
- AML/CFT risk assessment methodologies (e.g., enterprisewide risk assessment, horizontal risk assessment, line of business/legal entity risk assessment, geographic risk assessment, product/service risk assessment, customer risk assessment, OFAC/Sanctions risk assessment)
- Customer acceptance and maintenance standards (CIP, CDD, EDD)
- Monitoring and investigation, including adequate transaction testing

- Recordkeeping and reporting
- AML Training
- AML policies and procedures
- Management reporting
- A review of the results of previous independent reviews and regulatory examinations
- Use of third parties
- Use of technology (e.g., implementation, maintenance, tuning, validation)

807. Should the OFAC Sanctions Compliance Program be included in the scope of the independent testing of the AML Program?

Since the OFAC Sanctions Listings include alleged narcotics traffickers, terrorists and proliferators of weapons of mass destruction (WMDs), financial institutions often consider the OFAC Sanctions Compliance Program to be a subset of their overall AML Program. For additional guidance on what should be considered with respect to independent testing of an OFAC Sanctions Compliance Program, refer to the Office of Foreign Assets Control and International Sanctions Programs section.

808. How often should the AML Program be independently tested?

The frequency of the independent testing should be based upon the risk profile of the institution. Typically, AML Programs are tested every 12 to 18 months.

809. Can AML Program elements be tested separately, or does the entire program need to be tested at one time?

Elements of the AML Program can be tested separately. A summary of the testing results should be prepared periodically to provide an overall assessment of the AML Program.

810. If an institution manages its AML Program at the corporate level, does there need to be a separate independent testing for each legal entity?

The requirement that an independent testing be conducted applies to each covered legal entity, so even though the AML Program may be uniform across the organisation, either a separate independent testing report should be prepared for each applicable legal entity or the entire report should be presented to the board of each legal entity.

811. What are some of the common criticisms of independent AML testing?

Regulatory criticisms of AML testing have included inexperienced or inadequately trained testers/auditors, insufficient or not appropriately risk-based coverage of the AML Program, insufficient transaction testing, limited attention paid to the quality of training, limited understanding and inadequate testing of automated monitoring software, poor quality work papers, and inadequate follow-up on previously identified issues in prior audits or in regulatory examination reports.

812. Have financial institutions ever been penalised for not having performed an independent review, or for having a review conducted that was deemed to be inadequate?

Yes. The requirement to perform periodic independent testing is one of the four required components of an AML Program. As such, not performing an independent review or not addressing cited deficiencies in the independent review provides the basis for an enforcement action. It is not uncommon for AML/CFT-related enforcement actions to cite multiple deficiencies related to independent testing.

813. How should the independent testing address senior management and board involvement and reporting?

Independent testing of senior management and board involvement and reporting should include testing to ensure that required reports (e.g., information on SARs) are provided to the board of directors. The testing also should evaluate whether management and the board of directors are sufficiently informed of the trends and issues related to AML/CFT compliance, internally and within the industry.

814. What should be considered with respect to independent testing of the compliance organisation?

An assessment of the compliance organisation must include verifying that the institution has a duly appointed AML compliance officer as required by Section 352 and making a determination that this individual has the experience, qualifications, and stature within the organisation necessary to direct the AML Program. However, the success of the AML/CFT compliance effort depends on much more than the performance of one individual. Other factors that impact the effectiveness of the compliance effort which should be considered include the resources (staff and tools) available for AML compliance; the autonomy of the AML/CFT compliance function; the level of access the AML compliance officer has to senior management, counsel, and the audit or compliance committee; how well roles and responsibilities with respect to AML/CFT compliance have been delineated throughout the institution; and the extent to which senior management and the board of directors are involved in the AML/CFT compliance effort.

815. How should the independent testing address the AML/CFT risk assessment methodologies?

The independent testing should include a reasonableness test of the risk assessment methodologies (e.g., a determination that the data used for risk assessments is accurate and complete, a determination of whether risk assessment methodologies incorporate the right variables to identify the institution's high-risk accounts and customers; tests to determine whether risk ratings are applied consistently). Additionally, the independent tester should assess how the risk assessment process has an impact on other aspects of the institution's AML Program, notably the account opening (CIP/CDD/EDD/KYC) process, transaction monitoring, compliance monitoring, audits and training. Effective and meaningful risk assessment processes will drive the documentation requirements for new

customers, be used to establish priorities for monitoring, and assist AML/CFT compliance with focusing its resources on business lines and customers posing the highest risk in terms of money laundering and terrorist financing. For additional guidance on risk assessment methodologies, please refer to the Risk Assessments section.

816. What should the independent testing of monitoring and investigations include?

Independent testing of monitoring should include verifying that the institution has procedures for (a) keeping customer information current (such as requirements that customer profiles are updated on a periodic basis, customer visits/calls are documented for the file, and adequate follow-up occurs on any media or other third-party information about a customer), and (b) transaction and account monitoring. The independent testing also should consider the staffing of the monitoring and investigative functions, both in terms of whether there is an adequate number of people and if they have the experience and skills necessary to be effective.

Tests also should be conducted to assess the timeliness and quality of the monitoring and investigative functions; this should include reviewing a sample of transactions/accounts (often both) to determine how potentially unusual or suspicious activities are identified, what prompts the decision to conduct an investigation, and how well-documented and timely the institution's decisions are to file or not file a Suspicious Activity Report (SAR). Additionally, the independent testing should consider reviewing a sample of investigations, as well as a sample of SARs filed to determine whether they have been prepared in accordance with the guidance provided by FinCEN.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

817. Are there additional considerations that should be included for testing AML/CFT technology that is used to support suspicious activity monitoring processes?

The most common technology solutions used to support suspicious activity monitoring processes include suspicious transaction monitoring software and case management software, collectively referred to as the monitoring system. When conducting an independent test, these technology solutions should be tested not only for how end users are utilising the capabilities of the system, but the operating effectiveness of the system as well. Some institutions opt to include some of this testing as part of their overall independent test of the AML/CFT Compliance Program or separately, as part of an IT systems-specific review.

For testing to determine whether the monitoring system is utilised adequately by end users to address the unique monitoring needs and transactional risks of a financial institution, the review should include, but not be limited to, the following:

- **Coverage** – Does the system accommodate all of the products, services and transactions of the institution? If so, did end users tailor the system to monitor these products, services and transactions adequately?
- **Risk-based approach** – Does the system allow for consideration of risk ratings (e.g., customers, transactions, alerts)? If so, have risk ratings been used in the design of monitoring rules and determination of thresholds?

- **Types of monitoring rules** – What types of monitoring rules and parameters for generating alerts does the system perform (e.g., artificial intelligence (AI), rules-based, profiling, outlier detection)? Did end users implement meaningful rules and parameters to detect potentially suspicious activity? Are rules subject to periodic review and tuning?
- **Case management** – How does the system output alerts? Does the system have an adequate case management/audit trail functionality? If so, did end users adequately document reviews of alerts and/or investigations within the system?

A review of the operating effectiveness of a monitoring system should include, but not be limited to, the following:

- **Data integrity and continuity** – Does information being input into the system correspond to the information output by the system?
- **Data source and feeds** – Is the information needed for the system to operate correctly actually being captured by the system? This may include the linking and tying of multiple information platforms across the institution.
- **Data processing** – Does the system perform its intended functions at the appropriate times, including as information is processed or on a cumulative periodic basis?
- **Model risk management** – Is there effective review and challenge of the system by knowledgeable personnel?
- **Model Governance** – Does the institution have effective policies and procedures for managing the entire lifecycle of deployed models?
- **Third party risk management** – Does the institution have adequate procedures for management the risks of vendor-supplied technology?
- **Security and change management** – Are there restrictions or monitoring tools in place to prohibit users from making modifications to the software's capabilities?
- **Information reporting** – Do the end-user reports generated by the system contain the appropriate information and accurately reflect the various types of occurrences which may take place within the system?
- **Business continuity** – Are technologies that support the compliance program considered in the institution's business continuity/disaster recovery planning?

For further guidance on technology solutions, please refer to the AML/CFT Technology section.

818. What should the independent testing of recordkeeping and reporting requirements include?

In addition to SAR filing requirements, financial institutions may be subject to the following AML/CFT-related recordkeeping and reporting requirements: CTRs, designation of exempt persons, CMIRs, FBARs, wire transfer recordkeeping, monetary instrument recordkeeping, foreign bank certifications, 314(a) notifications, 314(b) participation, the "120-hour rule," OFAC Sanctions

Compliance Program, Special Measures and record retention requirements. The audit of recordkeeping and reporting should be designed to include testing of appropriate samples for each of the applicable requirements.

819. Determining whether AML training is taking place seems straightforward, but what else about the AML training program should be considered as part of the independent testing?

In addition to monitoring attendance to ensure all designated individuals have received training, it is important for the independent testing to consider the quality of the AML training being provided. That means making a determination of whether the training is customised appropriately to the audience. A financial institution may offer generic AML training to introduce management and employees to AML concepts and issues, but individuals who play key roles in carrying out the institution's AML Program (including, for example, individuals with customer contact and operations staff) should be provided with customised training that focuses on clearly explaining the responsibilities these individuals have in helping the institution combat money laundering and terrorist financing, and includes "red flags" appropriate to the areas in which the individuals work.

The audit also should consider the importance the financial institution places on AML training. In part, this may be gauged by whether the institution is diligent in ensuring that designated individuals attend training. Another factor to consider may be whether training is followed by testing and, also, what (if anything) happens to individuals who are unable to pass the test.

820. How should the independent testing address third-party reliance?

The Customer Identification Program (CIP) rules specifically allow financial institutions to rely on other regulated financial institutions to conduct elements of CIP. In this instance, the independent testing should verify that the third-party financial institution is subject to AML/CFT requirements and is regulated by a federal functional regulator, that the two institutions have entered into a contract delineating their respective responsibilities, and that the third-party financial institution certifies annually that it is complying with the requirements of the contract.

Financial institutions may rely on other financial institutions for other elements of their AML Program (e.g., monitoring). In these instances, the independent testing also should assess how the third party was selected, verify the existence of detailed contractual arrangements, and determine how the relying financial institution satisfies itself that the third-party financial institution is meeting its contractual arrangements. Often, internal audit or SSAE 18 reports may be available for review by the independent tester.

Financial institutions may rely on nonfinancial institution third parties, as well. Real estate brokers or automobile dealers, for example, may act as de facto agents of a bank; in these instances, the independent testing should include steps to determine how the financial institution conducts due diligence of its business associates and how it communicates its expectation for AML/CFT compliance to these associates.

821. Who should perform the independent testing of an institution's AML Program?

The independent testing of an institution's AML Program must be performed by individuals who are not responsible for the execution or monitoring of the institution's AML Program.

An institution's internal audit department can perform the testing, individuals not involved in AML/CFT compliance or AML/CFT-related operations can perform the testing, or the institution can engage an outside party to perform such testing. In every case, the individuals performing the independent review must be qualified to execute the testing.

822. What experience and qualifications are necessary for conducting independent tests of AML Programs?

In addition to basic auditing skills, independent testers must have knowledge of AML/CFT and sanctions risks and the applicable legal and regulatory requirements. They also must have a good understanding of the financial institution's customer base and the products and services it offers so they can identify the risks involved. Increasingly, as financial institutions continue to expand how technology is used to support their compliance efforts, independent testers need technology skills, quantitative skills and a strong grasp of how AML/CFT software works as well as in-depth knowledge of data lineage and governance.

823. When should the independent testing of the AML Program be performed?

The independent testing of the AML Program should be done in accordance with the financial institution's applicable Section 352 requirements and regulatory expectations.

Additionally, an independent test of an AML Program should be conducted as part of the overall due diligence prior to acquiring new financial institutions to mitigate the risk of inheriting regulatory problems.

824. How should financial institutions evidence the performance of independent testing?

Upon completion of the independent testing, a written report should be issued to summarise the findings of the testing, including an explicit statement about the AML Program's adequacy and effectiveness. Any recommendations arising from the testing also should be documented, and management should provide a written comment as to how and when it will address those recommendations.

The written report should be provided to senior management and/or the board of directors, the compliance department and the internal audit department, as well as any other relevant individuals or departments.

Work papers and other supporting documentation also should be maintained.

Ongoing Monitoring & Updates

825. Did the new "fifth pillar" of the AML Program add additional AML/CFT requirements for financial institutions?

Since FinCEN issued the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) in July 2016, a fifth pillar has been added to the AML Program:

Ongoing risk-based monitoring of customer activity and information with updates as necessary.

The "fifth pillar" of the Beneficial Ownership Rule did not add new AML/CFT requirements for financial institutions; it only served to make existing AML/CFT expectations explicit requirements for the sake of clarity and consistency. The fifth pillar is implicitly required by existing suspicious activity reporting requirements. For further guidance on due diligence requirements, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

Section 505 – Miscellaneous National Security Authorities

826. What is a National Security Letter?

National Security Letters (NSLs) are written, investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) office and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following:

- Telephone and electronic communications records from telephone companies and internet service providers
- Information from credit bureaus
- Financial records from financial institutions

The authority to issue NSLs was expanded under Section 505 of the USA PATRIOT Act, which allows the use of NSLs to scrutinise U.S. residents, visitors or U.S. citizens who are not suspects in any ordinary criminal investigation.

827. Are NSLs subject to judicial review?

The USA PATRIOT Act Improvement and Reauthorisation Act of 2005 imposed safeguards on the use of NSLs including explicit judicial oversight. Under Section 505, NSLs cannot be issued for ordinary criminal activity, and may only be issued upon the assertion that information would be relevant to an ongoing terrorism investigation.

828. Are NSLs confidential?

NSLs are highly confidential. If accompanied by a nondisclosure order, financial institutions, their officers, employees and agents are precluded from disclosing to any person, except to persons necessary to comply with the order or with legal counsel, that a government authority or the FBI has sought or obtained access to records. Financial institutions that receive NSLs must take appropriate measures to ensure the confidentiality of the letters.

829. Should an institution automatically file a SAR upon receipt of an NSL?

No. A financial institution should not automatically file a SAR upon receipt of an NSL. The decision to file a SAR should be based on the institution's own investigation into the activity of the party(ies) that/who is the subject of the NSL. If a financial institution files a SAR after receiving an NSL, the SAR should not contain any reference to the receipt or existence of the NSL. The SAR should reference only those facts and activities that support a finding of unusual or suspicious transactions identified by the financial institution.

Questions regarding NSLs should be directed to the financial institution's local FBI field office. Contact information for the FBI field offices can be found at www.fbi.gov.

OFFICE OF FOREIGN ASSETS CONTROL AND INTERNATIONAL SANCTIONS PROGRAMS

OFAC Basics

830. What is the role of the Office of Foreign Assets Control (OFAC)?

The purpose of OFAC, the successor of the Office of Foreign Funds Control (FFC), is to promulgate, administer and enforce economic and trade sanctions against certain individuals, entities, and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy.

The U.S. Department of the Treasury has a long history of dealing with sanctions, dating as far back as the War of 1812 when the then Secretary of the Treasury administered sanctions against Great Britain for harassing American soldiers. OFAC, as we know it today, was formally created in 1950, when President Harry S. Truman declared a national emergency following China's entry into the Korean War and blocked all Chinese and North Korean assets subject to U.S. jurisdiction.

OFAC Sanctions Programs comprise country, regime and industry-based programs, including but not limited to, the following:

- Counter Terrorism Sanctions
- Counter Narcotics Trafficking Sanctions
- Non-Proliferation Sanctions
- Transnational Criminal Organisations Sanctions
- Cyber-Related Sanctions
- Rough Diamond Trade Controls
- Country- and Regime-Based Sanctions (e.g., Cuba, Iran, Iraq, Libya, North Korea, Russia, South Sudan, Syria)

An overview of each OFAC Sanctions Program is provided below. Further details of each of the OFAC Sanctions Programs can be found on the U.S. Department of the Treasury's website at www.treas.gov/ofac.

831. What are the key laws that grant OFAC the authority to administer and enforce economic and trade sanctions?

OFAC administers and enforces economic and trade sanctions under U.S. presidential national emergency powers and under authority granted by specific legislation. Key laws include, but are not limited to, the following:

- **Trading With the Enemy Act (TWEA)** (1917), amended a number of times, including but not limited to the International Emergency Economic Powers Act (IEEPA) Enhancement Act (2007),

prohibits trade with enemies or allies of enemies and authorises the president of the United States to declare a national emergency, regulate domestic and international commerce during time of war and national emergencies, and activate existing statutory provisions to address the threat to national security.

- **International Emergency Economic Powers Act (IEEPA)** (1977), amended by the IEEPA Enhancement Act (2007), authorises the president to regulate commerce after declaring a national emergency in response to an unusual and extraordinary threat to the United States which has a foreign source. It further authorises the president, after such a declaration, to block transactions and freeze assets to deal with the threat. In the event of an actual attack on the United States, the president can also confiscate property connected with a country, group or person who aided in the attack.
- **National Emergencies Act (NEA)** (1976), limits open-ended states of national emergency and formalises the power of Congress to provide checks and balances on the president's emergency powers. It also imposes "procedural formalities" on the president when invoking such powers (e.g., Proclamation 7463: Declaration of National Emergency by Reason of Certain Terrorist Attacks [September 14, 2001]; Proclamation 8693: Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions [July 24, 2011]).
- **Foreign Narcotics Kingpin Designation Act (Kingpin Act)** (1999), applies sanctions to designated persons involved in international narcotics trafficking as recommended by the Secretary of the Treasury, the Attorney General, the Secretary of State, the Secretary of Defense, the Director of the Central Intelligence Agency (CIA), the Department of Homeland Security and the Directorate of National Intelligence.
- **Antiterrorism and Effective Death Penalty Act (AEDPA)** (1996), passed shortly after the Oklahoma City bombing, prohibits international terrorist fundraising and assistance to terrorist states; applies sanctions to designated organisations engaged in terrorist activities; updates criminal procedures related to terrorism (e.g., increases penalties for terrorism crimes, clarifies and extends criminal jurisdiction for terrorism offenses transcending national boundaries); updates procedures related to terrorist and criminal aliens (e.g., denial of applications for visas, relief or asylum; arrests; detainments; deportations; and extraditions); updates restrictions related to nuclear, biological and chemical weapons (e.g., enhanced penalties, controls and reporting of explosive materials and biological agents); reforms habeas corpus procedures; outlines justice procedures and assistance for victims of terrorism; and provides assistance to law enforcement to combat terrorism (e.g., funding, training, research and development to support counterterrorism technologies).
- **International Security and Development Cooperation Act (ISDCA)** (1985) banned the import of goods and services from countries supporting terrorism.
- **Immigration and Nationality Act (INA)** (1952), as amended, is the basic legislative framework for immigration law; Acts 219 and 236A of the INA are related to terrorist aliens (e.g.,

designation of foreign terrorist organisations, mandatory detention of suspected terrorists, limitation on indefinite detention, habeas corpus).

- **Arms Export Control Act of 1976 (AECA), Export Administration Act of 1979 (EAA), Chemical and Biological Weapons Control and Warfare Elimination Act of 1991 (CBW), Iran-Iraq Arms Nonproliferation Act of 1992, Iran Nonproliferation Act of 2000 (INPA) (amended the Iran, North Korea, Syria Nonproliferation Act [INKSNA])** all relate to the non-proliferation of weapons and missiles and control items that have military applications.
- **Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA)** authorises the president to terminate unilateral agricultural or medical prohibitions to sanctioned countries (e.g., Cuba, Iran, Libya, Sudan) and implement licensing mechanisms for the provision of agricultural commodities, medicines and medical devices to sanctioned countries.
- **Clean Diamond Trade Act (CDTA)**, 19 U.S.C. 3901-3913 (2003), prohibits the import/export of diamonds to/from nonparticipants of the Kimberley Process Certification Scheme (KPCS) by requiring all diamonds imported into/exported out of the United States to have a Kimberley Process Certificate.
- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949) provides the framework for the U.S. participation in the United Nations and a mechanism to implement economic and other sanctions against a target country, organisation or individual as outlined in the United Nations Security Council Resolutions (UNSCRs).
- **Country- or Regime-Based Laws** (e.g., Cuban Democracy Act of 1992; Syria Accountability and Lebanese Sovereignty Act of 2003; Comprehensive Iran Sanctions, Accountability and Divestment Act [CISADA] in 2010; Iran Threat Reduction and Syria Human Rights Act in 2012).
- **The Criminal Code at 18 U.S.C. §1001** provides for criminal fines and imprisonment for knowingly making false statements or falsifying or concealing material facts when dealing with OFAC in connection with matters under its jurisdiction.
- **Executive Orders,** various official orders issued by the president including, but not limited to, the following:
    - **Executive Order 12978** – Blocking Assets and Prohibiting Transactions With Significant Narcotics Traffickers (1995);
    - **Executive Order 13224** – Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism (2001);
    - **Executive Order 13312** – Executive Order Implementing the Clean Diamond Trade Act (2003);
    - **Executive Order 13382** – Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters (2005);

- **Executive Order 13581** – Blocking Property of Transnational Criminal Organisations (2011);
- **Executive Order 13608** – Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria (2012);
- **Executive Order 13662** – Blocking Property of Additional Persons Contributing to the Situation in Ukraine (2014); and
- **Executive Order 13694** – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (2015).

For a more comprehensive list of statutes and executive orders, please visit OFAC's Resource Center at www.treasury.gov/resource-center/sanctions/Pages/statutes-links.aspx.

832. Are there any sanctions laws that have been enacted at the state level?

Yes. Multiple states have enacted laws requiring businesses to:

- Disclose activities related to sanctioned countries/regimes (e.g., Iran)
- Certify that companies do not conduct business activities prohibited by sanctions
- Divest from sanctioned countries/regimes

Penalties for noncompliance include debarment (e.g., ban from conducting business with public entities on a state by state level) and/or divestment by state investment funds. Information about state-level sanctions laws related to Iran can be found at http://www.unitedagainstnuclearіran.com.

In addition to state-level sanctions, some state regulators have also engaged in enforcement activity related to federal sanctions laws. For further guidance on enforcement actions, please refer to the Consequences of Noncompliance with OFAC Laws and Regulations section.

833. What key international treaties and conventions have influenced or shaped OFAC Sanctions Programs?

The United States has ratified the following treaties:

- **Treaty on the Non-proliferation of Nuclear Weapons of 1968 (NPT**), is a multilateral treaty with legally binding commitments that regulates nuclear arms and is focused on non-proliferation, disarmament and the peaceful use of nuclear energy.
- **United Nations International Convention for the Suppression of the Financing of Terrorism** (1999) (the Terrorist Financing Convention), contains obligations regarding freezing, seizure and confiscation as it relates to terrorism and terrorist financing.
- **United Nations Convention Against Transnational Organised Crime** (2000) (the Palermo Convention), contains obligations regarding freezing, seizure and confiscation as it relates to transnational organised crime.

- **Arms Trade Treaty (ATT)** (2013), a multilateral treaty that regulates international trade in conventional arms (e.g., tanks, armoured combat vehicles, artillery systems, military aircraft, small arms, light weapons, combat support equipment).

The United Nations (U.N.) Security Council has adopted multiple resolutions to maintain international peace and security since the 1940s. These resolutions are formal expressions of the U.N. Security Council and generally include a description of the issue(s) and action(s) to be taken to address the issue (e.g., freezing funds, travel bans, arms embargo). Key resolutions relating to the prevention and suppression of terrorism and terrorist financing include, but are not limited to, the following:

- **Al-Qaida Sanctions Lists** – Resolutions 1267 (1999), 1333 (2000), 1526 (2004), 1989 (2011) and its successor resolutions.
- **Taliban Sanctions Lists** – Resolutions 1267 (1999), 1526 (2004), 1988 (2011) and its successor resolutions.
- **Islamic State of Levant/Sham (ISIL/ISIS/Da'esh)-Sanctions Lists** – Resolutions 2249 (2015), 2253 (2015), and its successor resolutions.
- **Resolution 1373** (2001) was passed shortly after the September 11, 2001 attacks in New York City, Washington, D.C., and Pennsylvania. Resolution 1373 reaffirmed past resolutions related to combating terrorism (e.g., Resolution 1269 [1999], Resolution 1368 [2001]) and called on all members to implement fully relevant international conventions relating to terrorism. Resolution 1373 provided a mechanism for identifying targets for designation on a national or supranational level.
- **Resolutions related to the non-proliferation of weapons of mass destruction (WMDs)** – Resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), 1929 (2010) and its successor resolutions.

The United Nations Participation Act (UNPA) provided the United States with a framework to implement U.N.-related treaties and resolutions. A comprehensive list of United Nations Security Council Resolutions (UNSCRs) enacted by the United States can be found on OFAC's Resource Center at www.treasury.gov/resource-center/sanctions/Pages/UNSCR-links.aspx.

834. How do OFAC Sanctions Programs correspond to the Financial Action Task Force (FATF) Recommendations?

OFAC Sanctions Programs (e.g., Counter Terrorism Sanctions Program, Counter Narcotics Trafficking Sanctions Program, Non-Proliferation Sanctions Program) parallel the Financial Action Task Force (FATF) Recommendations as outlined below:

- **Recommendation 4 – Confiscation and Provisional Measures** – FATF recommends the implementation of measures to freeze or seize proceeds from criminal activity (e.g., predicate offenses outlined by FATF), laundered funds, funds used to finance terrorism or support a terrorist act or organisation, or property of corresponding value.

- **Recommendation 6 – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing** – FATF recommends compliance with various UNSCRs requiring the freezing of property of persons designated by relevant authorities as terrorists or terrorist organisations.
- **Recommendation 7 – Targeted Financial Sanctions Related to Proliferation** – FATF recommends compliance with various UNSCRs requiring the freezing of property of persons designated by relevant authorities as proliferators of weapons of mass destruction (WMDs).
- **Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation** – FATF recommends the implementation of international instruments to assist with foreign requests to identify, freeze and seize affected property.

For further guidance on international standards, please refer to the Financial Action Task Force section.

835. How do OFAC regulations fit into AML/CFT compliance?

Section 326, the Customer Identification Program (CIP) provision of the USA PATRIOT Act, requires covered financial institutions to consult government lists of suspected terrorists or terrorist organisations provided to the financial institution by any government agency when establishing accounts for new customers. Since OFAC Sanctions Listings include alleged narcotics traffickers, terrorists and proliferators of WMDs, institutions often consider the OFAC Compliance Program to be a subset of their overall AML/CFT Compliance Program.

836. Who is required to comply with OFAC sanctions?

OFAC sanctions apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches. Requirements of certain OFAC Sanctions Programs also apply to subsidiaries of U.S. companies and to foreign persons in possession of goods of U.S. origin.

All individuals and entities subject to compliance are commonly referred to as "U.S. persons."

Some OFAC sanctions also apply to non-U.S. companies and individuals, such as those authorising restrictions on any person who engages in substantial transactions involving the Islamic Revolutionary Guard Corps (IRGC) in Iran.

837. Should a foreign financial institution with no U.S. presence consider incorporating OFAC into a sanctions compliance program?

OFAC requirements apply to the property or property interest of an individual, entity or a country subject to sanctions, which is in the United States or in the possession or control of a U.S. person.

Many international payments are settled in U.S. dollars through a U.S. dollar clearing account held at a U.S. institution that is required to comply with OFAC sanctions. A foreign financial institution (FFI) faces credit risk and reputation damage if it sends or receives funds to or from an OFAC-sanctioned

individual, entity or country, since these funds likely will be blocked by the U.S. institution asked to clear the funds.

Additionally, if an FFI is complicit in violating or evading sanctions, directly or on behalf of its customers, the FFI can face direct sanctions as well (e.g., loss of correspondent banking or payable-through account, blocked assets under control by a U.S. financial institution). Moreover, some sanctions can apply to foreign subsidiaries of a U.S. person.

838. How does OFAC define the term "prohibited transactions"?

OFAC defines the term "prohibited transactions" as trades or financial transactions and other dealings in which "U.S. persons" may not engage unless previous authorisation was granted by OFAC, or other licensing authority (with jurisdiction), or was expressly exempted by statute.

839. Is there a dollar threshold applicable to prohibited transactions?

No. There is no defined minimum or maximum amount subject to OFAC regulations.

840. How does OFAC define the term "property"?

"Property" is defined by OFAC as "anything of value." Examples of property include, but are not limited to: money, checks, drafts, debts, obligations, notes, warehouse receipts, bills of sale, evidences of title, negotiable instruments, trade acceptance, contracts, and anything else real, personal or mixed, tangible or intangible, "or interest or interests therein, present, future, or contingent."

841. How does OFAC define the term "interest"?

"Interest" is broadly defined by OFAC as "any interest whatsoever, direct or indirect."

842. If a sanctioned entity or individual is a minority owner of property or interests, are these properties/interests subject to sanctions?

Possibly. In most instances, property and interests (e.g., entities) that are 50 percent or more owned in aggregate by designees, directly or indirectly, are subject to sanctions (e.g., require blocking or rejecting).

However, if two persons with minority-ownership (e.g., 25 percent each) in a "property" become designees under OFAC Sanctions Programs, the aggregate ownership (now 50 percent across both designees) will subject that property to OFAC sanctions.

Moreover, some OFAC sanctions programs subject property or interests "controlled" by designees, regardless of ownership.

843. Does OFAC require entities over which one or more blocked persons exercise control, even if the control party/parties own less than 50 percent to be blocked pursuant to OFAC's 50 percent rule?

Not under OFAC's 50 percent rule, which relates only to ownership and not to control. An entity that is controlled (but not owned 50 percent or more) by one or more blocked persons is not considered

automatically blocked pursuant to OFAC's 50 percent rule. OFAC may, however, separately designate the control party and add it to the OFAC Sanctions Listing (e.g., SDN List) pursuant to statute or executive order and some OFAC authorities impose restrictions on property or interests "controlled" by designees, regardless of ownership.

844. If an entity was previously majority-owned by a sanctioned person, are these properties/interests still subject to sanctions?

No. Entities that were previously majority-owned by a sanctioned person are not subject to the blocking provision. However, as a precaution, these formerly majority-owned entities should be subject to enhanced monitoring as ownership stakes change or in anticipation of the entity's direct designation as a sanctioned entity.

845. Can subsidiaries of a designated entity be subject to sanctions even if the subsidiary is not a designee?

Possibly. If the subsidiary is majority owned by a designated entity, the property and interests may be subject to OFAC sanctions.

846. Can property and interests of persons who are not designated by OFAC be subject to the blocking provision?

Yes. If the person has provided material assistance to a designee on the OFAC Specially Designated Nationals and Blocked Persons List (SDN List), their property and interests may be blocked, even if the person is not listed as a designee. Moreover, certain sanctions apply to countries, geographical areas or specific regimes, and U.S. persons are required to block property of such sanctioned parties, even if not named on the SDN List.

847. Can U.S. persons provide legal counsel to OFAC-designated persons?

According to OFAC's Guidance on the Provision of Certain Services Relating to the Requirements of U.S. Sanctions Law issued in January 2017, consistent with previous guidance, U.S. persons may provide services including, but not limited to, the following:

- Provision of information or guidance regarding the requirements of U.S. sanctions laws including statutes, regulations and Executive Orders
- Provision of opinions on the legality of specific transactions under U.S. sanctions laws regardless of whether it would be prohibited for a U.S. person to engage in those transactions

U.S. persons are permitted to solicit information from OFAC-designated persons and conduct research to make their determinations.

848. What parties, activities and transactions are subject to OFAC sanctions?

All activities, including all trade or financial transactions, regardless of the amount, and all relationships, whether direct or indirect (e.g., customer, noncustomer), are subject to OFAC sanctions. This includes, but is not limited to:

- **Account types:** deposits, loans, trusts, safety deposit boxes;
- **Transaction types:** wire transfers, Automated Clearing House (ACH) transfers, letters of credit, currency exchanges, deposited/cashed checks, purchases of monetary instruments, loan payments, security trades, retail purchases; and
- **Individuals/entities:** account holders, authorised signers, guarantors, collateral owners, beneficiaries, nominee shareholders, noncustomers, employees, vendors.

It is important to note that persons who are not listed on OFAC Sanctions Listings can also be subject to sanctions if they provided material assistance to a designated target or assisted the target to evade OFAC sanctions.

As a practical matter, however, institutions must decide, based on their assessment of OFAC compliance risk, which parties, activities and transactions will be screened against the OFAC Sanctions Listings, as well as how often, since 100 percent screening is not a viable option for most institutions. For further guidance on screening, please refer to the Screening Customers and Transactions and Interdiction Software sections.

849. Are e-commerce/internet transactions subject to OFAC sanctions?

Yes. All transactions, regardless of the amount or type, are subject to OFAC sanctions. An individual or an entity that transacts with a party subject to OFAC sanctions via an e-commerce or internet transaction is liable.

850. Are virtual currency transactions subject to OFAC sanctions?

The conversion of cash to virtual currency, and in fact any transactions involving virtual currency, are subject to compliance with OFAC regulations, which cover transfers involving essentially anything of value. For further guidance, please refer to the sections, Virtual Currency Systems and Participants and Money Services Businesses.

851. What types of parties, activities and transactions pose a heightened OFAC compliance risk to a U.S. financial institution?

Heightened OFAC compliance risk may be posed by the following:

- Foreign offices located in high-risk jurisdictions;
- Foreign correspondent banking relationships with FFIs located in high-risk jurisdictions;
- Customers engaged in international business (e.g., exporters/importers);
- International funds transfers;
- Trade finance products and services (e.g., letters of credit); and
- E-commerce transactions with entities/customers located in high-risk jurisdictions.

852. What is an OFAC/Sanctions risk assessment?

An OFAC/Sanctions risk assessment is a systematic method of qualifying and quantifying OFAC compliance risks to ensure an OFAC Sanctions Compliance Program mitigates potential risks identified. For additional guidance on OFAC/Sanctions risk assessments, please refer to the Risk Assessments section.

853. Does OFAC prescribe specific requirements for compliance programs?

Unlike AML/CFT laws and regulations, OFAC does not dictate specific components of compliance programs; however, OFAC has released industry-specific guidance (e.g., exporters/importers, securities, insurance, money services businesses [MSB]) which should be taken into consideration. Financial institution regulators do expect companies to develop compliance programs. An effective OFAC Sanctions Compliance Program should include the following:

- Blocking/rejecting transactions with designees on OFAC Sanctions Listings
- Reporting blocked or rejected transactions
- Designating an individual to be responsible for OFAC compliance
- Developing and implementing written OFAC policies and procedures
- Conducting an OFAC/sanctions risk assessment
- Conducting comprehensive and ongoing training
- Designing and maintaining effective monitoring, including timely updates to the OFAC filter
- Periodic, independent testing of the program's effectiveness (there is no single compliance program suitable for every institution)

Developing risk-based internal controls for OFAC compliance, including screenings and reviewing of customers and transactions, as appropriate, against lists of sanctioned entities, collectively referred to as "OFAC Sanctions Listings":

- OFAC Specially Designated Nationals and Blocked Persons List (SDN List)
- Non-SDN Palestinian Legislative Council List (NS-PLC List)
- Foreign Sanctions Evaders List (FSE List)
- Sectoral Sanctions Identifications List (SSI List)
- List of Foreign Financial Institutions Subject to Part 561 List (Part 561 List)
- Non-SDN Iranian Sanctions Act (NS-ISA) List
- List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List)

854. What lists beyond those administered by OFAC (e.g., SDN, the NS-PLC, FSE, SSI, Part 561, NS-ISA, 13599 Lists) can be incorporated into an OFAC Sanctions Compliance Program?

Section 311 of the USA PATRIOT Act provides the U.S. Department of the Treasury broad authority to impose one or more of five Special Measures against foreign jurisdictions, foreign financial institutions, classes of international transactions or types of accounts, if it determines that such jurisdictions, financial institutions, types of transactions or accounts are of primary money laundering concern. Designations under Section 311 can be incorporated into the existing screening process of an OFAC Sanctions Compliance Program.

Other U.S. government agencies, such as the U.S. Bureau of Industry and Security (BIS), the Department of Commerce, and the State Department, have independent prohibitions on transactions with certain individuals or entities beyond those included in OFAC Sanctions Listings.

Additionally, there are several sanctions lists maintained by other countries that can be considered for inclusion.

For further guidance, please refer to the Other U.S. and International Sanctions Programs section.

855. What are "white lists" and how can financial institutions incorporate them into an OFAC Sanctions Compliance Program?

"White lists" are lists of names that have been flagged as potential OFAC matches but subsequently cleared through investigation by the financial institution. White lists are used to improve the efficiency of sanctions screening by reducing the number of false positives by leveraging the results of past investigations.

856. How should a financial institution manage the use of a white list to ensure its ongoing usefulness and effectiveness?

Financial institutions should have documented procedures for managing white lists, which include, but are not limited to, the following:

- Criteria (e.g., number/frequency of false positives) that would justify adding a name to the white list.
- Screening of the white list against updates to the sanctions lists to ensure that white listed names are not subsequently added to a sanctions list.
- Periodic screening of the white list against the financial institution's customer/transaction base to determine whether it's necessary to retain a name on the white list.

857. What types of actions are required upon identifying a designated person or prohibited transaction or activity?

Each OFAC Sanctions Program outlines specific actions that must be taken upon identifying a designated person or prohibited transaction or activity. These actions include, but are not limited to, the following:

- Blocking property and interests of designees;
- Rejecting transactions of designees;
- Blocking property and interests of persons providing material assistance to designees or of persons assisting in the evasion of sanctions (or conspiracy to evade sanctions);
- Reporting of blocked and rejected transactions;
- Prohibiting the opening or maintenance of correspondent accounts and payable-through accounts; or
- Taking appropriate actions to not provide a prohibited service or transaction (in addition to blocking property and interests as required) (e.g., denial of visa, suspension of exports/imports, prohibiting donations of prohibited goods, prohibiting investments or divesting).

For further guidance, please refer to the sections: Blocking and Rejecting Transactions and OFAC Reporting Requirements.

858. How do the new obligations of the Customer Due Diligence Requirements for Financial Institutions final rule impact obligations under OFAC Sanctions Compliance Programs?

Previously, covered financial institutions were required to obtain beneficial ownership information in the following situations, as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Customer Due Diligence Requirements for Financial Institutions (Beneficial Owner Rule) issued in July 2016 by the Financial Crimes Enforcement Network (FinCEN) requires financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers. The Beneficial Owner Rule impacts the OFAC Sanctions Compliance Program of financial institutions, as certain beneficial owners would be subject to screening against required OFAC Sanctions Listings to the extent that financial institutions are not screening beneficial owners.

For further guidance on the Beneficial Owner Rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

859. Are there exemptions from the OFAC Sanctions Programs?

Yes. Many of the OFAC Sanctions Programs contain provisions that exempt exports and imports of information or informational materials (subject to restrictions), transactions ordinarily incident to travel (except for Cuba), and transactions for the conduct of official U.S. government business.

In addition, certain transactions involving exports of certain food, agricultural commodities, medicine and medical devices are eligible for specific licenses issued by OFAC or BIS, or, in some cases, a general license. For further guidance, please refer to the OFAC Licensing section.

860. Are existing contracts and licenses still valid after the issuance of subsequent OFAC sanctions?

Generally, existing contracts that cover prohibited activities or involve designated individuals or entities will no longer be legitimate, unless a valid license has been issued. Persons who have been issued licenses involving persons designated under OFAC Sanctions Programs should check with the issuing agency regarding the ongoing validity of their licenses.

For further guidance, please refer to the OFAC Licensing section.

861. What enforcement authority does OFAC have?

OFAC can impose penalties against any organisation or entity that conducts or facilitates transactions with those associated with individuals/entities on the OFAC Sanctions Listings. OFAC may also conduct civil investigations and/or may refer potential violations to prosecutors to conduct criminal investigations of potential violations.

862. Who is responsible for examining financial institutions for compliance with OFAC sanctions?

For regulated financial institutions, an institution's primary regulator is responsible for examining OFAC compliance. Other types of organisations may not be subject to regular OFAC examinations by a regulatory body, but are nonetheless at risk for penalties imposed on noncompliance.

863. Does OFAC offer any guidance on its expectations for specific industries?

OFAC has promulgated specific guidance for the following industries/businesses:

- Financial community (e.g., banks)
- Securities industry
- Money services businesses (MSBs)
- Exporters and importers
- Insurance industry
- Nongovernmental organisations (NGOs)/Nonprofits
- Credit reporting businesses
- Corporate registration businesses

864. What resources has OFAC provided to the public?

Among the resources provided by OFAC are the following:

- **OFAC Sanctions Listings** – OFAC publishes a list of designated individuals and companies owned or controlled by, or acting for or on behalf of, the governments of targeted countries that are subject to sanctions under its various programs. Key lists are included below. For further guidance, please refer to the OFAC Sanctions Listings section.
    - **Specially Designated Nationals and Blocked Persons List (SDN List)** – The SDN List identifies individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Their assets are blocked, and U.S. persons generally are prohibited from dealing with them.
    - **Non-SDN Palestinian Legislative Council List (NS-PLC List)** – The NS-PLC List is composed of members of the Palestinian Legislative Council who were elected on the party slate of Hamas or other designated foreign terrorists or terrorist organisations not named on the SDN List.
    - **Sectoral Sanctions Identifications List (SSI List) –** The SSI List includes designated persons operating in financial and energy sectors of the Russian economy subject to sanctions related to Ukraine.
    - **Foreign Sanctions Evaders List (FSE List) –** The FSE List includes persons engaged in conduct relating to the evasion of U.S. sanctions with respect to Iran, Syria, antiterrorism and non-proliferation of WMDs.
    - **List of Foreign Financial Institutions Subject to Part 561 (Part 561 List)** – The Part 561 List includes entities who have violated Iranian Financial Sanctions Regulations (IFSR).
- **OFAC Sanctions Programs –** OFAC publishes an overview of each of its sanctions programs. Designated individuals and entities are listed on various OFAC Sanctions Listings as described above. For further guidance, please refer to the OFAC Sanctions Programs section.
    - Counter Terrorism Sanctions (e.g., Specially Designated Global Terrorists [SDGT], Foreign Terrorist Organisations [FTO], Specially Designated Terrorists [SDT])
    - Counter Narcotics Trafficking Sanctions (e.g., Specially Designated Narcotics Traffickers [SDNT], Specially Designated Narcotics Traffickers - Kingpins [SDNTK])
    - Cyber-Related Sanctions Program (e.g., [CYBER])
    - Transnational Criminal Organisations Sanctions (TCO)
    - Non-Proliferation Sanctions (NPWMD)
    - Rough Diamond Trade Controls Sanctions
- **Country- and Regime-Based Sanctions Programs** – OFAC publishes current Country- and Regime-Based Programs, including, but not limited to, the Balkans (BALKANS), Cuba (CUBA), Iran ([IRAN], [IRGC], [IFSR], [IRAN-HR], [HRIT]), Iraq ([IRAQ], [IRAQ2]), North Korea (DPRK), Syria (SYRIA), and Ukraine/Russia ([UKRAINE-EO 13660], [UKRAINE-EO 13661], and

[UKRAINE-EO 13662]). For further guidance, please refer to the Country- and Regime-Based Sanctions Programs section.

- **OFAC Information for Industry Groups** – OFAC compiles guidance by certain industry groups (e.g., financial sector, money services businesses [MSBs], insurance industry, exporting and importing). These sections include items such as links to the relevant sections of the compiled FAQs, articles and industry brochures.
- **Frequently Asked Questions (FAQs)** – OFAC's own FAQ list, regarding frequently asked questions it has received and answers to those questions on topics such as the SDN List, licensing, technology from multiple industries (e.g., financial institutions, insurance, importers/exporters), and country sanctions programs.
- **OFAC Risk Matrix** – A matrix that assists institutions with rating (low, medium, high) areas of their own OFAC Sanctions Compliance Programs to ensure effective risk management. They have been produced for different sectors (e.g., financial institutions, charitable organisations, securities).
- **OFAC License Application Page** – OFAC's application for licensing and guidance on general, transactional and program-specific licensing.
- **OFAC Reporting Forms –** OFAC maintains current reports (e.g., Report of Blocked Transactions Form), license application forms, and requests to release blocked funds (e.g., Application for the Release of Blocked Funds).
- **OFAC Legal Library –** Documents that grant OFAC the authority to administer and enforce economic and trade sanctions (e.g., statutes, regulations, United Nations Security Council Resolutions [UNSCRs]) and provide an overview of each OFAC Sanctions Program (e.g., Non-Proliferation Sanctions, Country- and Regime-Based Sanctions).
- **OFAC Recent Actions** – OFAC maintains a list of current actions that it has made, such as updates to the SDN List or OFAC Sanctions Programs, and notifications of the release of certain reports.
- **Civil Penalties Actions and Enforcement Information** – An archive of the published civil penalties, enforcement actions and settlements taken against entities, dating back to 2003.
- **Economic Sanctions Enforcement Guidelines** – Enforcement guidance for persons subject to the requirements of U.S. sanctions statutes, executive orders and regulations.
- **Memorandum of Understanding (MOU) Between OFAC and the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA) and the Office of the Comptroller of the Currency (OCC)** – An MOU that explains the relationship between OFAC and the banking regulators.
- **Interpretive Rulings on OFAC Policy** – An archive of published rulings and interpretations to clarify OFAC policy.

- **Terrorist Assets Report (TAR)** – An annual report submitted to Congress concerning the nature and extent of assets held in the United States by terrorist-supporting countries and organisations.
- **OFAC Training and Events** – A list of OFAC events, symposiums and training.

All guidance is available on OFAC's website: www.ustreas.gov/offices/enforcement/ofac.

OFAC Sanctions Listings

865. What lists should U.S. institutions incorporate into their OFAC Sanctions Compliance Program?

An effective OFAC Sanctions Compliance Program should include screenings of customers and transactions, as appropriate, against the following lists collectively referred to as "OFAC Sanctions Listings":

- OFAC Specially Designated Nationals and Blocked Persons List (SDN List)
- Non-SDN Palestinian Legislative Council List (NS-PLC List)
- Foreign Sanctions Evaders List (FSE List)
- Sectoral Sanctions Identifications List (SSI List)
- List of Foreign Financial Institutions Subject to Part 561 (Part 561 List)
- Non-SDN Iranian Sanctions Act (NS-ISA) List
- List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List)

These OFAC Sanctions Listings include designees from the various OFAC Sanctions Programs. Many financial institutions incorporate certain other countries' sanctions lists as well. For ease of compliance, OFAC offers its non-SDN sanctions lists in a consolidated file titled "Consolidated Sanctions List."

U.S. offices of a foreign organisation may have additional obligations related to sanction requirements of their home jurisdictions. For further guidance, please refer to the sections: OFAC Sanctions Programs and Other U.S. and International Sanctions Programs.

866. How can institutions search for names on the OFAC Sanctions Listings?

Institutions can search for names on the SDN and Consolidated Sanctions Lists using OFAC's search tool, recently renamed "Sanctions List Search," which is available at https://sdnsearch.ofac.treas.gov. Guidance on technical details, such as the types of searches, algorithms and confidence levels (e.g., Minimum Name Score) of the Sanctions List Search is also provided by OFAC.

Most institutions use other technology solutions to facilitate searching. Interdiction software, also known as filtering or screening software, is a tool that facilitates the comparison of separate sets of data (e.g., a customer database, list of individuals/businesses linked to illicit activity) for possible hits. For further guidance, please refer to the AML/CFT Technology and Interdiction Software sections.

867. What does a positive "hit" mean?

A positive "hit" is defined as a confirmed true match to the OFAC Sanctions Listings.

868. How frequently are the OFAC Sanctions Listings updated?

Prior to September 11, 2001, updates to the OFAC Sanctions Listings (e.g., SDN List) were relatively sporadic. The infrequent additions lulled many institutions, particularly smaller ones, into thinking that compliance responsibilities were easily manageable and did not require automated tools. In the current environment, however, names are added and removed to the OFAC Sanctions Listings often and without prior notice. As soon as a name is added to the OFAC Sanctions Listings, OFAC expects compliance.

869. What is a reasonable time for compliance with updates to the OFAC Sanctions Listings?

OFAC can update Sanctions Listings at any time without prior notice and expects compliance as soon as a name is added to the OFAC Sanctions Listings. An institution must weigh its risk and determine the appropriate time frame for ensuring that updates are processed. Some institutions process updates the same day, while others, in accordance with their risk profile, may process updates less frequently than daily. Documentation of updates should be maintained by the responsible department.

870. How can an institution stay up-to-date on the changes to the OFAC Sanctions Listings?

OFAC offers real-time email notifications of any changes to a Sanctions Program or Sanctions Listing. Many vendors also provide automatic notifications and updates as part of their interdiction software package.

871. Can an individual/entity be designated under multiple OFAC Sanctions Programs?

Yes. An individual/entity can be designated under multiple OFAC Sanctions Programs.

872. Who has the authority to designate an individual or entity as a target for OFAC Sanctions Programs?

The authority to designate persons as a target for sanctions rests with the Secretary of the Treasury and the president. The Secretary of the Treasury will also consult with the U.S. Attorney General, the Director of the Central Intelligence Agency (CIA), the Director of the Federal Bureau of Investigation (FBI), the Administrator of the Drug Enforcement Administration (DEA), the Secretary of Defense, the Secretary of Homeland Security and the Secretary of State, as needed.

873. Are designees notified when added to OFAC Sanctions Listings?

No. OFAC does not notify designees when they are added to OFAC Sanctions Listings, primarily to prevent designees from hiding assets subject to blocking sanctions.

874. Can a designee request to be delisted?

Yes. A request for reconsideration can be sent to OFAC by the designee. The designation can also be challenged in court. Designations can also be revoked by the Secretary of State or by an act of Congress if the designation is no longer warranted.

875. When a designee is removed from the SDN List, how can a financial institution verify that the person has been officially removed?

Designees who have been removed from the SDN List receive an "SDN Removal Letter." Financial institutions may contact OFAC to confirm the authenticity of such letters by emailing ofac.reconsideration@treasury.gov.

876. Are designees with pending investigations included on OFAC Sanctions Listings?

Yes. Designees with pending investigations may be included on OFAC Sanctions Listings program tags, including, but not limited to the following:

- Blocked Pending Investigation, Patriot Act (BPI-PA)
- Blocked Pending Investigation, Foreign Narcotics Kingpin Sanctions Regulations, 31 CFR Part 598 (BPI-SDNTK)
- Blocked Pending Investigation, Cyber-Enabled Regulations, 31 CFR Part 578 (BPI-CYBER)

Specially Designated Nationals and Blocked Persons List

877. What is the Specially Designated Nationals and Blocked Persons List?

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, the governments of targeted countries. The Specially Designated Nationals and Blocked Persons List (SDN List) also identifies individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs that are not country-specific. Their assets are blocked and U.S. persons generally are prohibited from dealing with them.

The program tags for individuals/entities on the SDN List include, but are not limited to, the following:

- Specially Designated Terrorists (SDT)
- Specially Designated Global Terrorists (SDGT)
- Foreign Terrorist Organisations (FTO)
- Specially Designated Narcotics Traffickers (SDNT)
- Specially Designated Narcotics Traffickers – Kingpins (SDNTK)
- Non-Proliferation of Weapons of Mass Destruction (NPWMD)
- Transnational Criminal Organisation (TCO)
- Cyber-Related Sanctions (CYBER)

- Iran Sanctions Act, Executive Order 13574 (ISA)
- Iranian Transactions and Sanctions Regulations 31 CFR Part 560 (IRAN)

Although this SDN List allows U.S. persons to know they are prohibited from dealing with persons or entities on the list, it is not comprehensive, as it does not include, for example, the names of all individuals in Cuba (who are subject to blocking, except under limited exceptions).

878. What action must institutions take if a positive "hit" is identified on the SDN List?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

879. How can institutions ensure they are using the most current SDN List to screen customers and transactions?

Institutions can register with OFAC to receive a notification, via email, whenever the SDN List has been updated. Additionally, many technology service providers are providing automated notifications to their users when updated lists have been incorporated into the interdiction software. When notifications are received, institutions should test their interdiction software to ensure the updated SDN List is being used to screen customers and transactions.

880. What information is provided on the SDN List?

The SDN List provides the following information, if known:

- Name(s) (including variations in spelling)
- Alias(es)
- Address(es)
- Website address(es)
- Email address(es)
- Nationality(ies)
- Citizenship(s)
- Place of birth(s) (POB)
- Date of birth(s) (DOB)
- Information provided on identification(s)/documentation (e.g., cedula number, passport number, expiration date, date of issuance, country of issuance, business registration number)
- Title(s)/position(s) (e.g., former Minister of Higher Education and Research, Republican Guard Secretary)
- Customer type (i.e., individual; if not stated, assumed as business/entity type)

- Reason(s) for inclusion on SDN List (e.g., SDNT, SDGT, SDNTK, Liberia, Iraq)

This information can be used to assist in investigating potential matches with the SDN and other list-based sanctions programs.

881. What are "weak aliases"?

OFAC defines "weak aliases" or "weak AKAs" as broad or generic aliases for designated individuals and entities on the SDN List (e.g., nicknames by which targets refer to themselves or are referred to by others). Weak aliases are included on the SDN List to assist with confirming a potential match. Due to their potential to generate a high volume of false positives, OFAC suggests institutions utilise a risk-based approach to determine whether weak aliases should be included in the OFAC screening process.

882. Are all designees on the SDN List foreign?

No. Designees on the SDN List consist of many nationalities, including U.S. individuals and entities, although most are foreign.

883. What is the process for adding a name to the SDN List?

The process of adding a name to the SDN List involves evidence being vetted through several agencies prior to OFAC's final designation on the SDN List. This information is labelled classified. In some cases, the designations are made through executive orders directly from the U.S. President.

884. If a designee dies, is that individual removed from the applicable OFAC Sanctions Listing?

No. Even though the individual is deceased, his or her assets remain blocked until OFAC sees fit to unblock them. For example, if a designee dies, the individual's assets should not be released to beneficiaries until further guidance is received from OFAC.

Non-Specially Designated Nationals Palestinian Legislative Council List

885. What is the Non-SDN Palestinian Legislative Council List?

Pursuant to the Global Terrorism Sanctions Regulations (31 C.F.R. Part 594), the Terrorism Sanctions Regulations (31 C.F.R. Part 595) and the Foreign Terrorist Organisations Sanctions (31 C.F.R. Part 597), OFAC published the Non-Specially Designated Nationals Palestinian Legislative Council List (NS-PLC List) in April 2006. The NS-PLC List is composed of members of the Palestinian Legislative Council who were elected on the party slate of Hamas or other designated foreign terrorists or terrorist organisations not named on the SDN List.

The program tag for individuals/entities on the NS-PLC List is [NS-PLC].

886. Is the NS-PLC List part of the SDN List?

No. The NS-PLC List is separate from the SDN List, and the individuals included on the NS-PLC List are not necessarily listed on the SDN List.

887. Who should screen customers/transactions against the NS-PLC List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

888. What action must institutions take if a positive "hit" is identified for the NS-PLC List?

The U.S. Department of the Treasury has authorised U.S. financial institutions to reject transactions with designees on the NS-PLC List. A Report of Rejected Transactions must be filed with OFAC within 10 business days. Prohibition of other goods, services and technology to the NS-PLC designee beyond the rejected transaction may apply as well.

In the case where an NS-PLC designee is also on the SDN List, transactions/property may need to be blocked.

For additional guidance on reporting rejected or blocked transactions to OFAC, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Foreign Sanctions Evaders List

889. What is the Foreign Sanctions Evaders (FSE) List?

Established in 2012 by Executive Order 13608 – Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders with Respect to Iran and Syria, the Foreign Sanctions Evaders List (FSE List) includes persons engaged in conduct relating to the evasion of U.S. sanctions with respect to Iran, Syria, anti-terrorism and non-proliferation of weapons of mass destruction (WMDs). Designees include persons who have violated, attempted to violate, conspired to violate, or caused a violation of OFAC Sanctions Programs related to Iran and Syria.

The program tags for individuals/entities on the FSE List are as follows:

- Foreign Sanctions Evaders – Syria [FSE-SY]
- Foreign Sanctions Evaders – Iran [FSE-IR]
- Foreign Sanctions Evaders – Non-Proliferation of Weapons of Mass Destruction [FSE-WMD]
- Foreign Sanctions Evaders – Anti-Terrorism [FSE-SDGT]

890. Is the FSE List part of the SDN List?

No. The FSE List is separate from the SDN List, and the individuals included on the FSE List are not necessarily listed on the SDN List.

Identification on the FSE List does not block any assets. However, a U.S. person may not provide or procure goods or services, including financial services, or technology to or from a listed person without authorisation from OFAC, unless the transaction is otherwise exempt (e.g., certain travel-related transactions).

891. Who should screen customers/transactions against the FSE List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

892. What action must institutions take if a positive "hit" is identified for the FSE List?

The U.S. Department of the Treasury has authorised U.S. financial institutions to reject transactions with designees on the FSE List. A Report of Rejected Transactions must be filed with OFAC within 10 business days. Prohibition of other goods, services and technology to the FSE designee beyond the rejected transaction may apply as well.

In the case where an FSE designee is also on the SDN List, transactions/property may need to be blocked.

For additional guidance on reporting rejected or blocked transactions to OFAC, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Sectoral Sanctions Identifications List

893. What is the Sectoral Sanctions Identifications (SSI) List?

Established in 2014 by Executive Order 13662 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine, the Sectoral Sanctions Identifications List (SSI List) includes designated persons operating in financial, defence, and energy sectors of the Russian economy. U.S. persons are prohibited from transacting with or providing financing for, or otherwise dealing in the following for entities listed under four Directives:

- Debt with a maturity of longer than 30 days (for SSI List financial and defence sector companies (Directives 1 and 3);
- Debt with a maturity of longer than 90 days (for SSI List energy sector companies) (Directive 2);
- Equity with or on behalf of financial sector companies on or after July 16, 2014 (Directive 1); and
- Engaging in certain transactions in support of exploration or production for deepwater, Arctic offshore, or shale projects that have the potential to produce oil in the Russian Federation, or in the maritime area claimed by the Russian Federation and extending from its territory (Directive 4).

The prohibitions also extend to entities owned 50 percent or more by SSI designees. However, if two persons with minority-ownership (e.g., 25 percent each) in a third "property" become SSI designees, the aggregate ownership (now 50 percent across both designees) will subject that property to OFAC sanctions.

The program tag for individuals/entities on the SSI List is [UKRAINE-EO13662]. The program is referenced as the "Ukraine-related sanctions."

894. How are "debt" and "equity" instruments defined as they relate to the SSI Sanctions Program?

OFAC provided the following examples of debt and equity instruments:

- Debt with a maturity of longer than 90 days, including bonds, loans, extensions of credit, loan guarantees, letters of credit, drafts, bankers acceptances, discount notes or bills or commercial paper
- Equity includes stocks, share issuances, depositary receipts or any other evidence of title or ownership

The SSI Sanctions Program only applies to new debt and equity created on or after July 16, 2014.

895. Is the SSI List part of the SDN List?

No. The SSI List is separate from the SDN List, and the individuals included on the SSI List are not necessarily listed on the SDN List.

896. Are correspondent accounts prohibited for SSI designees?

The SSI List is specific to the listed companies and the types of transactions (debt with a maturity longer than 30 days or 90 days, new equity, and certain energy projects, depending on which Directive and entity is listed). All other transactions involving the listed companies, including maintaining correspondent accounts or other financial relationships, are permitted.

897. Who should screen customers/transactions against the SSI List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

898. What action must institutions take if a positive "hit" is identified for the SSI List?

Financial institutions should review their service offerings to the SSI designee for prohibited offerings and discontinue the service if confirmed.

The U.S. Department of the Treasury has authorised U.S. financial institutions to reject transactions related to these prohibited products with designees on the SSI List. A Report of Rejected Transactions must be filed with OFAC within 10 business days.

In the case where an SSI designee is also on the SDN List, transactions may need to be blocked.

For additional guidance on reporting rejected or blocked transactions to OFAC, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

899. What challenges have financial institutions experienced with the SSI Program?

Financial institutions have struggled with how to apply the SSI prohibitions to their product offerings (e.g., revolving credit facility, long-term loan arrangements).

OFAC has continued to provide guidance on the implementation of the SSI Sanctions Program on their website under Frequently Asked Questions on Sanctions. Please visit http://www.treasury.gov/resource-center for further guidance.

Due to the dynamic nature of the situation in eastern Ukraine and Russia, OFAC Sanctions Programs are continuously evolving (e.g., may expand to include other products, services or prohibited activities). For the latest guidance on the SSI Sanctions Program, please refer to OFAC's website: http://www.treasury.gov/resource-center.

List of Foreign Financial Institutions Subject to Part 561

900. What is the List of Foreign Financial Institutions Subject to Part 561 (Part 561 List)?

The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List) includes entities which have violated Iranian Financial Sanctions Regulations (IFSR) pursuant to the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) (2010).

For further guidance, please refer to the Iranian and Syrian Sanctions Overview section.

901. Is the Part 561 List part of the SDN List?

No. The Part 561 List is separate from the SDN List, and the entities included on the Part 561 list are not necessarily listed on the SDN List.

902. Who should screen against the Part 561 List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

903. What action must institutions take if a positive "hit" is identified for the Part 561 List?

U.S. financial institutions are prohibited from opening or maintaining a correspondent or payable-through account for any foreign financial institution on the Part 561 List.

904. How many designations are currently on the Part 561 List?

Since the removal of the Elaf Islamic Bank in Iraq in 2013, the Part 561 List includes one entity: Bank of Kunlun, also known as Karamy City Commercial Bank and Karamy Urban Credit Cooperatives.

Non-SDN Iranian Sanctions Act (NS-ISA) List

905. What is the Non-SDN Iranian Sanctions Act (NS-ISA) List)?

The Non-SDN Iranian Sanctions (NS-ISA) List implements the non-blocking provisions in Section 6 of the Iran Sanctions Act of 1996, the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA), as amended and the Iran Threat Reduction and Syria Human Rights Act of 2012

(ITRSHRA). Pursuant to the Joint Comprehensive Plan of Action (JCPOA) of 2015 and 2016, these sanctions have been suspended and all designees removed from the NS-ISA List.

906. Is the NS-ISA List part of the SDN List?

No. When active, the NS-ISA List is separate from the SDN List, and the entities included on the NS-ISA List are not necessarily listed on the SDN List. Persons subject to blocking/rejecting sanctions pursuant to the Iran Sanctions Act of 1996 are included on the SDN List with the program tag [ISA].

907. Who should screen against the NS-ISA List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

The 13599 List

908. What is the List of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List)?

The list of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 (the 13599 List) includes persons that meet the definition of "Government of Iran" or "Iranian financial institution" as set forth in Part 560 of the Iranian Transactions and Sanctions regulations that are not blocked but are subject to other restrictions limiting transactions/trade.

For further guidance on Iranian sanctions, please refer to Country- and Regime-Based Sanctions Programs section.

909. Is the 13599 List part of the SDN List?

No. The 13599 List is separate from the SDN List, and the entities included on the 13599 List are not necessarily listed on the SDN List. Persons subject to blocking/rejecting sanctions pursuant to Executive Order 13599 are included on the Specially Designated Nationals and Blocked List (SDN List) with the program tag [IRAN].

910. Who should screen against the 13599 List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

911. What action must institutions take if a positive "hit" is identified for the 13599 List?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For

guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

OFAC Sanctions Programs

Counter Terrorism Sanctions Program

912. What is OFAC's Counter Terrorism Sanctions Program?

OFAC's Counter Terrorism Sanctions Program blocks the property and property interests of individuals, entities and regimes involved in terrorism-related activities, including countries that have been designated as state sponsors of terrorism.

The Counter Terrorism Sanctions Program was created pursuant to the following:

- **National Emergencies Act** (NEA) (1976)
- **International Emergency Economic Powers Act** (IEEPA) (1977)
- **Antiterrorism and Effective Death Penalty Act of 1996** (AEDPA) (1996)
- **United Nations Participation Act** (UNPA) (1945; amended by the United Nations Participation Act, 1949)
- **Hizballah International Financing Prevention Act of 2015** (HIFPA)
- **Executive Order 12947 – Prohibiting Transactions With Terrorists Who Threaten to Disrupt the Middle East Peace Process** (1995)
- **Executive Order 13099 – Prohibiting Transactions With Terrorists Who Threaten to Disrupt the Middle East Peace Process** (1998)
- **Executive Order 13224 – Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism** (2001)
- **Executive Order 13268 – Termination of Emergency With Respect to the Taliban and Executive Order 13224 of September 23, 2001** (2002)
- **Executive Order 13372 – Clarification of Certain Executive Orders Blocking Property and Prohibiting Certain Transactions** (2005)

Counter Terrorism Sanctions are implemented under the following regulations:

- **31 C.F.R. Part 594 – Global Terrorism Sanctions Regulations**
- **31 C.F.R. Part 595 – Terrorism Sanctions Regulations**
- **31 C.F.R. Part 596 – Terrorism List Governments Sanctions Regulations**
- **31 C.F.R. Part 597 – Foreign Terrorist Organisations Sanctions Regulations**
- **31 C.F.R. Part 566 – Hizballah Financial Sanctions Regulations**

913. Are designees under the Counter Terrorism Sanctions Program included on the SDN List?

Yes. The program tags for designees under the Counter Terrorism Sanctions Program on the SDN List are as follows:

- Specially Designated Terrorists (SDT)
- Specially Designated Global Terrorists (SDGT)
- Foreign Terrorist Organisations (FTO)

914. How is "terrorism" defined under the Counter Terrorism Sanctions Program?

The term "terrorism" is defined as an "activity that:

- Involves a violent act or an act dangerous to human life, property or infrastructure; and
- Appears to be intended:
  - To intimidate or coerce a civilian population;
  - To influence the policy of a government by intimidation or coercion; or
  - To affect the conduct of a government by mass destruction, assassination, kidnapping or hostage-taking."

915. What are "foreign terrorist organisations"?

"Foreign terrorist organisations" (FTOs) are designated by the Secretary of State as being engaged in terrorist activities. Currently, there are nearly 60 organisations designated as FTOs, including, but not limited to, the following:

- Al-Qaeda (AQ) (1999)
- Al-Qaeda in the Islamic Maghreb (AQIM) (2002)
- Al-Qaeda in the Arabian Peninsula (AQAP) (2010)
- Boko Haram (2013)
- Hamas (1997)
- Hizballah (1997)
- Mujahidin Shura Council in the Environs of Jerusalem (MSC) (2014)
- Real Irish Republican Party (RIRA) (2001)
- Revolutionary Armed Forces of Colombia (FARC) (1997)
- Tehrik-e Taliban Pakistan (TTP) (2010)
- Hilal Ahmar Society Indonesia (Indonesia) (2014)
- Al-Furqan Foundation Welfare Trust (Al-Furqan) (2015)

- Al-Rahmah Welfare Organisation (RWO)(Pakistan) (2016)

916. What are "state sponsors of terrorism"?

"State sponsors of terrorism" are countries that have repeatedly provided support for acts of international terrorism as designated by the Secretary of State. Currently, there are three countries that have been designated as state sponsors of terrorism:

- Iran (1984)
- Sudan (1993)
- Syria (1979)

Rescinded designations included:

- Cuba (Designated in 1982; removed in 2015)
- Iraq (Designated in 1979; removed in 2004)
- Libya (Designated in 1979; removed in 2006)
- North Korea (Designated in 1988; removed in 2008; possible re-designation in 2017)
- South Yemen (Designated in 1979; removed in 1990)

917. What are some common methods of terrorist financing?

According to the National Terrorist Financing Risk Assessment (2015), major funding sources of terrorist organisations such as ISIL, al-Qaeda and Boko Haram include, but are not limited to, the following:

- Kidnapping for ransom (KFR)
- Private donations, solicited directly or indirectly through charitable organisations;
- Extortion of the population and resources in controlled territory;
- Revenue from legitimate businesses located in controlled territory;
- Illicit revenue from criminal activities (e.g., smuggling, narcotics trafficking); and
- State sponsorship.

918. What types of entities are vulnerable to terrorist financing?

Historically, charities have been susceptible to abuse by terrorists. The following characteristics heighten the ML/TF risks of charitable organisations:

- Cash-intensive
- Lack of transparency in complex transactions
- Increased frequency of international transactions
- Global presence facilitates quick transfer of funds internationally

- Varied source of funds (e.g., funds received from donors around the world)
- Subject to little or no oversight

Terrorist organisations have been known to divert donations and humanitarian aid (e.g., food, agricultural commodities, medicine, medical devices) to use or to trade to support their activities. For further guidance on the ML/TF risks of charitable organisations, please refer to the Charitable Organisations and Nongovernmental Organisations section.

Additionally, as sanctions increasingly restrict access to the traditional financial systems, foreign exchange houses and trading companies acting as money transmitters are increasingly being used to circumvent sanctions. For further guidance, please refer to the Money Services Businesses section.

919. What is an example of a terrorist financing-related court case?

The U.S. Anti-Terrorism Act of 1992 permits U.S. citizens to sue for damages arising from international terrorism. In September 2014, Arab Bank PLC, a Jordanian financial institution, was the first bank to be found liable in a U.S. civil proceeding of providing banking services to terrorists and faced a potential jury award in the hundreds of billions of dollars in treble damages. The litigation was brought by victims and family members of victims in over 20 terror attacks in Israel, Gaza and the West Bank from 2001 – 2004. The plaintiffs alleged that Arab Bank PLC provided services to Hamas, specifically to charities that were not identified as terrorist organisations, but which made payments, originating in the United States, to families of alleged terrorists who were injured or killed in terrorist attacks, such as suicide bombings. While Arab Bank PLC was held liable because the banking services provided were deemed a substantial contributor to the plaintiffs' injuries, an undisclosed settlement was ultimately reached between Arab Bank PLC and hundreds of plaintiffs for this and other terrorist-financing related cases.

Many more cases similar to this against other foreign banking organisations are now pending in U.S. federal court. For more cases and other trends in terrorist financing, please refer to the United States Attorney's Bulletin "Terrorist Financing" Volume 62, Number 5 (2014).

Counter Narcotics Trafficking Sanctions Program

920. What is OFAC's Counter Narcotics Trafficking Sanctions Program?

Established by the Kingpin Act (1999), IEEPA, NEA and Executive Order 12978 – Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers (1995), OFAC's Counter Narcotics Trafficking Sanctions Program blocks the property and property interests of specially designated individuals and entities involved in significant narcotics trafficking in Colombia or other significant foreign narcotics traffickers, or that materially assist in, or provide financial or technological support for or goods or services in support of, the narcotics trafficking activities.

Counter Narcotics Trafficking Sanctions are implemented under the following regulations:

- **31 C.F.R. Part 536 – Narcotics Trafficking Sanctions Regulations**
- **31 C.F.R. Part 598 – Foreign Narcotics Kingpin Sanctions Regulations**

921. Are designees under the Counter Narcotics Trafficking Sanctions Program included on the SDN List?

Yes. The program tags for designees under the Counter Narcotics Trafficking Sanctions Program on the SDN List are as follows:

- Specially Designated Narcotics Traffickers (SDNT)
- Specially Designated Narcotics Traffickers – Kingpins (SDNTK)
- Blocked Pending Investigation, Foreign Narcotics Kingpin (BPI-SDNTK)

922. How is the term "narcotics trafficking" defined under the Counter Narcotics Trafficking Sanctions Program?

The term "narcotics trafficking" is defined as "any activity undertaken illicitly to cultivate, produce, manufacture, distribute, sell, finance or transport, or otherwise assist, abet, conspire, or collude with others in illicit activities relating to narcotic drugs, including, but not limited to, cocaine."

Under Section 802 of the Controlled Substances Act (CSA), the term "narcotic drug" includes controlled substances, such as opium, opiates, poppy straw, ecgonine and its derivatives.

923. Is the Counter Narcotics Trafficking Sanctions Program limited to traffickers from Colombia?

No. While Executive Order 12978 focused on cocaine traffickers based out of Colombia, the Kingpin Act expanded the program to include international traffickers from any country other than the United States.

924. Are marijuana traffickers subject to the Counter Narcotics Trafficking Sanctions Program?

Although marijuana is not a narcotic, it is a controlled substance subject to the Foreign Narcotics Kingpin Sanctions Regulations. Significant marijuana traffickers may be designated as SDNTKs under the Counter Narcotics Trafficking Sanctions Program.

For further guidance on businesses engaged in marijuana-related activities, please refer to the Marijuana-Related Businesses section.

Transnational Criminal Organisations Sanctions Program

925. What is OFAC's Transnational Criminal Organisations Sanctions Program?

Established by IEEPA, NEA and Executive Order 13581 – Blocking Property of Transnational Criminal Organisations (2011), OFAC's Transnational Criminal Organisations (TCO) Sanctions Program blocks the property and property interests of individuals and entities determined to be significant transnational criminal organisations or to have provided material support for, or to be owned or controlled by, or to have acted on behalf of such organisations. The Executive Order states that the activities of the listed transnational criminal organisations threaten the stability of international

political and economic systems and constitute an unusual and extraordinary threat to the national security, foreign policy and economic interests of the United States.

TCO Sanctions are implemented under 31 C.F.R. Part 590 – Transnational Criminal Organisations Sanctions Regulations.

926. Are designees under the TCO Sanctions Program included on the SDN List?

Yes. The program tag for designees under the Transnational Criminal Organisations Sanctions program on the SDN List is [TCO]. Examples of TCOs include, but are not limited to, the following:

- The Brother's Circle (also known as Family of Eleven, The Twenty)
- Camorra
- Mara Salvatrucha (MS-13)
- Yakuza (also known as Boryokudan, Gokudo)
- Los Zetas

927. How is the term "significant transnational criminal organisation" defined under the TCO Sanctions program?

The TCO Sanctions Program defines "significant transnational criminal organisations" as a group of persons that "engages in an ongoing pattern of serious criminal activity involving the jurisdictions of at least two foreign states; and threatens the national security, foreign policy or economy of the United States."

Non-Proliferation Sanctions Program

928. What is OFAC's Non-Proliferation Sanctions Program?

The Non-Proliferation Sanctions Program blocks the property and property interests of individuals and entities involved in proliferation-related activities and their support networks; bans foreign persons involved in proliferation-related activities from entering the United States; bans certain imports into the United States related to weapons of mass destruction (WMDs); restricts the use of materials extracted from Russian nuclear weapons to use in commercial nuclear reactors; and specifically prohibits U.S. persons and others from engaging in any transaction or dealing with designated parties.

The Non-Proliferation Sanctions Program was created pursuant to the following:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 12938 – Proliferation of Weapons of Mass Destruction** (1994)
- **Executive Order 13094 – Proliferation of Weapons of Mass Destruction** (1998)
- **Executive Order 13382 – Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters** (2005)

- **Executive Order 13608 – Prohibiting Transactions with and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria** (2012)
- **Executive Order 13617 – Blocking Property of the Government of the Russian Federation Relating to the Disposition of Highly Enriched Uranium Extracted From Nuclear Weapons** (2012)
- **Executive Order 13159 – Blocking Property of the Government of the Russian Federation Relating to the Disposition of Highly Enriched Uranium Extracted From Nuclear Weapons** (2012)

Non-Proliferation Sanctions are implemented under the following regulations:

- **31 C.F.R. Part 539 – Weapons of Mass Destruction Trade Control Regulations**
- **31 C.F.R. Part 540 – Highly Enriched Uranium (HEU) Agreement Assets Control Regulations**
- **31 C.F.R. Part 544 – Weapons of Mass Destruction Proliferators Sanctions Regulations**

929. Are designees under the Non-Proliferation Sanctions Program included on the SDN List?

Yes. The program tag for designees under the Non-Proliferation Sanctions Program on the SDN List is [NPWMD].

930. How is the term "weapon of mass destruction" defined under the Non-Proliferation Sanctions program?

Under Title 18 U.S. Code 2332a, a "weapon of mass destruction" (WMD) is defined as:

- Any destructive device (e.g., explosive, incendiary or poison gas bomb, grenade, rocket, missile, mine);
- Any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination or impact of toxic or poisonous chemicals or their precursors;
- Any weapon involving a biological agent, toxin or vector (e.g., living organism or molecule capable of carrying a biological agent or toxin to a host); or
- Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life.

Nuclear, biological, chemical or radiological WMDs and their delivery systems (e.g., any apparatus, equipment, device, or means of delivery specifically designed to deliver or disseminate a biological agent, toxin or vector) are subject to sanctions by OFAC's Non-Proliferation Sanctions Program.

931. How is the term "highly enriched uranium" defined under the Non-Proliferation Sanctions Program?

"Highly enriched uranium" (HEU) is defined as "uranium enriched to 20 percent or greater in the U235 isotope."

932. Is the Non-Proliferation Sanctions Program limited to nuclear weapons?

No. Arms traffickers, distinct from arms traders (e.g., persons engaged in legitimate trade in conventional arms governed by multilateral treaties), may be subject to the Non-Proliferation Sanctions Program.

Conventional arms include tanks, armoured combat vehicles, artillery systems, military aircraft, small arms, light weapons, and combat support equipment.

Multiple U.S. government agencies administer programs to monitor trade in arms and nuclear materials, including, but not limited to, the following:

- **The Commerce Control List (CCL)**, administered by the Commerce Department pursuant to the Export Administration Act of 1979 (EAA) (as amended), is used to regulate the export and re-export of items that have commercial uses but also have possible military applications (dual-use items). Examples of items on the CCL include, but are not limited to, the following:
  - Nuclear materials, chemicals, microorganisms and toxins
  - Computers
  - Telecommunications
  - Information security
  - Navigation and avionics
  - Aerospace and propulsion
- **The U.S. Munitions List (USML)**, administered by the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs within the State Department pursuant to the Arms Export Control Act of 1976 (AECA) and the International Traffic in Arms Regulations (ITAR), is used to control the export of defence articles, services and related technologies. Examples of items on the USML list include, but are not limited to, the following:
  - Firearms, such as close assault weapons, combat shotguns, guns over calibre 0.50 and flamethrowers
  - Launch vehicles, guided missiles, ballistic missiles, rockets, torpedoes, bombs and mines
  - Explosives, propellants and incendiary agents
  - Armored combat ground vehicles, special naval equipment, fighter bombers, attack helicopters, unmanned aerial vehicles (UAV)
  - Military training equipment

  - Personal protective equipment, such as body armour, helmets and select face paints
  - Military electronics, such as radios and radar systems

- **The AECA Debarments** list, also administered by the Directorate of Defense Trade Controls within the State Department pursuant to AECA and ITAR, includes persons who have been convicted in court for violations (or conspiracy to violate) the AECA (statutory debarments) or have been debarred during an administrative hearing for violating (or conspiring to violate) the AECA (administrative debarment). The Energy Department, through the National Nuclear Security Administration (NNSA), is responsible for the security of the U.S. nuclear weapons, nuclear proliferation and naval reactor programs. This includes controlling nuclear technology and technical data for nuclear power.

Cyber-Related Sanctions Program

933. What is OFAC's Cyber-Related Sanctions program?

Established by Executive Order 13694 – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities and Executive Order 13757 – Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, the Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Harmed, or otherwise significantly compromised the provision of services by a computer or network of computers that supports one or more entities in a critical infrastructure sector;
- Caused a significant disruption to the availability of a computer or network of computers;
- Caused a significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain;
- Engaged in the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in or materially contribute to a significant threat to the national security, foreign policy or economy of the United States;
- Tampered with, altered or caused a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions;
- Materially assisted, sponsored or provided financial, material or technological support for, or goods or services to or in support of the aforementioned acts; or

- Owned or controlled property or interests, acted or purported to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Cyber-Related Sanctions Program.

The Cyber-Related Sanctions Program is implemented under 31 CFR 578 – Cyber-Related Sanctions Regulations. OFAC intends to publish more comprehensive regulations to provide additional guidance (e.g., key definitions, licensing policy).

934. Are designees under the Cyber-Related Sanctions Program included on the SDN List?

Yes. Designees under the Cyber-Related Sanctions Program are included on the SDN List with the program tag [CYBER].

935. How did allegations of Russian involvement in the U.S. presidential election in 2016 influence the Cyber-Related Sanctions Program?

E.O. 13694 was issued on April 2015 and was further expanded under the Obama administration with E.O. 13757 (December 2016) as a direct result of reported allegations of Russian involvement in the U.S. presidential elections of 2016. Several Russian intelligence agencies and officials were placed on the SDN List as a result of cyber-espionage conducted during the presidential election.

In February 2017, a general license was issued authorising certain transactions that are otherwise prohibited pursuant to E.O. 13757 with the Federal Security Service of the Russian Federation (FSB), the successor security agency to the Komitet gosudarstvennoy bezopasnosti (KGB).

For further guidance on sanctions against Russia, please refer to the Russian and Ukraine-Related Sanctions Program section.

936. How is "significant malicious cyber-enabled activity" defined by OFAC?

"Significant malicious cyber-enabled activity" is defined by OFAC as "any act that is primarily accomplished through or facilitated by computers or other electronic devices" intended to cause harm which can include, but are not limited to, the following activities:

- Harms or otherwise significantly compromises the provision of services by a computer or network of computers that supports one or more entities in a critical infrastructure sector;
- Significantly compromises the provision of services by one or more entities in a critical infrastructure sector;
- Causes a significant disruption to the availability of a computer or network of computers; or
- Causes a significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain.

937. How is "critical infrastructure sector" defined by OFAC?

"Critical infrastructure sector," consistent with Section 1016 of the USA PATRIOT Act, is defined by OFAC as "systems and assets, whether physical or virtual, so vital to the United States that the

incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters." Sixteen critical infrastructure sectors were identified in Presidential Policy Directive – Critical Infrastructure Security and Resilience published in 2013 with the following designated sector-specific agencies (SSA):

- Chemical – SSA: Department of Homeland Security (DHS)
- Commercial Facilities – SSA: DHS
- Communications – SSA: DHS
- Critical Manufacturing – SSA: DHS
- Dams – SSA: Department of Defense (DOD)
- Defense Industrial Base – SSA: DOD
- Emergency Services – SSA: DHS
- Energy – SSA: Department of Energy (DOE)
- Financial Services – SSA: Department of the Treasury (U.S. Treasury)
- Food and Agriculture – SSA: Department of Agriculture (DOA) and Department of Health and Human Services (DHHS)
- Government Facilities – SSA: DHS and General Services Administration (GSA)
- Healthcare and Public Health – SSA: DHHS
- Information Technology – SSA: DHS
- Nuclear Reactors, Materials and Waste – SSA: DHS
- Transportation Systems – SSA: DHS and Department of Transportation (DOT)
- Water and Wastewater Systems – SSA: Environmental Protection Agency (EPA)

938. How is "misappropriation" defined by OFAC?

"Misappropriation" is defined by OFAC as "any taking or obtaining by improper means, without permission or consent, or under false pretenses."

939. Who should screen against the Cyber-Related Sanctions Program List?

As with all OFAC Sanctions Programs, these requirements apply to U.S. persons. "U.S. persons" are defined as U.S. citizens and permanent resident aliens, regardless of where they are located in the world; all persons and entities within the United States; and all U.S.-incorporated entities and their foreign branches.

940. What action must institutions take if a positive "hit" is identified for the Cyber-Related Sanctions List?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Financial institutions may also be required to file Suspicious Activity Reports (SARs) if the cyber-related-event transaction involves or aggregates to US$5,000 (including assets directly involved and put at risk by the cyber event). Previously, financial institutions have been required to file SARs on electronic intrusions and computer-related crimes. That activity was typically related to the use of cyberspace to commit financial crimes. The Cyber-Related Sanctions Program targets the cyber-attack itself which may be executed for financial gain or terrorism-related. For further guidance on filing SARs on cyber-related activity, please refer to the Suspicious Activity Reports section.

FinCEN has established a hotline, 1.866.556.3974, for institutions to report to law enforcement suspicious activity that may relate to recent cyber attacks against the United States.

941. Do financial institutions have any other obligations to report cyber attacks?

In addition to filing SARs and reporting ongoing cyber attacks to FinCEN via their hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals with links to fraudulent websites);
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware)

Other federal agencies with reporting mechanisms include, but are not limited to, the following:

- United States Computer Emergency Readiness Team (US-CERT);
- The Federal Bureau of Investigation (FBI) through the Internet Crime Complaint Center (IC3); and
- The Department of Defense (DoD) for companies performing DoD contracts.

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. In 2016, the New York State Department of Financial Services (DFS) proposed "Part 500 – Cybersecurity

Requirements for Financial Services Companies" that will require the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Incidents section.

942. What information and guidance have been issued with respect to cybercrimes and cybersecurity?

The following key guidance and resources have been provided related to cybercrimes and cybersecurity:

- **Cybersecurity Framework Frequently Asked Questions** by the National Institute of Standards and Technology (NIST)
- **Glossary of Key Information Security Terms** (2013) by the NIST
- **Advanced Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards** (2016) by the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC)
- **Cybersecurity Assessment Tool** (2015) by the Federal Financial Institutions Examination Council (FFEIC)
- **Cybersecurity Assessment General Questions** by the FFIEC
- **Protecting Personal Information: A Guide for Business** by the Federal Trade Commission (FTC)
- **Data Breach Response: A Guide for Business** by the FTC
- **Start with Security: A Guide for Business: Lessons Learned from FTC Cases** by the FTC
- **Cyber Criminal Exploitation of Electronic Payment Systems and Virtual Currencies** (2011) by the FBI
- **Cyber Criminal Exploitation of Real-Money Trading** (2011) by the FBI

- **Typology Report: Cybercrime and Money Laundering** (2014) by the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)
- **The NIST Cybersecurity Framework and the FTC** (2016) by the FTC and Andrea Arias
- **Guidance on Cyber Resilience for Financial Market Infrastructures** (2016) by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO)
- **The National Strategy to Secure Cyberspace** (2003) by the Department of Homeland Security (DHS)
- **Infrastructure Threats - Intrusion Risks** (2000) by the OCC
- **Guidance Concerning Reporting Computer-Related Crimes by Financial Institutions** (1997) by the FRB
- **Guidance for Financial Institutions on Reporting Computer-Related Crimes** (1997) by the National Credit Union Administration (NCUA)
- **Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime** (2016) by FinCEN
- **Frequently Asked Questions (FAQs) Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime and Cyber-Related Information through Suspicious Activity Reports (SARs)** (2016) by FinCEN
- **Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes** (2016) by FinCEN
- **Account Takeover Activity** (2011) by FinCEN
- **Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation and Additional Resources** (2014) by the FFIEC
- **Destructive Malware and Compromised Credentials** (2015) by the FFIEC
- **Cyber Attacks Involving Extortion** (2015) by the FFIEC
- **Presidential Policy Directive – Critical Infrastructure Security and Resilience** (2013) by the White House
- **Best Practices for Victim Response and Reporting of Cyber Incidents** (2015) by the Cybersecurity Unit of the Computer Crime & Intellectual Property Section (CCIPS) of the Department of Justice (DOJ)
- **Ransomware: What Is It and What To Do About It** (2016) by the Cybersecurity Unit
- **How to Protect Your Networks from Ransomware: Interagency Technical Guidance Document** (2016) by the Cybersecurity Unit and other agencies

- **Avoiding Social Engineering and Phishing Attacks** (2017) by the United States Computer Emergency Readiness Team (US-CERT)
- **Fact Sheet: Cybersecurity National Action Plan** (2016) by the White House
- **Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government** by the U.S. Department of Homeland Security (DHS)
- **Reporting Computer, Internet-Related or Intellectual Property Crime** by the U.S. Department of Justice (DOJ) Computer Crime and Intellectual Property Section (CCIPS)
- **Public Service Announcements (PSAs) by the Internet Crime Complaint Center** (IC3) of the Federal Bureau of Investigation (FBI):
    - **Business E-Mail Compromise** (2015 & 2016)
    - **E-Mail Account Compromise** (2015)
    - **E-Mail Extortion Campaigns Threatening Distributed Denial of Service Attacks** (2015)
    - **Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes** (2015)
    - **Criminals Host Fake Government Services Web Sites to Acquire Personally Identifiable Information and to Collect Fraudulent Fees** (2015)
    - **FBI Warns of Fictitious 'Work-From-Home' Scam Targeting University Students** (2015)
    - **Gift Card Scams** (2015)
    - **Hacktivists Threaten to Target Law Enforcement Personnel and Public Officials** (2015)
    - **Internet of Things Poses Opportunities for Cyber Crime** (2015)
    - **ISIL Defacements Exploiting Wordpress Vulnerabilities** (2015)
    - **New Microchip-Enabled Credit Cards May Still Be Vulnerable to Exploitation by Fraudsters** (2015)
    - **Scammers May Use Paris Terrorist Attack to Solicit Fraudulent Donations** (2015)
    - **Tax Return Fraud** (2015)
    - **University Employee Payroll Scam** (2015)
- **Internet Crime Report** (2015; published annually) by IC3
- **Infrastructure Threats – Intrusion Risks** (2000) by the Office of the Comptroller of the Currency (OCC)

- **Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions** (1997) by the Federal Reserve Board (FRB)
- **Guidance for Financial Institutions on Reporting Computer-Related Crimes** (1997) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance for Reporting Computer-Related Crimes** (1997) by the National Credit Union Association (NCUA)
- **Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015** by the U.S. Department of Homeland Security (DHS)
- **Start with Security: A Guide for Business: Lessons Learned from FTC Cases** by the Federal Trade Commission (FTC)
- **Framework for Improving Critical Infrastructure Cybersecurity** (2014) by the National Institute of Standards and Technology (NIST)
- **Report on Cybersecurity Practices** (2015) by the Financial Industry Regulatory Authority (FINRA)
- **Principles for Effective Cybersecurity: Insurance Regulatory Guidance** (2015) by the National Association of Insurance Commissioners (NAIC)
- **Cybersecurity Examination Initiative** (2015) by the Office of Compliance Inspections and Examinations (OCIE)
- **Cybersecurity Examination Sweep Summary** (2015) by the OCIE
- **Report on Cyber Security in the Insurance Sector** (2014) by New York State Department of Financial Services (DFS)
- **Report on Cyber Security in the Insurance Sector** (2015) by NYDFS
- **Update on Cyber Security in the Banking Sector: Third Party Service Providers** (2015) by NYDFS
- **Council Framework Decision: Combating Fraud and Counterfeiting of Non-Cash Means of Payment** (2001) by the Council of the European Union
- **Internet Organised Crime Threat Assessment (IOCTA)** (2011, 2014, 2015, 2016) by Europol's European Cybercrime Center (EC3)

Rough Diamond Trade Controls Sanctions Program

943. What is OFAC's Rough Diamond Trade Controls Sanctions program?

Established by the Clean Diamond Trade Act (CDTA), IEEPA, NEA, UNPA and Executive Order 13312 – Implementing the Clean Diamond Trade Act, OFAC's Rough Diamond Trade Controls Sanctions Program prohibits the import and export of rough diamonds from countries that do not participate in

the Kimberley Process Certification Scheme (KPCS) and prohibits any transaction that evades or attempts to evade these prohibitions on or after July 30, 2003.

The Rough Diamond Trade Control Sanctions Program is implemented under 31 C.F.R. Part 592 – Rough Diamonds Control Regulations.

944. Are designees under the Rough Diamond Trade Controls Sanctions Program included on the SDN List?

No. Unlike the other OFAC Sanctions Programs, the Rough Diamond Trade Controls Sanctions Program does not designate targets. Instead, the program requires importers and exporters of rough diamonds to participate in the KPCS and report their activities to the Department of State.

945. What is the Kimberley Process Certificate Scheme (KPCS)?

Launched in 2003, the Kimberley Process Certificate Scheme (KPCS) is an international program that implements certification requirements and other import/export controls to prevent the production and trade in rough diamonds that are used to finance violence in countries in conflict (e.g., Democratic Republic of the Congo, Cote d'Ivoire). These diamonds are also known as "conflict diamonds" or "blood diamonds."

The Kimberley Process Certificate is a unique tamper- and forgery-resistant document that certifies that a shipment of rough diamonds was handled in accordance with the KPCS. Kimberley Process Certificates can only be obtained from entities licensed by the U.S. Kimberley Process Authority (USKPA).

For imported rough diamonds, the ultimate consignee is required to report receipt of the shipment to the relevant foreign exporting authority (e.g., the agency with the authority to validate the Kimberley Process Certificate). Reports must be made within 15 calendar days of the date that the shipment arrived at a U.S. port of entry.

For exported rough diamonds, exporters must report the shipment to the U.S. exporting authority, the U.S. Bureau of Census, through the Automated Export System (AES).

U.S. Customs will not release shipments of rough diamonds without formal and complete documentation.

946. How are "rough diamonds" defined under the Rough Diamond Trade Controls Sanctions Program?

"Rough diamonds" are defined as "any diamond that is unworked or simply sawn, cleaved or bruted and classifiable under subheading 7102.10, 7102.21, or 7102.31 of the Harmonised Tariff Schedule of the United States."

947. Do the prohibitions under the Rough Diamond Trade Controls Sanctions Program apply to rough diamonds of any value?

Yes. There is no minimum threshold. Rough diamonds of all values are subject to the Rough Diamond Trade Controls Sanctions Program.

948. How is a "stockpile" defined under the Rough Diamond Trade Controls Sanctions program?

A "stockpile" is defined as "the amount of rough diamonds held unsold at the end of the reporting period (e.g., January 1 – December 31)."

949. How are "participants" defined under the Rough Diamond Trade Controls Sanctions program?

"Participants" are defined as a "state, customs territory or regional economic integration organisation identified by the Secretary of State as one for which rough diamonds are controlled through the Kimberley Process Certification Scheme (KPCS)."

The Department of State publishes eligible participants (and their importing and exporting authorities) in the Federal Register. Currently, there are more than 50 participants, with the countries of Cambodia, Cameroon, Kazakhstan, Mali and Panama added and the Central African Republic removed in recent years. The latest list of KPCS participants can be found at the Conflict Diamonds section of the U.S. State Department's website at http://www.state.gov/e/eb/tfs/tfc/diamonds/index.htm.

950. Are there exceptions that allow for import/export of rough diamonds to a nonparticipating country?

Yes. The Department of State may waive the prohibitions for a particular country for a set time frame, not more than one year. Exceptions are published in the Federal Register.

951. Who is required to file Rough Diamond Trading Reports?

By April 1 of each year, all persons who import or export rough diamonds to/from the United States are required to file reports covering their import/export activity (e.g., total carats, total shipments) for the previous year (e.g., January 1 – December 31). Reports must be filed with the Office of the Special Advisor for Conflict Diamonds at the U.S. Department of State.

952. What should financial institutions do with regard to the Rough Diamond Trade Controls Sanctions Program?

Financial institutions should identify customers who may be involved in the rough diamond business and conduct appropriate due diligence to mitigate their AML/CFT and sanctions risks.

For further guidance, please refer to the Dealers in Precious Metals, Precious Stones or Jewels section.

953. Are any other types of jewels, stones or minerals subject to sanctions by OFAC?

Yes. Section 1245 of the Iran Freedom and Counter-Proliferation Act of 2012 (IFCA) imposes sanctions on persons engaged in trade in precious metals, graphite, raw or semifinished metals, such as aluminium and steel, with sanctioned persons as outlined in Executive Order 13645. Additionally, a number of the sanctions, such as the Iranian and Cuban sanctions, impose broad prohibitions on a wide range of imports and exports. Some of the country-based sanctions programs aim to protect other "natural resources" (e.g., jade, oil) of select countries in conflict (e.g., Myanmar [Burma], Libya).

Although not a sanction per se, Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act requires that a company publicly disclose if it uses conflict minerals that originated in the Democratic Republic of the Congo or adjoining countries (collectively, the covered countries) that are "necessary to the functionality or production" of a product manufactured or contracted to be manufactured by the company.

The purchase of these so-called conflict minerals allegedly benefits armed rebels in these countries, and the required disclosure is expected to put pressure on companies to disassociate with the covered countries.

The U.S. Securities and Exchange Commission (SEC) rule implementing this provision of the Dodd-Frank Act requires both domestic and foreign issuers that file with the SEC to publicly disclose their use of conflict minerals on a new form, Form SD, the first of which were to be filed by June 2, 2014, and required annually on May 31 thereafter. In instances where a company determines that conflict materials are from covered countries, a Conflict Minerals Report must accompany Form SD.

The regulation does provide for a two-year transition period (four years for smaller companies) in which a company may consider its products "DRC conflict undeterminable" if it is unable to determine the source of minerals used.

"False or misleading statements" in the form will subject a company to liability under Section 18 of the Securities Exchange Act of 1934.

954. How is the term "conflict mineral" defined by the SEC?

Conflict minerals "outside of the supply chain" (e.g., have not been smelted or refined) from covered countries include the following minerals:

- Cassiterite
- Columbite-tantalite
- Gold
- Wolframite
- Any derivatives of the aforementioned minerals
- Any mineral designated by the U.S. Secretary of State

Covered countries include the following:

- Democratic Republic of the Congo (DRC)
- The Republic of the Congo
- Angola
- Burundi
- Central African Republic (CAR)
- Rwanda

- South Sudan
- Tanzania
- Uganda
- Zambia

955. What are some uses of these "conflict minerals"?

These minerals are often used in the manufacturing of consumer electronics (e.g., computers, mobile phones), automobiles and jewellery.

956. Is there a similar "Kimberley Certification" scheme in place to certify that minerals did not originate in covered countries in conflict?

No. However, the SEC does require that a company conduct a reasonable country of origin inquiry (RCOI) to determine if the company's minerals originated from covered countries.

Further guidance on a due diligence framework for assessing global mineral supply chains is provided in the OECD Due Diligence Guidance for Responsible Supply Chains of Minerals From Conflict-Affected and High-Risk Areas (2013) by the Organisation for Economic Co-operation and Development (OECD).

Country- and Regime-Based Sanctions Programs

Overview

957. What are the Country- and Regime-Based Sanctions Programs administered by OFAC?

OFAC administers a number of U.S. economic sanctions, ranging from comprehensive bans against conducting activity with all individuals/entities from a specified country (e.g., there is a broad ban on Cuban transactions with only limited exceptions) or jurisdiction, to limited regime-based bans that prohibit transactions/trade with a particular individual/entity/regime or activity (e.g., diamond-related activity). A sample of countries and regimes subject to OFAC sanctions include, but are not limited to, the following:

- Balkans [BALKANS]
- Belarus [BELARUS]
- Burundi [BURUNDI]
- Central African Republic [CAR]
- Cuba [CUBA]
- Democratic Republic of the Congo [DRCONGO]
- Iran [IRAN], [IRAN-HR], [IRAN-TRA], [IFSR], [IRGC], [ISA], [IFCA], [HRIT-IR], [EO13622], [EO13645], [FSE-IR]

- Iraq [IRAQ2], [IRAQ3]
- Lebanon [LEBANON]
- Libya [LIBYA2]
- Magnitsky (Russian Officials Involved in Sergei Magnitsky's Death) [MAGNIT]
- North Korea [DPRK]
- Somalia [SOMALIA]
- South Sudan [SOUTH SUDAN]
- Syria [SYRIA], [HRIT-SY], [FSE-SY]
- Ukraine [UKRAINE-EO13660], [UKRAINE-EO13661], [UKRAINE-EO13662]
- Venezuela [VENEZUELA]
- Yemen [YEMEN]
- Zimbabwe [ZIMBABWE]

Sanctions programs for the following were terminated:

- Burma [BURMA] (2016)
- Côte d'Ivoire [CÔTED] (2016)
- Former Liberian Regime of Charles Taylor [LIBERIA] (2015)
- Sudan [SUDAN] (2017)

For details of OFAC Country- and Regime-Based Sanctions Programs, please see below and refer to OFAC's website: www.treas.gov/offices/enforcement/ofac.

958. What are the primary objectives of OFAC Sanctions Programs affecting these countries and regimes?

In addition to the objectives of OFAC to combat terrorism, narcotics trafficking, the proliferation of WMDs, and transnational criminal organisations, the primary objective of the U.S. government with respect to the aforementioned countries and regimes vary but overall, aim for the following:

- Reduce/eliminate political corruption;
- Reduce/eliminate misappropriation of public assets and natural resources;
- Politically stabilise regions;
- Protect sovereignty and territorial integrity;
- Reduce/eliminate human rights violations with an emphasis on acts of violence against women, children and refugees;
- Reduce/eliminate the use and recruitment of child soldiers;

- Protect internationally accepted human rights (e.g., freedom of expression, religion, right to assemble)
- Protect channels delivering humanitarian assistance; and
- Protect international peacekeeping missions.

Summaries of each of the country and regime based programs are provided below.

959. Are there exemptions from OFAC country-and-regime based sanctions programs?

Yes. Both OFAC sanctions exempt exports and imports of information or informational materials (subject to restrictions) and transactions ordinarily incident to travel. In addition, certain transactions, such as those involving the provision of legal services or those involving exports (e.g., food, agricultural commodities, medicine, medical devices) are eligible for specific licenses issued by OFAC or BIS or, in some cases, general licenses. In fact, nearly any transaction can be licensed specifically by OFAC on a case-by-case basis. For further guidance, please review each country-and-regime based sanctions program.

960. Are existing contracts and licenses still valid after the issuance of subsequent OFAC sanctions?

Generally, existing contracts that cover prohibited activities or involve designated individuals or entities are no longer enforceable under U.S. law -- and performance under such contracts is not permissible--unless a valid license has been issued authorising the contract. Persons who have been issued licenses involving persons designated under OFAC sanctions should check with the issuing agency regarding the ongoing validity of their licenses.

For further guidance, please refer to the OFAC Licensing section.

Balkans-Related Sanctions Program Overview

961. What are the major U.S. government sanctions programs affecting the Balkans?

The U.S. government has imposed sanctions on the Western Balkans (e.g., former Yugoslav Republic of Macedonia, Bosnia, Serbia, Federal Republic of Yugoslavia), including those mandated by the following statutes and executive orders:

- National Emergencies Act (NEA) (1976)
- International Emergency Economic Powers Act (IEEPA) (1977)
- Executive Order 13219 – Blocking Property of Persons Who Threaten International Stabilisation Efforts in the Western Balkans (2001)
- Executive Order 13304 – Termination of Emergencies With Respect to Yugoslavia and Modification of Executive Order 13219 of June 26, 2001 (2003)

The following United Nations Security Council Resolution (UNSCR) was issued with respect to the Balkans:

UNSCR 1244 (1999)

The following regulation implements Balkans-Related sanctions:

31 C.F.R. Part 588 – Western Balkans Stabilisation Regulations

962. What are the primary objectives of OFAC Sanctions Programs affecting the Western Balkans?

The primary objective of the U.S. government is to stabilise and secure the Western Balkans region in accordance with international efforts as outlined by the United Nations (e.g., United Nations Security Resolution [UNSR] 1244 (1999)), North Atlantic Treaty Organisation [NATO], the Dayton Accords in Bosnia and other international organisations present in the Western Balkan area.

According to OFAC's Western Balkan Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Committed or posed a significant risk of committing acts of violence that have the purpose or effect of threatening the peace in or diminishing the stability or security in the Western Balkans;
- Undermined the authority, efforts or objectives of international organisations in the Western Balkans;
- Endangered the safety of persons participating in or providing support to the activities of international organisations in the Western Balkans;
- Actively obstructed or posed a significant risk of actively obstructing the implementation of the Dayton Accords in Bosnia or the UNSR 1244;
- Assisted materially, sponsored or provided financial or technological support for good or services in support of such acts of violence or obstructionism; or
- Owned or controlled property or interests, acted or purported to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Balkans Sanctions Program.

963. Where can one find a list of designated entities under the Balkans Sanctions Program?

Designations are maintained in the appendices of applicable Balkans regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [BALKANS].

964. What action must institutions take if a positive "hit" is identified for the Balkans Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Belarus Sanctions Program Overview

965. What are the major U.S. government sanctions programs affecting Belarus?

The U.S. government has imposed sanctions on the Republic of Belarus, including those mandated by the following statutes and executive orders:

- National Emergencies Act (NEA) (1976)
- International Emergency Economic Powers Act (IEEPA) (1977)
- Executive Order 13405 – Blocking Property of Certain Persons Undermining Democratic Processes or Institutions in Belarus (2006)

The following regulation implements Belarusian sanctions:

- 31 C.F.R. Part 548 – Belarus Sanctions Regulations

966. What are the primary objectives of OFAC Sanctions Programs affecting Belarus?

The primary objectives of the U.S. government with respect to Belarusian sanctions are to protect the democratic processes and institutions of Belarus.

According to OFAC's Belarus Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Participating in actions or policies that undermine democratic processes or institutions in Belarus;
- Participating in human rights abuses related to political repression in Belarus;
- Are senior-level officials, family members of such officials, or persons closely linked to such officials who were responsible for or engaged in public corruption related to Belarus;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services in support of the aforementioned activities or SDNs designated by Belarusian sanctions; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Belarus Sanctions Program.

967. Where can one find a list of designated entities under the Belarus Sanctions Program?

Designations are maintained in the appendices of applicable Belarusian regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [BELARUS].

968. What action must institutions take if a positive "hit" is identified for the Belarusian Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For

guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Burma (Myanmar) Sanctions Program Overview

969. What are the major U.S. government sanctions programs affecting Burma?

The U.S. government has imposed sanctions on the Republic of the Union of Myanmar (Burma), including those mandated by the following statutes and executive orders:

- National Emergencies Act (NEA) (1976)
- International Emergency Economic Powers Act (IEEPA) (1977)
- Foreign Operations, Export Financing and Related Programs Appropriations Act, Section 570 (1997)
- Burma Freedom and Democracy Act of 2003 (BFDA) (2003)
- Tom Lantos Block Burmese Jade Act of 2008 (Junta's Anti-Democratic Efforts) (JADE) (2008)
- Executive Order 13047 – Prohibiting New Investment in Burma (1997)
- Executive Order 13310 – Blocking Property of the Government of Burma and Prohibiting Certain Transactions (2003)
- Executive Order 13448 – Blocking Property and Prohibiting Certain Transactions Related to Burma (2007)
- Executive Order 13464 – Blocking Property and Prohibiting Certain Transactions Related to Burma (2008)
- Executive Order 13619 – Blocking Property of Persons Threatening the Peace, Security or Stability of Burma (2012)
- Executive Order 13651 – Prohibiting Certain Imports of Burmese Jadeite and Rubies (2013)
- Executive Order 13742 – Termination of Emergency With Respect to the Actions and Policies of the Government of Burma (2016)

The following regulation implemented Burmese sanctions:

- 31 C.F.R. Part 537 – Burmese Sanctions Regulations

As of October 2016, the U.S. terminated the Burmese Sanctions Programs.

970. What were the primary objectives of OFAC Sanctions Programs affecting Burma?

The primary objective of the U.S. government was to restrict and eliminate the large-scale repression of the democratic opposition in Burma primarily lead by the Government of Burma (then ruled by military junta). Due to human rights and labour concerns, the Burmese Sanctions Program also restricted the importation of any jadeite or rubies mined or extracted from Burma pursuant to the Tom Lantos Block Burmese Jade Act of 2008 (Junta's Anti-Democratic Efforts [JADE] of 2008).

971. What is a "military junta" according to the Burmese Sanctions Program?

The Burmese Sanctions Program does not define "military junta." It is generally understood to mean a military dictatorship.

972. What is "jadeite" according to the Burmese Sanctions Program?

Per the Burmese Sanctions Program, "jadeite" means "any jadeite classifiable under heading 7103 of the Harmonised Tariff Schedule of the United States" (HTSA), the primary resource for determining tariff rates and statistical categories for all merchandise imported into the United States.

973. Where can one find a list of designated entities under Burmese Sanctions Program?

Designations were maintained in the appendices of the Burmese regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [BURMA]. As of October 2016, the U.S. terminated the Burmese Sanctions Programs.

974. Does the termination of the Burmese Sanctions Program impact Burmese persons pursuant to other OFAC Sanctions Programs (e.g., Counter Narcotics Trafficking Sanctions Program)?

No. The termination of the Burmese Sanctions Program does not impact designees pursuant to other OFAC Sanctions Programs.

975. Does the termination of the Burmese Sanctions Program impact Burmese persons pursuant to Burma's special designation under Section 311 of the USA PATRIOT Act?

In 2003, Burma was designated as a "jurisdiction of primary money laundering concern" under Section 311 of the USA PATRIOT Act. While that designation is current and independent of the Burmese Sanctions Program, FinCEN has also issued an administrative ruling suspending the Section 311 designation to allow U.S. financial institutions to provide correspondent banking accounts to Burmese financial institutions.

Burundi Sanctions Program Overview

976. What are the major U.S. government sanctions programs affecting Burundi?

The U.S. government has imposed sanctions on the Republic of Burundi, including those mandated by the following statutes and executive orders:

- National Emergencies Act (NEA) (1976)
- International Emergency Economic Powers Act (IEEPA) (1977)
- Executive Order 13712 – Blocking Property of Certain Persons Contributing to the Situation in Burundi (2015)

The following regulation implemented Burmese sanctions:

- 31 C.F.R. Part 554 – Burundi Sanctions Regulations

977. What are the primary objectives of OFAC Sanctions Programs affecting Burundi?

The primary objective of the U.S. government with respect to Burundi sanctions is to restrict and eliminate the violence against civilians and significant political repression that threatens the peace, security and stability of Burundi.

According to Executive Order 13712, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions or policies that threaten the peace, security or stability of Burundi;
- Actions or policies that undermine democratic processes or institutions in Burundi;
- Committing human rights abuses;
- Targeting women, children or any civilian through the commission of acts of violence (e.g., killing, maiming, torture, rape, abduction, forced displacement) or other conduct that may constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Targeting schools, hospitals, religious sites or locations where civilians are seeking refuge through the commission of acts of violence or other conduct that may constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Actions or policies that prohibit, limit or penalise the exercise of freedom of expression or freedom of peaceful assembly;
- Using or recruiting children for armed groups or forces;
- Obstructing the delivery, distribution or access to humanitarian assistance;
- Attacking, attempting to attack or threatening United Nations missions, international security presences or other peacekeeping operations;
- Being a leader or official of an entity, including any government entity or armed group, that has, or whose members have, engaged in any of the aforementioned activities;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned activities; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Burundi Sanctions Program.

978. Where can one find a list of designated entities under the Burundi Sanctions Program?

Designations are maintained in the appendices of applicable Burundi regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [BURUNDI].

979. What action must institutions take if a positive "hit" is identified for the Burundi Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Central African Republic (CAR) Sanctions Program Overview

980. What are the major U.S. government sanctions programs affecting the Central African Republic (CAR)?

The U.S. government has imposed sanctions on the Central African Republic (CAR), including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949)
- **Immigration and Nationality Act of 1952** (1952)
- **Executive Order 13667 – Blocking Property of Certain Persons Contributing to the Conflict in the Central African Republic** (2014)

The following regulation implemented CAR sanctions:

- **31 C.F.R. Part 553 – Central African Republic Sanctions Regulations**

981. What are the primary objectives of OFAC Sanctions Programs affecting the CAR?

The primary objectives of the U.S. government with respect to the CAR sanctions are to restrict and eliminate the breakdown of law and order, intersectarian tension, widespread violence and atrocities, forced recruitment and use of child soldiers that threaten the peace, security or stability of the CAR.

According to OFAC's CAR Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions or policies that threaten the peace, security or stability of the CAR;
- Actions or policies that threaten transitional agreements or the political transition process in the CAR;
- Targeting of women, children or any civilian through the commission of acts of violence (e.g., killing, maiming, torture, rape, abduction, forced displacement) or other conduct that may constitute a serious abuse or violation of human rights or a violation of international humanitarian law;

- Targeting of schools, hospitals, religious sites or locations where civilians are seeking refuge through the commission of acts of violence or other conduct that may constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Actions or policies that prohibit, limit or penalise the exercise of freedom of expression or freedom of peaceful assembly;
- The use or recruitment of children for armed groups or forces;
- Obstruction of the delivery, distribution or access to humanitarian assistance;
- Attacking or attempting to attack or threaten United Nations missions, international security presences or other peacekeeping operations;
- Have been a leader or official of an entity, including any government entity or armed group, that has, of whose members have, engaged in any of the aforementioned activities;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned activities; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the CAR Sanctions Program.

982. Where can one find a list of designated entities under CAR Sanctions Program?

Designations are maintained in the appendices of applicable CAR regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [CAR].

983. What action must institutions take if a positive "hit" is identified for the CAR Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Côte d'Ivoire (Ivory Coast) Sanctions Program Overview

984. What were the major U.S. government sanctions programs affecting the Côte d'Ivoire?

The U.S. government has imposed numerous sanctions on the Republic of Côte d'Ivoire, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949)

- **Executive Order 13396 – Blocking Property of Certain Persons Contributing to the Conflict in Côte d'Ivoire** (2006)
- **Executive Order 13739 – Termination of Emergency with Respect to the Situation in or in Relation to Côte d'Ivoire** (2016)

The following United Nations Security Council Resolutions (UNSCR) was issued with respect to Côte d'Ivoire:

- **UNSCR 1572** (2004)

The following regulation implemented Côte d'Ivoire sanctions:

- **31 C.F.R. Part 543– Côte d'Ivoire Sanctions Regulations**

As of September 2016, the U.S. terminated the Côte d'Ivoire Sanctions Program.

985. What were the primary objectives of OFAC Sanctions Programs affecting Côte d'Ivoire?

The primary objectives of the U.S. government with respect to Côte d'Ivoire sanctions were to restrict and eliminate the widespread human rights abuses committed against citizens of Côte d'Ivoire (e.g., massacres), political violence and unrest and fatal attacks against international peacekeeping forces.

According to OFAC's Côte d'Ivoire Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Threatening the peace and reconciliation process in Côte d'Ivoire (e.g., by blocking initiatives such as the Linas-Marcoussis Agreement of January 24, 2003, the Accra III Agreement of July 30, 2004, Pretoria Agreement of April 6, 2005);
- Serious violations of international law in Côte d'Ivoire;
- Supplying, selling or transferring to Côte d'Ivoire arms or any related material or assistance, advice or training related to military activities;
- Publicly incited violence and hatred contributing to the conflict in Côte d'Ivoire;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned acts; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Côte d'Ivoire Sanctions Program.

986. Where can one find a list of designated entities under Côte d'Ivoire Sanctions Program?

Designations were maintained in the appendices of applicable Côte d'Ivoire regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [CÔTED]. As of September 2016, the U.S. terminated the Côte d'Ivoire Sanctions Program.

987. Does the termination of the Côte d'Ivoire Sanctions Program impact Côte d'Ivoire persons pursuant to other OFAC Sanctions Programs (e.g., Counter Narcotics Trafficking Sanctions Program)?

No. The termination of the Côte d'Ivoire Sanctions Program does not impact designees pursuant to other OFAC Sanctions Programs.

Cuban Sanctions Program Overview

988. What are the major U.S. government sanctions programs affecting the Cuba?

The U.S. government has imposed numerous sanctions on the Republic of Cuba, including those mandated by the following statutes and executive orders, which are listed in chronological order:

- **Trading With the Enemy Act of 1917 (TWEA)** (1917)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Cuban Democracy Act of 1992 (CDA)** (1992)
- **Executive Order 12854 - Implementation of the Cuban Democracy Act** (1993)
- **Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA)** (1996)
- **Cuban Liberty and Democratic Solidarity (Libertad) Act of 1996** (1996)
- **Trade Sanctions Reform and Export Enhancement Act of 2000 (TSRA)** (2000)

The following regulation implements Cuban sanctions:

- **31 C.F.R. Part 515 – Cuban Assets Control Regulations**

989. What are the primary objectives of OFAC Sanctions Programs affecting Cuba?

The primary objective of the U.S. government with respect to Cuban sanctions was to isolate the Cuban government economically and deprive it of U.S. dollars in response to past hostile acts by the Cuban government.

990. What significant updates were made to the Cuban Sanctions Program under the Obama administration?

Under the Obama administration, while many of the Cuban sanctions remained in place, between 2014 and 2016, the Cuban Sanctions Program was amended to facilitate economic opportunity for Cubans and Americans in areas including, but not limited to, the following:

- Health-Related (e.g., joint medical research, Cuban-origin pharmaceuticals)
- Humanitarian-Related (e.g., grants, scholarships related to scientific research, religion, disaster-relief, historical preservation)
- Travel-Related (e.g., travel agents and airlines authorised to provide travel services without a specific license from OFAC)

- Banking and Financial Services-Related (e.g., allowance of financial transactions in U.S. dollars presented by Cuban financial institutions and Cuban nationals; increased limit on quarterly remittances to Cuba)
- Telecommunications and Internet-Related (e.g., provision of services to enhance the flow of information to, from and within Cuba and between Cuba and the U.S.)
- Civil Aviation-Related (e.g., provision of safety-related services to promote safe operation of commercial aircrafts)
- Trade and Commerce-Related (e.g., consumer goods for personal use of Cuban-origin merchandise, financing of agricultural commodities)
- Diplomatic Relations-Related (e.g., general license permitting authorised transactions with Cuban official missions)

991. What types of travel-related activities are permitted under the Cuban Sanctions Program?

The following types of travel-related activities are permitted under general license, subject to the criteria and conditions in each general license, under the Cuban Sanctions Program:

- Family visits
- Official business of the U.S. government, foreign governments and certain intergovernmental organisations
- Journalistic activity
- Professional research and professional meetings
- Educational activities
- Religious activities
- Public performances, clinics, workshops, athletic and other competitions and exhibitions
- Support for the Cuban people
- Humanitarian projects
- Activities of private foundations or research or educational institutes
- Exportation, importation or transmission of information or information materials
- Certain authorised export transactions

For further guidance on definitions and permissible activities, OFAC has released numerous guides (e.g., Fact Sheets and Frequently Asked Questions) addressing trade, travel, remittances, banking, telecommunications and humanitarian assistance, including, but not limited to, the following:

- **Frequently Asked Questions Related to Cuba** (2016)

- **FACT SHEET: Treasury and Commerce Announce Regulatory Amendments to the Cuba Sanctions** (January 2015)
- **FACT SHEET: Treasury and Commerce Announce Further Amendments to the Cuba Sanctions Regulations** (2015)
- **FACT SHEET: Treasury and Commerce Announce Further Amendments to the Cuba Sanctions Regulations** (2016)
- **FACT SHEET: Treasury and Commerce Announce Significant Amendments to the Cuba Sanctions Regulations** (2016)
- **FACT SHEET: Treasury and Commerce Announce Further Amendments to the Cuba Sanctions Regulations** (2016)
- **OFAC Guidance Regarding Travel Between the United States and Cuba** (2016)
- **OFAC Guidance on Certain Publishing Activities** (2016)

992. Are U.S. financial institutions now permitted to provide financial services to Cuban nationals or Cuban financial institutions under the Cuban Sanctions Program?

Generally, the provision of financial services to Cuban nationals or Cuban financial institutions by U.S. financial institutions is prohibited. When permitted, restrictions apply, including, but not limited to, the following:

- Transactions conducted through accounts must be permissible under OFAC general and/or specific licenses or exempted from Cuban Sanctions;
- Access to accounts must be restricted to when the account holder is lawfully within the United States or outside of Cuba if offered in a third-country.

For further guidance on permissible activities, please refer to the Fact Sheets and frequently asked questions guidance provided by OFAC.

993. Are U.S. financial institutions permitted to establish correspondent accounts at Cuban financial institutions under the Cuban Sanctions Program?

Yes, U.S. financial institutions are permitted to establish correspondent accounts at Cuban financial institutions, however, some restrictions may apply, such as transactions may be limited to those permissible under OFAC general and/or specific licenses or exempted from Cuban Sanctions.

994. Are U.S. financial institutions permitted to process transactions originating and terminating outside the United States on behalf of Cuban financial institutions as intermediary institutions?

Yes. Although U.S. institutions are generally prohibited from providing correspondent accounts to Cuban financial institutions, U.S. financial institutions are permitted to process transactions that originate and terminate outside of the United States as intermediary institutions provided the originator and beneficiary are not subject to Cuban Sanctions (e.g., Specially Designated Nationals

[SDNs]). These transactions are commonly known as "U-turn" payments and are permitted under general license issued by OFAC.

995. What authorisations are required for U.S. financial institutions to release funds that are no longer blocked under the amended Cuban Sanctions Program?

If OFAC has issued a general license authorising U.S. financial institutions to release previously blocked funds, no further authorisation is required. If a general license has not been issued, U.S. financial institutions would require a specific license to release previously blocked funds/accounts.

996. Are U.S. financial institutions expected to verify that a customer's travel is authorised under the Cuban Sanctions Program when processing Cuba-related transactions?

No. U.S. financial institutions are expected to collect certifications of authorised travel from customers when processing Cuba-Related transactions. U.S. financial institutions are not expected to independently verify that the travel is authorised under the Cuban Sanctions Program, unless they have reason to suspect otherwise.

997. Where can one find a list of designated entities under the Cuban Sanctions Program?

Designations are maintained in the appendices of applicable Cuban regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [CUBA].

998. What action must institutions take if a positive "hit" is identified for the Cuban Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

999. What recent changes were made to the Cuba Sanctions Program?

In June 2017, the Trump administration released a Fact Sheet on Cuba Policy outlining key policy changes intended to roll-back the Obama administration's Cuban policy changes, including, but not limited to, the following:

- Channelling economic activities away from the Cuban military monopoly, Grupo de Administración Empresarial (GAESA), including most travel-related transactions, and toward the private, small business sector in Cuba;
- Enhanced travel restrictions (e.g., limiting travel for non-academic educational purposes to group travel, prohibiting self-directed, individual travel);
- Reaffirmation of the United States statutory embargo of Cuba and opposition to calls in the United Nations and other international forums for its termination; and

- Statement that further improvements in the United States-Cuba relationship will be dependent on the Cuban government's willingness to improve the lives of the Cuban people (e.g., promoting the rule of law, respecting human rights, fostering political and economic freedoms).

Policy changes will take effect once the Treasury and Commerce Departments issue new regulations.

Democratic Republic of the Congo Sanctions Program Overview

1000. What are the major U.S. government sanctions programs affecting the Democratic Republic of the Congo?

The U.S. government has imposed sanctions on the Democratic Republic of the Congo (DRC), including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949)
- **Executive Order 13413 – Blocking Property of Certain Persons Contributing to the Conflict in the Democratic Republic of the Congo** (2006)
- **Executive Order 13671 – Taking Additional Steps to Address the National Emergency With Respect to the Conflict in the Democratic Republic of the Congo** (2014)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to the DRC:

- **UNSCR 1596 (2005)**
- **UNSCR 1649 (2005)**
- **UNSCR 1698 (2006)**

The following regulation implemented DRC sanctions:

- **31 C.F.R. Part 547 – Democratic Republic of Congo Sanctions Regulations**

1001. What are the primary objectives of OFAC Sanctions Programs affecting the Democratic Republic of Congo?

The primary objectives of the U.S. government with respect to the DRC sanctions are to restrict and eliminate widespread violence threatening the peace, security and stability of the DRC.

According to OFAC's DRC Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Being a political or military leader of a foreign or Congolese armed group operating in the DRC that impedes the disarmament, demobilisation, voluntary repatriation, resettlement or reintegration of combatants;
- Actions or policies that threaten the peace, security or stability of the DRC;
- Actions or policies that undermine the democratic processes or institutions of the DRC;
- Targeting of women, children or any civilians through the commission of acts of violence (e.g., killing, maiming, torture, rape), abduction, forced displacement that would constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Attacks on schools, hospitals, religious sites or locations where civilians are seeking refuge;
- The use or recruitment of children by armed groups or armed forces in the context of conflict in the DRC;
- Obstruction of the delivery, distribution or access to humanitarian assistance;
- Attacks against United Nations missions, international security presences or other peacekeeping operations;
- Support to persons, including armed groups, involved in activities that threaten the peace, security or stability of the DRC or that undermine democratic processes or institutions in the DRC through the illicit trade in natural resources of the DRC.
- Supplying, selling or transferring to the DRC or been the recipient in the DRC of arms and related material (e.g., military aircraft and equipment), advice, training or assistance (e.g., financing, financial assistance) related to military activities;
- Being a leader of an entity, including any armed group, that has or whose members have engaged in any of the aforementioned acts;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned acts; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the DRC Sanctions Program.

1002. Where can one find a list of designated entities under the Democratic Republic of Congo Sanctions Program?

Designations are maintained in the appendices of applicable DRC regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [DRCONGO].

1003. What action must institutions take if a positive "hit" is identified for the Democratic Republic of Congo Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For

guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Iranian and Syrian Sanctions Program Overview

1004. What are the major U.S. government sanctions programs affecting Iran?

The U.S. government has imposed numerous sanctions on the Islamic Republic of Iran, including those mandated by the following statutes and executive orders, which are listed in chronological order:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 12170 – Blocking Iranian Government Property** (1979)
- **Executive Order 12205 – Prohibiting Certain Transactions With Iran** (1980)
- **Executive Order 12211 – Prohibiting Certain Transactions With Iran** (1981)
- **Executive Order 12276 – Direction Relating to Establishment of Escrow Accounts** (1981)
- **Executive Order 12277 – Direction to Transfer Iranian Government Assets** (1981)
- **Executive Order 12278 – Direction to Transfer Iranian Government Assets Overseas** (1981)
- **Executive Order 12279 – Direction to Transfer Iranian Government Assets Held by Domestic Banks** (1981)
- **Executive Order 12280 – Direction to Transfer Iranian Government Financial Assets Held by Non-Banking Institutions** (1981)
- **Executive Order 12281 – Direction to Transfer Certain Iranian Government Assets** (1981)
- **Executive Order 12282 – Revocation of Prohibitions Against Transactions Involving Iran** (1981)
- **Executive Order 12283 – Non-Prosecution of Claims of Hostages and for Actions at the United States Embassy and Elsewhere** (1981)
- **Executive Order 12284 – Restrictions on the Transfer of Property of the Former Shah of Iran** (1981)
- **Executive Order 12294 – Suspension of Litigation Against Iran** (1981)
- **International Security and Development Cooperation Act of 1985 (ISDCA), Section 505**
- **Executive Order 12613 – Prohibiting Imports From Iran** (1987)

- **Executive Order 12735 – Chemical and Biological Weapons Proliferation** (1990)
- **Executive Order 12851 – Administration of Proliferation of Sanctions, Middle East Arms Control, and Related Congressional Reporting Responsibilities** (1993)
- **Executive Order 12938 – Proliferation of Weapons of Mass Destruction** (1994)
- **Executive Order 12947 – Prohibiting Transactions With Terrorists Who Threaten to Disrupt the Middle East Peace Process** (1995)
- **Executive Order 12957 – Prohibiting Certain Transactions With Respect to the Development of Iranian Petroleum Resources** (1995)
- **Executive Order 12959 – Prohibiting Certain Transactions With Respect to Iran** (1995)
- **Iran-Libya Sanctions Act** (1995)
- **Antiterrorism and Effective Death Penalty Act of 1996** (AEDPA)
- **Iran Sanctions Act of 1996** (ISA)
- **Executive Order 13059 – Prohibiting Certain Transactions With Respect to Iran** (1997)
- **Executive Order 13099 – Prohibiting Transactions With Terrorists Who Threaten to Disrupt the Middle East Peace Process** (1998)
- **Trade Sanctions Reform and Export Enhancement Act of 2000** (TSRA)
- **Executive Order 13224 – Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism** (2001)
- **Executive Order 13382 – Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters** (2005)
- **Executive Order 13553 – Blocking Property of Certain Persons With Respect to Serious Human Rights Abuses by the Government of Iran and Taking Certain Other Actions** (2010)
- The **Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010** (CISADA)
- **National Defense Authorisation Act for Fiscal Year 2012 (NDAA), Section 1245** (2012)
- **Pub. L. 112-158 – Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA)** (2012)
- **Iran Freedom and Counter-Proliferation Act of 2012 (IFCA)** (2012)
- **Executive Order 13574 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Sanctions Act of 1996** (2011) (Revoked in 2016)

- **Executive Order 13590 – Authorizing the Imposition of Certain Sanctions With Respect to the Provision of Goods, Services, Technology or Support for Iran's Energy and Petrochemical Sectors** (2011) (Revoked in 2016)
- **Executive Order 13599 – Blocking Property of the Government of Iran and Iranian Financial Institutions** (2012)
- **Executive Order 13606 – Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology** (2012) (GHRAVITY E.O.)
- **Executive Order 13608 – Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders with Respect to Iran and Syria** (2012)
- **Executive Order 13622 – Authorizing Additional Sanctions With Respect to Iran** (2012) (Revoked in 2016)
- **Executive Order 13628 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions With Respect to Iran** (2012) (Amended in 2016)
- **Executive Order 13645 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Freedom and Counter-Proliferation Act of 2012 and Additional Sanctions With Respect to Iran** (2013)
- **Executive Order 13716 – Revocation of Executive Orders 13574, 13590, 13622 and 13645 with Respect to Iran, Amendment of Executive Order 13628 With Respect to Iran and Provision of Implementation Authorities for Aspects of Certain Statutory Sanctions Outside the Scope of U.S. Commitments Under the Joint Comprehensive Plan of Action of July 14, 2015** (2016)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Iran:

- **UNSCR 1696 (2006)**
- **UNSCR 1737 (2006)**
- **UNSCR 1747 (2007)**
- **UNSCR 1803 (2008)**
- **UNSCR 1929 (2010)**

Following are the regulations that implement Iranian sanctions:

- **31 C.F.R. Part 535 – Iranian Assets Control Regulations** – Regulations that governed the 1979 seizure of US$12 billion in Iranian government bank deposits and securities held by overseas branches of U.S. banks. The asset freeze was later expanded to a full trade embargo, which

remained in effect until 1981. Part 535 has since been substantially modified in scope by subsequent laws and regulations.

- **31 C.F.R. Part 560 – Iranian Transactions and Sanctions Regulations (ITSR)** – General sanctions programs related to Iran administered by the Office of Foreign Assets Control (OFAC), along with unexpired provisions of Part 535.
- **31 C.F.R. Part 561 – Iranian Financial Sanctions Regulations (IFSR)** – Implementing regulations of Sections 104(c) and 104(d) of CISADA.
- **31 C.F.R. Part 562 – Iranian Human Rights Abuses Sanctions Regulations** – Implementing regulations of laws addressing human rights violations by Iran (e.g., ITRSHRA, Executive Order 13553).
- **31 C.F.R. Part 1060 – Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements** – Regulation implementing Section 104(e) of CISADA.

Additionally, the U.S. Department of the Treasury issued a notice of proposed rulemaking on November 28, 2011, designating Iran as a jurisdiction of primary money laundering concern pursuant to Section 311 – Special Measures.

Major provisions of CISADA, NDAA, ITRSHRA, IFCA and select executive orders are summarised below.

1005. What are the major U.S. government sanctions programs affecting Syria?

The U.S. government has imposed sanctions on the Syrian Arab Republic (Syria), including those mandated by the following statutes and executive orders, which are listed in chronological order:

- **United Nations Participation Act (UNPA), Section 5** (1945)
- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 13224 – Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism** (2001)
- **Executive Order 13315 – Blocking Property of the Former Iraqi Regime, Its Senior Officials and Their Family Members, and Taking Certain Other Actions** (2003)
- **Executive Order 13382 – Blocking Property of Weapons of Mass Destruction Proliferators and Their Supporters** (2005)
- **Executive Order 13338 – Blocking Property of Certain Persons and Prohibiting the Export of Certain Goods to Syria** (2004)
- **Executive Order 13399 – Blocking Property of Additional Persons in Connection With the National Emergency With Respect to Syria** (2006)
- **Executive Order 13441 – Blocking Property of Persons Undermining the Sovereignty of Lebanon or Its Democratic Processes and Institutions** (2007)

- **Executive Order 13460 – Blocking Property of Additional Persons in Connection With the National Emergency With Respect to Syria** (2008)
- **Executive Order 13338 – Blocking Property of Certain Persons and Prohibiting the Export of Certain Goods to Syria** (2004)
- **Syria Accountability Act and Lebanese Sovereignty Restoration Act (SAA) of 2004**
- **Executive Order 13572 – Blocking Property of Certain Persons With Respect to Human Rights Abuses in Syria** (2011)
- **Executive Order 13573 – Blocking Property of Senior Officials of The Government Of Syria** (2011)
- **Executive Order 13582 – Blocking Property of the Government of Syria and Prohibiting Certain Transactions With Respect to Syria** (2011)
- **Executive Order 13606 – Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology** (2012) (GHRAVITY E.O.)
- **Executive Order 13608 – Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria** (2012)
- **Iran Threat Reduction and Syria Human Rights Act of 2012** (ITRSHRA)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Syria:

- **UNSCR 1595 (2005)**
- **UNSCR 1636 (2005)**

Syrian sanctions are implemented under **31 C.F.R. Part 542 – Syrian Sanctions Regulations.**

Additionally, on March 9, 2006, the U.S. Department of the Treasury designated the Commercial Bank of Syria, including its subsidiary, Syrian Lebanese Commercial Bank, as financial institutions of primary money laundering concern pursuant to Section 311 – Special Measures of the USA PATRIOT Act.

1006. What are the primary objectives of OFAC Sanctions Programs affecting Iran and Syria?

The primary objectives of the U.S. government with respect to Iranian and Syrian sanctions are to restrict and eliminate the following:

- Support of international terrorism;
- Acquisition of weapons of mass destruction (WMDs) (e.g., nuclear weapons);
- Human rights violations against the people of Iran and Syria; and
- Evasion of U.S. sanctions.

1007. Where can one find a list of designated entities under Iranian and Syrian sanctions?

Designations are maintained in the appendices of applicable Iranian regulations, on lists administered by OFAC, or both. Examples of Iranian and Syrian sanction designations and lists include, but are not limited to, the following:

- Specially Designated Nationals and Blocked Persons List (SDN List):
  - Persons designated under Executive Order 13606 (GHRAVITY E.O.) appear on the SDN List bearing the **Human Rights Information Technology [HRIT-IR] and [HRIT-SY]** program tags.
  - Persons designated under Executive Order 13599 appear on the SDN List bearing the **[IRAN]** program tag.
  - **Iran's Islamic Revolutionary Guard Corps (IRGC)**, its agents and affiliates designated under Section 104(d) of CISADA, IEEPA and IFSR appear on the SDN List, bearing the **[IRGC]** program tag.
  - Persons designated for evading Iranian and Syrian sanctions under **Foreign Sanctions Evaders Executive Order 13608** appear on the SDN List, bearing the **[FSE-IR], [FSE-SY]** or **[FSE-WMD]** program tag.
  - Persons designated under **Executive Order 13553** appear on the SDN List, bearing the **[IRAN-HR]** program tag.
  - Persons designated under **Executive Order 13628** appear on the SDN List, bearing the **[IRAN-TRA]** program tag.
  - Persons designated under **Executive Order 13645** appear on the SDN List, bearing the **[EO13645]** program tag.
  - Persons designated under **Executive Order 13622** appear on the SDN List, bearing the **[EO 13622]** program tag.
  - Persons designated under **Executive Order 13574** pursuant to the Iran Sanctions Act (ISA) appear on the SDN List, bearing the **[ISA]** program tag and non-SDNs bearing the program tag [NS-ISA].
  - Persons designated under the **Iran Freedom and Counter-Proliferation Act of 2012 (IFCA)** appear on the SDN List, bearing the **[IFCA]** program tag.
  - Persons designated under **Executive Orders 13399 and 13460** pursuant to Syrian sanctions appear on the SDN List, bearing the **[SYRIA]** program tag.
  - **Iranian financial institutions** designated in connection with Iran's WMDs or terrorism activities appear on the SDN List, bearing the **[IFSR]** program tag.
- **List of Foreign Financial Institutions Subject to Part 561 (Part 561 List)** – Foreign financial institutions that are deemed to have violated Iranian Financial Sanctions Regulations (IFSR) under CISADA and NDAA.

1008. What agency is responsible for administering Iranian and Syrian sanctions and regulations?

The Department of the Treasury (OFAC) has primary responsibility for implementing the economic sanctions contained in the ITSR.

The State Department is the agency primarily responsible for implementing the provisions of CISADA and ITRSHRA, including the designation of entities in the energy, shipping and transportation sectors.

The Bureau of Industry and Security (BIS) within the Department of Commerce, administers regulations pertaining to the export of goods and technology to Iran under the Export Administration Regulations, which are authorised by IEEPA.

OFAC has issued a few general licenses authorising certain categories of transactions and may issue specific licenses on a case-by-case basis. For further guidance, please refer to the OFAC Licensing section.

1009. Have any entities been penalised for violations of Iranian and Syrian sanctions?

Yes. Since 2010, several of the world's largest banks have been penalised by OFAC for processing US dollar transactions through U.S. financial institutions related to Iran and other sanction programs, including, but not limited to the following:

- BNP Paribas S.A.: A US$8.9 billion settlement in June 2014 for violations of Cuban, Iranian and Sudanese sanction programs.
- Clearstream Banking S.A.: A US$152 million settlement in January 2014 for violations of Iranian sanctions program.
- Royal Bank of Scotland PLC (RBS): A US$33 million settlement in December 2013 for violations of Iranian and Sudanese sanctions programs.
- HSBC Holdings PLC: A US$375 million settlement in December 2012 for violations of Cuban, Iranian, Libyan, Sudanese and Burmese sanctions programs.
- Standard Chartered Bank (SCB): A US$132 million settlement in December 2012 for violations of Burmese, Iranian, Libyan and Sudanese sanctions programs.
- ING Bank N.V.: A US$619 million settlement in June 2012 for violations of Cuban and Iranian sanctions programs.

Other aspects of the Iranian and Syrian sanctions have also resulted in enforcement actions:

In 2011, the U.S. Department of State sanctioned a number of companies for violations under the Iran Sanctions Act (ISA) of 1996, as amended by the CISADA in 2010, for activities in support of Iran's energy sector, specifically for refined-petroleum-related activities including, but not limited to, the following:

- Petrochemical Commercial Company International (PCCI) (Jersey/Iran);
- Royal Oyster Group (UAE);

- Speedy Ship aka Sepahan Oil Company (UAE/Iran);
- Tanker Pacific (Singapore);
- Ofer Brothers Group (Israel);
- Associated Shipbroking (Monaco); and
- Petróleos de Venezuela (PDVSA) (Venezuela).

On July 31, 2012, the U.S. Department of Treasury imposed sanctions under CISADA against the Bank of Kunlun in China and the Elaf Islamic Bank in Iraq. Specifically, these two banks violated Section 561.201 of IFSR, which implemented Section 104 of CISADA, which prohibits or imposes strict conditions with respect to correspondent accounts or payable-through accounts of certain foreign financial institutions that engage in activities that support the efforts of the government of Iran or the IRGC and its agents or affiliates. Both banks and their aliases were added to the List of Foreign Financial Institutions Subject to Part 561 (Part 561 List).

The Elaf Islamic Bank in Iraq has since been removed from the Part 561 List after reducing its financial exposure to sanctioned Iranian financial institutions. The Part 561 list currently includes one entity, Bank of Kunlun, also known as Karamy City Commercial Bank and Karamy Urban Credit Cooperatives.

Additionally, multiple entities from Cyprus, Georgia, Liechtenstein, Switzerland, Turkey, Ukraine and the United Arab Emirates have been added to the Foreign Sanctions Evaders List (FSE List) for evading or attempting to evade Iranian and Syrian sanctions.

1010. Can individuals and entities still be designated under the Iranian Sanctions Program under the modified program pursuant to the Joint Comprehensive Plan of Action (JCPOA)?

Yes. In February 2017, OFAC added multiple individual and entities to the Iranian Sanctions Program for activities related to Iran's ballistic missile program, which many reported as consistent with the JCPOA. For further guidance on the JCPOA, please refer to Other Executive Orders and Actions.

Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 and the Iran Threat Reduction and Syria Human Rights Act of 2012

1011. What additional sanctions did the United States impose on Iran due to the passage of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA) and the Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA)?

CISADA and ITRSHRA imposed new economic penalties designed to put additional pressure on Iran to end its nuclear weapons program. The law includes:

- Expansion of the scope of persons and the type of activities that may be subject to sanctions to include:
    - Investment (over certain threshold amounts) in Iran's development of petroleum resources;

  - Sales of goods, services or technology (over certain threshold amounts) that support Iran's ability to produce refined petroleum;
  - Exporting Iran's refined petroleum products (over certain threshold amounts);
  - Participation in joint ventures with the government of Iran to develop petroleum resources outside Iran;
  - Insuring vessels used to transport Iranian crude oil; and
  - Participation in joint ventures with the government of Iran related to uranium mining, production or transportation.
- Expansion of the types of sanctions that may be imposed to include:
  - Denial of foreign exchange transactions subject to U.S. jurisdiction that involve sanctioned entities;
  - Prohibition on transfers of credit or payments between, by, through or to financial institutions subject to U.S. jurisdiction and that involve any interest of sanctioned entities;
  - Prohibition on transactions (e.g., acquiring, holding, withholding, using, transferring, withdrawing, transporting, importing or exporting) or exercising rights, powers, and so on, with respect to property subject to U.S. jurisdiction in which a sanctioned entity has an interest;
  - Ban on investment in equity or debt of a sanctioned person;
  - Exclusion of corporate officers from the United States; and
  - Sanctions on principal executive officers of sanctioned companies.
- New restrictions for financial institutions barring U.S. banks from engaging in financial transactions with foreign banks doing business in Iran or facilitating Iran's nuclear program or support for terrorism;
- Mandatory investigations into possible sanctionable conduct upon the receipt of "credible evidence," subject to certain waiver provisions;
- Requiring new regulations to prohibit or impose strict conditions on the holding of a correspondent or payable-through account in the United States by foreign financial institutions engaged in specified activities, such as activities that facilitate the efforts of the government of Iran to acquire or develop WMDs or delivery for such systems; to provide support for organisations designated as foreign terrorist organisations (FTOs) or support for acts of international terrorism; or for facilitating efforts by Iranian financial institutions to carry out such activities;
- Requirement for the U.S. Department of the Treasury to promulgate regulations to prohibit any entity owned or controlled by a U.S. financial institution from knowingly transacting with or benefitting a foreign financial institution or covered individual;

- Authorisation/Safe Harbor for state and local governments to more easily divest themselves of or prohibit any investments of public funds in companies that engage in certain business with Iran;
- Certification by U.S. government contractors that neither they, nor any entity they own or control, engage in any activity subject to Iranian sanctions; and
- Codification of long-standing U.S. executive orders prohibiting U.S. persons, wherever located, from doing business with the government of Iran and any entities it owns or controls.

1012. Since most commerce between the United States and Iran is already prohibited under existing OFAC Sanctions Programs, what more is really gained by CISADA and ITRSHRA?

By targeting foreign firms that do business with Iran and restricting or denying them access, directly or indirectly, to the U.S. financial system, CISADA and ITRSHRA seek to bring pressure on these foreign firms to cease their business operations with Iran.

1013. Are CISADA and ITRSHRA unilateral actions on the part of the United States?

Yes, the specific sanctions in these statutes that authorise the imposition of sanctions on foreign persons are unique to the United States. However, U.S. policy toward Iran is broadly aligned with other countries as reflected in United Nations Security Council Resolutions. Australia, Canada and the European Union have all adopted their own sanctions on Iran, which include prohibiting exports of certain goods and technology, prohibiting transactions, blocking assets of Iranian financial institutions and other designated entities and prohibiting the transport of Iranian oil.

1014. How will CISADA and ITRSHRA affect foreign companies?

CISADA requires that sanctions be imposed on foreign persons who:

- Knowingly invest more than US$20 million (including by increments of at least US$5 million within 12 months) in Iran's development of petroleum resources;
- Sell, lease or provide goods, services, technology, information or support worth at least US$1 million (or, during a 12-month period, have an aggregate value of US$5 million or more) that could directly and significantly facilitate the maintenance or expansion of Iran's domestic production of refined petroleum products;
- Sell or provide Iran with refined petroleum products with a fair market value of US$1 million (or US$5 million during a 12-month period); or
- Provide goods or services that could directly and significantly contribute to the enhancement of Iran's ability to import refined petroleum products, including insuring, reinsuring, financing or brokering such transactions with a fair market value of US$1 million (or, during a 12-month period, have an aggregate value of US$5 million or more).

CISADA prescribes additional sanctions on persons who aid Iran's development of nuclear capabilities and on U.S. financial institutions that engage in financial transactions with foreign banks doing

business with Iran's Islamic Revolutionary Guard Corps (IRGC) or sanctioned Iranian banks, or facilitate Iran's illicit nuclear program or its support for terrorism.

Further, ITRSHRA requires that sanctions be imposed on persons who:

- Knowingly participate in a joint venture with respect to the development of petroleum resources outside Iran if the government of Iran is a substantial partner or investor or Iran could receive, through a direct operational role in the joint venture, technological knowledge that could directly and significantly contribute to the enhancement of Iran's ability to develop petroleum resources in Iran;
- Knowingly sell, lease or provide Iranian goods, services or technology with a fair market value of US$1 million (or US$5 million during a 12-month period) that support, or could directly and significantly contribute to, the maintenance or expansion of Iran's domestic production of petrochemical products;
- Own, operate, control or insure a vessel that was used to transport crude oil from Iran or such a person who knows that the vessel is being operated to conceal the transport of Iranian origin crude oil or refined petroleum or to conceal the ownership, operation or control of the vessel by the government of Iran, the National Iranian Oil Corporation (NIOC), the Islamic Republic of Iran Shipping Line (IRISL) or any other designated Iranian entity;
- Export, transfer or facilitate the transshipment by others of goods, services, technology or other items that would contribute materially to Iran's ability to acquire or develop chemical, biological or nuclear weapons; or
- Participate in a joint venture with the government of Iran or any Iranian entity involving any activity relating to the mining, production or transportation of uranium.

1015. How does CISADA define "person"?

CISADA defines "person" as a natural person, business enterprise, or government entity operating as a business enterprise, financial institution, insurer, underwriter, guarantor or any other business organisation. This definition also includes parent companies and affiliates of sanctioned persons.

1016. CISADA requires the imposition of sanctions when a person knowingly invests or takes certain other actions. What does "knowingly" mean in this context?

"Knowingly" in this context means actual knowledge or constructive knowledge (i.e., the person should have known).

1017. What sanctions will be imposed on foreign companies that violate the CISADA and ITRSHRA sanctions?

CISADA provided that nine possible sanctions may be imposed for violation of the sanctions:

- Prohibition within U.S. jurisdiction of foreign-exchange transactions in which a sanctioned person has any interest;

- Prohibition within U.S. jurisdiction of payments and other transactions that involve any interest of a sanctioned person;
- The blocking of the property (freezing of the assets) within the U.S. jurisdiction of a sanctioned person;
- Denial of U.S. Export-Import Bank loans or credit facilities for U.S. exports to the sanctioned person;
- Denial of licenses for the U.S. export of military or militarily useful technology;
- Denial of U.S. bank loans exceeding US$10 million in one year;
- If the sanctioned person is a financial institution, a prohibition on its service as a primary dealer in U.S. government bonds and/or a prohibition on its serving as a repository for U.S. government funds;
- Prohibition on U.S. government procurement from the sanctioned person; and
- Restriction on imports into the United States from the sanctioned person.

In addition, ITRSHRA added three new sanctions to the list:

- Ban on investment in equity or debt of a sanctioned person;
- Exclusion of corporate officers from the United States; and
- Sanctions on principal executive officers of sanctioned companies.

CISADA required that at least three of the above sanctions be imposed when there is a finding that a person has violated provisions set forth in CISADA. ITRSHRA strengthened the provision to require the imposition of at least five of the above sanctions. The U.S. president, however, does have the authority to waive the imposition of sanctions in certain circumstances.

1018. What sanctions will be imposed on persons who violate the provisions of CISADA related to the transfer of nuclear technology?

CISADA prohibits the issuance of export licenses to the country having primary jurisdiction over the person engaging in the sanctionable activity. The U.S. president may waive the sanctions with a certification to Congress that the relevant country did not know of the sanctionable activity or is taking steps to prevent it and to penalise the offender.

1019. Who is targeted within Syria with the passage of the ITRSHRA?

The ITRSHRA imposed sanctions against Syria with respect to persons who:

- Are responsible for or complicit in human rights abuses committed against citizens of Syria or their family members;
- Transfer goods or technologies to Syria that are likely to be used to commit human rights abuses; and

- Engage in censorship or other forms of repression in Syria.

1020. How did the Iran Freedom and Counter-Proliferation Act of 2012 (IFCA) amend CISADA?

Section 1249 of IFCA amended CISADA by imposing sanctions on persons who engage in diversion of humanitarian aid (e.g., food, agricultural commodities, medicine, medical devices). Sanctioned activities include both diversion and misappropriation of proceeds from the sale or resale of such goods.

Impact on Financial Institutions

1021. What is the impact of CISADA on U.S. financial institutions?

CISADA requires the U.S. Department of the Treasury to issue regulations restricting or prohibiting the opening or maintenance of correspondent or payable-through accounts by a foreign financial institution that:

- Facilitates the efforts of the government of Iran, the Islamic Revolutionary Guard Corps (IRGC) or any of its agents or affiliates to acquire weapons of mass destruction or provide support to foreign terrorist organisations;
- Facilitates the activities of persons subject to financial sanctions under the U.N. Security Council's Iranian resolution;
- Engages in money laundering related to the above activities; or
- Facilitates significant transaction(s) or provides financial services to the IRGC or any of its agents or affiliates or to financial institutions subject to U.S. blocking requirements.

CISADA also requires U.S. financial institutions that maintain correspondent or payable-through accounts in the United States for a foreign financial institution to do one or more of the following:

- Audit activities of the foreign financial institutions for which such accounts are made for indications that they are engaging in any prohibited activity;
- Report any such activity identified to the U.S. Department of the Treasury;
- Establish due diligence procedures, policies and controls that are reasonably designed to detect whether foreign financial institutions knowingly engage in prohibited activities; and
- Certify, to the best of their knowledge, that the foreign financial institutions with which they are maintaining accounts are not engaging in such activities.

For additional guidance on correspondent banking customers and payable-through accounts, please refer to sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Customers, Correspondent Banking and Payable-Through Accounts.

1022. How does CISADA define "financial institution" and "U.S. financial institution"?

The definition of "financial institution" is broad and includes any entity engaged in the business of accepting deposits; making, granting, transferring, holding or brokering loans or credits; purchasing or selling foreign exchange, securities, commodity futures or options; or procuring purchasers and sellers thereof, as principal or agent. It includes, but is not limited to, the following:

- Depository institutions
- Banks
- Savings banks
- Money services businesses (MSB)
- Trust companies
- Securities brokers and dealers
- Commodity futures and options brokers and dealers
- Forward contract and foreign exchange merchants
- Securities and commodities exchanges
- Clearing corporations
- Investment companies
- Employee benefit plans
- Dealers in precious metals, stones or jewels (as amended by Executive Order 13645)
- Holding companies, affiliates or subsidiaries of any of the foregoing

For purposes of the definition of "U.S. financial institution," the term also includes those branches, offices and agencies of a foreign financial institution located in the United States, but not such institution's foreign branches, offices or agencies.

1023. How does CISADA define "foreign financial institution"?

CISADA defines "foreign financial institution" to include foreign depository institutions, banks, savings banks, money service businesses, trust companies, securities brokers and dealers, commodities exchanges, clearing corporations, investment companies, employee benefit plans and holding companies, affiliates or subsidiaries of any of these entities.

1024. Does CISADA apply to persons or entities who own, directly or indirectly, the aforementioned financial institutions?

Yes, to the extent that a person whose property is blocked owns, directly or indirectly, 50 percent or greater in aggregate interest in the property of another entity. The property and interests in the property of that entity will also be blocked, regardless of whether that entity is itself included in Appendix A to Part 560.

1025. What will determine whether financial transactions are "significant"?

A number of factors will influence the determination of whether a transaction is significant, including, but not limited to, the following:

- The size of the transaction(s)
- The number and frequency of the transaction(s)
- The type and complexity of the transaction(s)
- The extent of management involvement in the transaction(s)
- The proximity of the parties to the transaction(s) with a blocked person appearing on the Specially Designated Nationals List and Blocked Persons List (SDN List)
- The effect of the transaction(s) on Iran's ability to obtain weapons of mass destruction or commit acts of international terrorism
- Any effort to conceal the transaction(s)

1026. How does CISADA treat pre-existing financial contracts?

There is no general exemption for payments arising out of pre-existing contracts. Whether such payments are "significant" will be examined on a case-by-case basis.

1027. How does CISADA define "financial services"?

As provided in the Iranian Financial Sanctions Regulations, 31 C.F.R. Part 561, CISADA' s definition of "financial services" includes loans, transfers, accounts, insurance, investments, securities, guarantees, foreign exchange, letters of credit and commodity futures or options.

1028. Has the U.S. Department of the Treasury issued implementing regulations related to the prohibitions on U.S. financial institutions related to CISADA and ITRSHRA?

The U.S. Department of the Treasury has issued the following implementing regulations related to CISADA and TRA:

- **Iranian Financial Sanctions Regulations (31 C.F.R. Part 561) (IFSR)**: On August 16, 2010, the U.S. Department of the Treasury issued regulations to implement Sections 104(c) and 104(d) of CISADA, dealing specifically with the identification of foreign financial institutions for which U.S. financial institutions would be restricted/prohibited from opening or maintaining accounts. The regulations were effective when issued. On March 15, 2013, updates to IFSRs were published to implement Sections 503 and 504 of the ITRSHRA and certain provisions of Executive Order 13622.
- **Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements (31 C.F.R. Part 1060)**: On April 27, 2011, the U.S. Department of the Treasury proposed regulations to implement Section 104(e) of CISADA which would require that U.S. financial institutions report certain information to FinCEN on specified foreign banks for which

the U.S. financial institution maintains a correspondent account. The regulations became effective October 5, 2011.

- **Iranian Transactions and Sanctions Regulations (31 C.F.R. Part 560) (ITSR)**: On October 22, 2012, the U.S. Department of the Treasury issued regulations to incorporate CISADA provisions as well as the provisions of Executive Order 13599 (blocking the property of the government of Iran and Iranian financial institutions) and certain provisions of Section 1245 of the National Defense Authorisation Act for Fiscal Year 2012. These final regulations replace the Iranian Transactions Regulations in effect prior to that date.

Other CISADA requirements are expected to be subject to additional rulemaking.

1029. What are the major provisions of Iranian Financial Sanctions Regulations implementing Sections 104(c) and 104(d) of CISADA?

Iranian Financial Sanctions Regulations (IFSRs) provide that the U.S. Department of the Treasury may prohibit or impose strict conditions on the opening or maintenance in the United States of a correspondent account or a payable-through account for a foreign financial institution that the U.S. Department of the Treasury finds knowingly (or should have known):

- Facilitated the efforts of the government of Iran, including Iran's Islamic Revolutionary Guard Corps (IRGC) or any of its agents or affiliates, to acquire or develop weapons of mass destruction or delivery systems for such weapons or to provide support for organisations deemed to be foreign terrorist organisations;
- Facilitated the activities of a person or entity subject to U.N. financial sanctions related to Iran;
- Engaged in money laundering to carry out such activity;
- Facilitated efforts by the Central Bank of Iran (CBI) or any other Iranian financial institution to carry out such activity; or
- Facilitated a significant transaction(s) or provided significant financial services for the IRGC or any of its agents or affiliates whose property is blocked under U.S. Iranian sanctions.

The U.S. Department of the Treasury may force the closing of such correspondent account or payable-through account (or other banking relationship) or impose certain conditions, such as:

- Prohibiting any provision of trade finance through the correspondent account or payable-through account;
- Restricting the transactions that may be processed through such accounts to certain types (e.g., prohibit all transactions except personal remittances);
- Placing monetary limits on the transactions that may be processed; or
- Requiring pre-approval from the U.S. financial institution for all transactions to be processed through such account.

Any person owned or controlled by a U.S. financial institution is prohibited from knowingly engaging in any transaction with or benefiting the IRGC or any of its agents or affiliates whose property is blocked.

U.S. financial institutions may not open or maintain correspondent or payable-through accounts for those identified institutions and may only conduct such transactions as are necessary to close an account or transfer funds to the account of a foreign financial institution outside of the United States.

The regulations also make clear that a U.S. financial institution is not authorised to unblock or otherwise deal in property blocked under any other part in the process of closing a correspondent or payable-through account for such a foreign financial institution. Findings, orders and regulations will be published in Appendix A to Part 560 of IFSR.

1030. Where can a list of Iranian-linked financial institutions be found?

The ITSR issued on October 22, 2012, deleted Appendix A to Part 560, which listed financial institutions determined to be owned or controlled by the government of Iran.

The persons who were listed in Appendix A are now listed on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) with the [IRAN] program tag and their property and interests in property are blocked pursuant to Executive Order 13599 and ITSR Section 560.211. On September 7, 2010, the U.S. Department of the Treasury added the first Iranian-linked financial institution, Europäisch-Iranische Handelsbank (EIH), to the SDN List pursuant to ITSR because of its alleged dealings with sanctioned Iranian banks in furtherance of Iran's activities related to the proliferation of weapons of mass destruction (WMDs). Since then, many more designees have been added.

U.S. financial institutions are encouraged to monitor the U.S. Department of the Treasury's website for information on additions to Appendix A.

1031. Is the Islamic Revolutionary Guard Corps (IRGC), its agents and affiliates included on the SDN List?

Yes. The IRGC, its agents and affiliates appear on the SDN List bearing the [IRGC] tag.

1032. Where can a list of foreign financial institutions that have violated IFSR be found?

The list of Foreign Financial Institutions Subject to Part 561 (Part 561 List) includes entities that have violated Iranian Financial Sanctions Regulations (IFSRs). U.S. financial institutions are prohibited from opening or maintaining a correspondent or payable-through account for any foreign financial institutions on the Part 561 List. The Part 561 List is available on OFAC's website at http://www.treasury.gov/ofac/downloads/561list.pdf.

1033. Are entities on the Part 561 List included on the SDN List?

No. Entities on the Part 561 List are not included on the SDN List.

1034. Have any foreign financial institutions violated IFSR?

Yes. On July 31, 2012, the U.S. Department of Treasury imposed sanctions under CISADA against the Bank of Kunlun Co. Ltd. in China and the Elaf Islamic Bank in Iraq. Specifically, these two banks were deemed to have violated Section 561.201 of IFSR, the implementing regulation of CISADA, which prohibits or imposes strict conditions with respect to correspondent accounts or payable-through accounts of certain foreign financial institutions that engage in activities that support the efforts of the government of Iran or the IRGC and its agents or affiliates.

As of July 31, 2012, the following entities were included on the Part 561 List:

- Bank of Kunlun Co. Ltd.
- Elaf Islamic Bank
- Karamay City Commercial Bank Co. Ltd.
- Karamay Urban Credit Cooperatives

Since the removal of the Elaf Islamic Bank in Iraq in 2013, the Part 561 List currently includes one entity, Bank of Kunlun, also known as Karamy City Commercial Bank and Karamy Urban Credit Cooperatives.

1035. What are the major provisions of the U.S. Department of the Treasury's Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements (31 C.F.R. Part 1060) implementing Section 104(e) of CISADA?

Comprehensive Iran Sanctions, Accountability, and Divestment Reporting Requirements (31 C.F.R. Part 1060) requires U.S. financial institutions, including U.S. branches and agencies of foreign banks, to report, upon request from FinCEN, certain information about specified foreign banks for which the U.S. bank maintains a correspondent account. This information includes:

- Whether the foreign bank maintains a correspondent account for an Iranian-linked financial institution designated under the International Emergency Economic Powers Act (IEEPA);
- Whether the foreign bank has processed one or more transfers of funds within the preceding 90 calendar days related to an Iranian-linked financial institution designated under IEEPA, other than through a correspondent account; or
- Whether the foreign bank has processed one or more transfers of funds within the preceding 90 calendar days related to Iran's Islamic Revolutionary Guard Corps (IRGC) or any of its agents or affiliates designated under IEEPA.

In addition, a U.S. bank would have to request notification of the above from any foreign bank specified by FinCEN if an account is established within one year of the response to the request above for any Iranian-linked financial institution designated under IEEPA. The U.S. bank would be required to request notification within 30 days of establishing the account and would be obligated to report this information to FinCEN within 10 days of receipt of the notification. FinCEN may also request, in certain instances, that a U.S. bank confirm that it does not maintain an account for a specified foreign

bank, with a response due to FinCEN within 45 days of receipt of FinCEN's request for this information.

The regulation adds additional reporting requirements – Know Your Customer's Customers – for U.S. banks that are based on a newly imposed "duty to inquire" about the identification of a correspondent bank's customers and the originators, beneficiaries and purposes of transactions handled by a correspondent bank, regardless of whether there is a connection to the U.S. bank through the use of services or processing of transactions.

1036. Are U.S. financial institutions required to review and independently verify responses from their foreign bank customers prior to submitting to the U.S. Department of the Treasury?

No. U.S. financial institutions are not required to review responses prior to submission to the U.S. Department of the Treasury. U.S. financial institutions are only required to respond to a written inquiry within 45 days of receipt, even if the response is a "non-response." However, if through the normal course of monitoring a U.S. financial institution detects activity inconsistent with that provided by the foreign bank, it is obligated to submit this information to the U.S. Department of the Treasury.

1037. What are the protocols for issuing Section 104(e) requests prior to distribution to financial institutions?

All Section 104(e) requests will be written and sent directly to banks that FinCEN, based on all available information, believes maintain correspondent accounts for the specified foreign bank(s).

1038. Is there a minimum threshold for reporting transfers of funds processed within the preceding 90 calendar days related to an Iranian-linked financial institution designated under IEEPA?

No. The regulations do not establish a minimum threshold for a foreign bank to report on transfers of funds processed within the preceding 90 calendar days related to an Iranian-linked financial institution designated under IEEPA.

1039. What guidance has the U.S. Department of the Treasury provided with regard to how a U.S. financial institution should query its foreign bank customers upon receipt of a written request under Section 104(e)?

FinCEN has created a model certification form that can be used by a U.S. financial institution to query their foreign bank customers. The model certification outlines the following:

- The purpose of the request;
- Information that a foreign bank is requested to report to the U.S. financial institution; and
- Links to lists of relevant designated entities and individuals on which a foreign bank is requested to report.

1040. Are all types of U.S. financial institutions required to comply with Section 104(e)?

No. Section 104(e) applies to domestic "banks," including commercial banks or trust companies, private banks, savings and loan associations, national banks, thrift institutions, credit unions and U.S. branches and agencies of foreign banks.

1041. Are U.S. financial institutions required to take any action, such as filing a Suspicious Activity Report (SAR), upon receipt of a written request under Section 104(e) regarding one of its foreign correspondent banking relationships?

U.S. financial institutions are not required to take any specific actions based on the information received in response to queries of the specified foreign banks, but the U.S. Department of the Treasury may, under CISADA, restrict or prohibit dealings with select foreign banks.

A financial institution should not automatically file a SAR upon receipt of a Notice from FinCEN. The decision to file a SAR should be based on the institution's own investigation into the activity of the party(ies) that/who is/are the subject of the Notice.

1042. Can U.S. financial institutions share information within a Section 104(e) request internally or externally?

A U.S. financial institution's ability to share information within a Section 104(e) request will be determined by the requirement for confidentiality explicitly stated in each request by FinCEN.

1043. Where directed by U.S. Department of the Treasury, what is the time frame for complying with an order to close a correspondent or payable-through account?

Where the U.S. Department of the Treasury orders such a correspondent or payable-through account to be closed, the U.S. financial institution holding such an account may process limited transactions that are needed to close the account within 10 days of such designation.

1044. What steps do U.S. financial institutions need to take to ensure compliance with the requirements of CISADA and ITRSHRA?

Given the significant consequences of noncompliance, it is recommended that U.S. financial institutions, even prior to the issuance of additional regulations, review their portfolios of correspondent and payable-through accounts for any potential problem foreign financial institutions and begin developing due diligence and monitoring procedures designed to help ensure ongoing compliance.

1045. When does the time period for record retention begin with written requests under Section 104(e)?

The record retention period begins on the date the Section 104(e) request from FinCEN is issued. Consistent with other AML/CFT laws and regulations, supporting documentation must be retained for five years.

1046. What supporting documentation should be retained for recordkeeping purposes?

FinCEN advised that all correspondence between the U.S. financial institution and FinCEN, or between the U.S. financial institution and the foreign bank, regarding a request for information under Section 104(e) be retained for recordkeeping purposes.

1047. How does ITRSHRA affect foreign subsidiaries of U.S. parent companies?

Section 218 of ITRSHRA prohibits an entity owned or controlled by a U.S. person (or U.S. entity) and established or maintained outside the U.S. from knowingly engaging in any transaction directly or indirectly with the government of Iran or any person subject to the jurisdiction of the government of Iran that would be prohibited by the Iranian Transactions and Sanctions Regulations if such transaction were engaged in by the U.S. parent company. The prohibition is enforceable against the U.S. parent company. Entities include "partnerships, associations, trusts, joint ventures, corporations and other organisations." The term "own or control" with respect to the entity means:

- To hold more than 50 percent of the equity interest by vote or value in the entity;
- To hold a majority of seats on the board of directors of the entity; or
- To otherwise control the actions, policies or personnel decisions of the entity.

Attempts to evade or avoid ITRSHRA are also prohibited.

1048. Is there a Safe Harbor provision for U.S. parent companies to avoid penalties for violations committed by their foreign subsidiaries?

Yes. Section 218 of ITRSHRA provides that civil penalties will not apply where the U.S. parent company divested or terminated business with the foreign subsidiary by February 6, 2013.

1049. How does ITRSHRA amend the reporting obligations of publicly traded companies?

Section 219 amends the Securities Exchange Act of 1934 to require publicly traded companies engaging in certain types of Iran-related business to publicly disclose such business to the U.S. Securities and Exchange Commission (SEC) through their mandatory annual or quarterly reports. This requirement is effective for reports required by the SEC after February 6, 2013. Covered companies must disclose whether the company or any of their affiliates knowingly engaged in certain activities described in the Iran Sanctions Act or CISADA or knowingly conducted any transaction or dealing with persons whose property has been blocked pursuant to Executive Orders 13224 or 13382 or with the government of Iran or any Iranian government owned or controlled entity without specific OFAC authorisation.

1050. What determinations were made about the National Iranian Oil Company (NIOC) and the National Iranian Tanker Company (NITC) pursuant to Section 312 of ITRSHRA?

Section 312 of ITRSHRA required the Secretary of the Treasury to determine whether NIOC or NITC were agents or affiliates of Iran's Islamic Revolutionary Guard Corps (IRGC). On September 24, 2012, the U.S. Department of the Treasury informed Congress that it had determined that NIOC and NITC were agents or affiliates of the IRGC. Although NIOC was already subject to previous sanctions, the determination can expose entities engaging in prohibited activities with NIOC to CISADA sanctions.

1051. What provisions of ITRSHRA are implemented by Executive Order 13628?

On October 9, 2012, the U.S. President issued Executive Order 13628 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions With Respect to Iran. Specifically, E.O. 13628 implemented the following provisions of TRA:

- Section 204: Expansion of sanctions available under the Iran Sanctions Act of 1996 (ISA);
- Section 218: Liability of parent companies for violations of sanctions by foreign subsidiaries;
- Section 402: Imposition of sanctions with respect to the transfer of goods or technologies to Iran that are likely to be used to commit human rights abuses; and
- Section 403: Imposition of sanctions with respect to persons who engage in censorship or other related activities against citizens of Iran.

E.O. 13628 also addresses several other issues, including providing penalties to be imposed on persons who improve Iranian petroleum refinement capacities, sell refined petroleum products to Iran, or provide certain enhancements to Iran's ability to import petroleum products where the value of the activity is over specified thresholds.

1052. What penalties may be imposed on a U.S. financial institution for violations of CISADA?

U.S. financial institutions that knowingly violate CISADA related to the opening and maintenance of correspondent and payable-through accounts may be subject to a civil and criminal penalties and 20 years in prison for individuals violating the sanctions. Violations of the due diligence, monitoring and reporting requirements of CISADA could also subject the financial institution to penalties prescribed by the USA PATRIOT Act.

National Defense Authorisation Act

1053. What is the National Defense Authorisation Act (NDAA)?

The NDAA is a federal law authorising appropriations for the U.S. Department of Defense (DOD), including military activities, military construction and defence activities of the Department of Energy (DOE). The NDAA is reauthorised each year.

The following section summarises key elements of the NDAA reauthorised in 2012, 2013 and 2014.

NDAA for Fiscal Year 2012

1054. What additional sanctions did the United States impose on Iran due to the passage of the NDAA?

Section 1245 of the Fiscal Year 2012 NDAA imposes the following sanctions with respect to Iran:

- Designation of the financial sector of Iran as a primary money laundering concern under Section 311 – Special Measures, including the Central Bank of Iran (CBI);

- Blocking and prohibiting all transactions in all property and interests in property of Iranian-linked financial institutions, including the CBI, if such property and interest is in the United States, comes within the United States, or comes within the possession or control of a U.S. person;
- Imposition of sanctions with respect to Iranian-linked financial institutions, including the CBI, that prohibits or imposes strict conditions on the opening and maintaining of a correspondent account or payable-through account for entities designated by the United States who knowingly conducted or facilitated any significant financial transaction with Iranian-linked financial institutions, including the CBI.

1055. What is the goal of Section 1245 of the NDAA?

The goal of Section 1245 of the NDAA is to reduce Iranian oil revenues and discourage transactions with the CBI by imposing sanctions on foreign financial institutions that knowingly conduct or facilitate certain significant financial transactions with the CBI.

1056. How are "petroleum products" defined for the purposes of Section 1245 of the NDAA?

The U.S. Energy Information Administration's (EIA) standard definition of "petroleum products" includes "unfinished oils, liquefied petroleum gases, pentanes plus, aviation gasoline, motor gasoline, naphtha-type jet fuel, kerosene-type jet fuel, kerosene, distillate fuel oil, residual fuel oil, petrochemical feedstock, special naphthas, lubricants, waxes, petroleum coke, asphalt, road oil, still gas and miscellaneous products obtained from the processing of crude oil (including lease condensate), natural gas and other hydrocarbon compounds."

The EIA's definition of petroleum products does not include nonpetroleum fuels, which include, but are not limited to, the following:

- Natural gas
- Liquefied natural gas
- Biofuels
- Methanol

1057. What activities can trigger sanctions on a foreign financial institution under the NDAA?

Sanctions may be imposed on financial institutions that knowingly conduct or facilitate significant financial transactions with the CBI or designated Iranian financial institutions, except for transactions involving the sale of food, medicine and medical devices. The U.S. president may also impose sanctions on the CBI. Further, foreign financial institutions can face sanctions under the NDAA if they knowingly conduct or facilitate significant financial transactions for the purchase of Iranian petroleum or petroleum products with a U.S.-designated Iranian financial institution or the CBI.

1058. How does the NDAA define the terms "significant" and "knowingly"?

The U.S. Department of the Treasury anticipates modelling the definition of "significant" for NDAA purposes on the IFSR. The IFSR, which implements Section 104 of CISADA, identifies factors to be

used in determining what is significant (as it relates to transactions) in 31 C.F.R. Section 561.404, which allows the Secretary of the Treasury to consider the totality of the facts and circumstances, while providing a list of seven broad factors that can play a role in the determination, including:

- The size, number and frequency of the transaction(s);
- The nature of the transaction(s);
- The level and awareness of management and whether the transaction(s) are part of a pattern of conduct;
- The nexus between the transactions and a blocked person appearing on the Specially Designated Nationals List (SDN List);
- The impact of the transaction(s) on statutory objectives;
- Whether the transactions involve deceptive practices; and
- Such other factors the Secretary of the Treasury deems relevant on a case-by-case basis.

"Knowingly" is defined in the IFSR with respect to conduct, a circumstance or a result, to mean that an entity or individual had actual knowledge, or should have known, about the conduct, the circumstance or the result.

OFAC has indicated it anticipates the use of a broad definition of "financial transaction" that encompasses "any transfer of value involving a financial institution." The term "transaction" includes, but is not limited to:

- The holding of nostro, vostro, or loro accounts for or with the CBI or designated banks, such as Bank Melli Iran and/or Bank Saderat Iran, including any of their branches or subsidiaries worldwide (Listed Parties);
- The provision of trade finance and/or letter of credit services for or with Listed Parties;
- The provision of guarantees or similar instruments for or with Listed Parties;
- The provision of investment products or instruments for Listed Parties and/or the participation with Listed Parties in investments; or the receipt or origination of wire transfers on behalf of or involving Listed Parties;
- The acceptance of commercial paper (retail and wholesale) drawn on Listed Parties and the clearance of such paper (e.g., checks and similar drafts);
- The receipt of or origination of ACH or ATM transactions with Listed Parties; and/or
- Any other transactions for or on behalf of, directly or indirectly, Listed Parties and/or with Listed Parties serving as correspondents, respondents or beneficiaries. That would include transactions where the Listed Parties do not appear on the face of the transaction but where the transaction is undertaken with knowledge of the involvement of a Listed Party based on a relationship that exists through a third party, such as a money exchange or trading house.

1059. Does the NDAA amend CISADA's provision that prohibits or imposes strict conditions on opening and maintaining correspondent accounts or payable-through accounts for designated entities?

No. The NDAA does not amend Section 104(c) of CISADA.

1060. What is the "significant reduction exception" under Section 1245 of the NDAA?

Under Section 1245, the U.S. president can waive sanctions against foreign financial institutions (FFIs) located in countries that have significantly reduced their volume of purchases of Iranian crude oil in a specified period of time.

1061. How has the "significant reduction exception" been amended?

There have been several amendments, the most important of which is the restricting of significant financial transactions to trade transactions between Iran and the country with primary jurisdiction over the FFI and the requirement that funds owed to Iran under these trades be deposited into an account held in the country with primary jurisdiction over the FFI.

1062. Has any country been granted a significant reduction exception under Section 1245 of the NDAA?

Yes. At least 20 countries have been granted a significant reduction exception under Section 1245 of the NDAA since its issuance.

1063. How do the NDAA and Executive Order 13599 and the blocking of all Iranian financial institutions affect the financial sanctions in terms of CISADA? Do CISADA sanctions apply to financial transactions with any Iranian financial institution?

CISADA applies to transactions only with Iranian financial institutions designated in connection with Iran's WMDs or terrorism activities and are identified on the SDN List with the [IFSR] program tag.

On February 5, 2012, the U.S. President issued Executive Order 13599 – Blocking Property of the Government of Iran and Iranian Financial Institutions to amend 31 C.F.R. Part 560: Iranian Transaction Regulations (ITR) to include the provisions within Section 1245 of the NDAA. E.O. 13599 blocks all property and interests in property of the government of Iran, including the Central Bank of Iran (CBI) and all Iranian financial institutions. E.O. 13599 is not grounded in the authorities that relate to counterterrorism or counterproliferation and accordingly does not implicate CISADA.

Previously, financial institutions were obligated to reject these transactions.

Blocked entities under E.O. 13599 appear on OFAC's Specially Designated Nationals List (SDN List) bearing the [IRAN] program tag.

1064. How does Executive Order 13622 impact the NDAA and ISA?

On July 30, 2012, the U.S. president signed Executive Order 13622 – Authorizing Additional Sanctions With Respect to Iran (E.O. 13622). E.O. 13622 provides additional sanctions authorities to the Secretary of the Treasury and the Secretary of State, building on prior authorities outlined in the NDAA

and ISA. The goal of E.O. 13622 is to impose new sanctions against the Iranian energy and petrochemical sectors.

E.O. 13622 imposes financial sanctions on foreign financial institutions found to have knowingly conducted or facilitated any significant financial transaction with the National Iranian Oil Company (NIOC) or Naftiran Intertrade Company (NICO) (except for sales of refined petroleum products to NIOC or NICO that are below the dollar threshold that could trigger sanctions under ISA).

E.O. 13622 also provides additional authority to impose sanctions on foreign financial institutions found to have knowingly conducted or facilitated significant transactions for the purchase or acquisition of petroleum or petroleum products from Iran through any channel, with the aim of deterring Iran or any other country or institution from establishing workaround payment mechanisms for the purchase of Iranian oil to circumvent the NDAA oil sanctions. The existing exception rules under the NDAA will apply to these new sanctions; accordingly, countries determined by the Secretary of State to have significantly reduced their purchases of Iranian crude oil will be excepted from this new measure.

E.O. 13622 further gives the Secretary of the Treasury the authority to block the property and interests in property of any person determined to have materially assisted, sponsored or provided financial, material or technological support for, or goods or services in support of, NIOC, NICO or CBI, or the purchase or acquisition of U.S. bank notes or precious metals by the government of Iran.

It also provides new powers to the Secretary of State (in consultation with the Secretary of the Treasury and other cabinet members) to impose a range of sanctions on individuals or entities determined to have knowingly engaged in significant transactions for the purchase or acquisition of petroleum, petroleum products or petrochemical products from Iran. Entities or individuals that have been found to meet such criteria are to be subject to the same sanctions that may be imposed under the ISA.

All property and interests in property of NIOC and NICO within U.S. jurisdiction are already blocked pursuant to E.O. 13599.

1065. Which Special Measures were authorised against Iran?

Currently, none. In November 2011, FinCEN issued a notice of proposed rulemaking proposing the imposition of a Special Measure against the Islamic Republic of Iran, including the Central Bank of Iran (CBI), as a jurisdiction of primary money laundering concern under Section 311 of the USA PATRIOT Act. The proposed rule would prohibit covered financial institutions from establishing, maintaining, administering or managing correspondent accounts for or on behalf of an Iranian banking institution.

FinCEN indicated in the proposal that prior regulations that have designated jurisdictions of primary money laundering concern under Section 311 have not included the jurisdiction's central bank within the scope of the regulation. Section 1245 of the National Defense Authorisation Act for Fiscal Year 2012 (NDAA) designated the Iranian financial sector as a jurisdiction of primary money laundering concern, effectively mirroring FinCEN's determination in its proposed rulemaking.

1066. Which Special Measures were authorised against Syrian financial institutions?

On March 9, 2006, the U.S. Department of the Treasury designated the Commercial Bank of Syria, including its subsidiary, Syrian Lebanese Commercial Bank, as financial institutions of primary money laundering concern pursuant to Section 311 – Special Measures of the USA PATRIOT Act.

1067. What are the penalties for violations of sanctions imposed by Section 1245 of the NDAA?

Any person who violates, attempts to violate, conspires to violate or causes a violation of the NDAA could be subject to civil penalties and criminal penalties and imprisonment of up to 20 years.

NDAA for Fiscal Year 2013

1068. What is the Iran Freedom and Counter-Proliferation Act of 2012?

Subtitle D of the NDAA for Fiscal Year 2013 is titled the "Iran Freedom and Counter-Proliferation Act of 2012" (IFCA). IFCA strengthens existing sanctions by imposing additional sanctions on the ports of and multiple sectors in Iran (e.g., energy, shipping, shipbuilding and ports) of proliferation concern and on persons providing material assistance to designees on the SDN List.

Additional sanctions are described below in the key sections of IFCA:

- **Section 1244** – Imposition of Sanctions With Respect to the Energy, Shipping and Shipbuilding Sectors and Ports of Iran Due to Proliferation Concerns (e.g., provides revenue to support Iran's nuclear program). Sanctions include:
  - Blocking of property and interests of persons who operate ports in Iran, persons related to the energy, shipping and shipbuilding sectors (e.g., the National Iranian Oil Company [NIOC], the National Iranian Tanker Company [NITC], the Islamic Republic of Iran Shipping Lines and its affiliates) and persons providing material assistance to designees on the Specially Designated Nationals and Blocked Persons List (SDN List);
  - Prohibition on the sale, supply or transfer of certain goods and services in connection with the energy, shipbuilding and shipping sectors of Iran;
  - Restrictions on correspondent and payable-through accounts of Iranian financial institutions that have not been designated for the imposition of sanctions in connection with WMDs, international terrorism or human rights violations; and
  - Provision for exceptions for humanitarian aid and Afghanistan reconstruction.
- **Section 1245 –** Imposition of Sanctions With Respect to the Sale, Supply or Transfer of Certain Materials to or From Iran. Materials include:
  - Precious metals, graphite, raw or semi-finished metals, such as aluminium and steel, coal and software for integrating industrial processes;

  - Any material that can be used in connection with the energy, shipping and shipbuilding sectors of Iran to be controlled by Iran's Islamic Revolutionary Guard Corps (IRGC);
  - Any material sold, supplied or transferred to or from a sanctioned person on the SDN List; and
  - Any material that can be used in connection with the nuclear, military or missile programs of Iran.

- **Section 1246 –** Imposition of Sanctions With Respect to the Provision of Underwriting Services or Insurance or Reinsurance for Activities or Persons with Respect to Which Sanctions Have Been Imposed.
- **Section 1247 –** Imposition of Sanctions With Respect to Foreign Financial Institutions That Facilitate Financial Transactions on Behalf of Specially Designated Nationals.
- **Section 1248 –** Imposition of Sanctions With Respect to the Islamic Republic of Iran Broadcasting
  - Due to their contribution to human rights violations by broadcasting forced confessions and show trials, sanctions under CISADA were imposed on the Islamic Republic of Iran Broadcasting and its president, Ezzatollah Zargami.
- **Section 1249 –** Imposition of Sanctions With Respect to Persons Engaged in the Diversion of Goods Intended for the People of Iran
  - Amends CISADA by imposing sanctions on persons who engage in diversion of humanitarian aid (e.g., food, agricultural commodities, medicine, medical devices). Sanctioned activities include both diversion and misappropriation of proceeds from the sale or resale of such goods.
- **Section 1250 –** Waiver Requirement Related to Exceptional Circumstances Preventing Significant Reductions in Crude Oil Purchases
  - Amends the "significant reduction exception" outlined in Section 1245 of the NDAA for 2012.
- **Section 1251 –** Statute of Limitations for Civil Actions Regarding Terrorist Acts
  - Increased from four years to 10 years.

1069. What sanctions are authorised by Executive Order 13645?

Issued on June 3, 2013, Executive Order 13645 – Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Freedom and Counter-Proliferation Act of 2012 and Additional Sanctions With Respect to Iran outlines a menu of sanctions available to the U.S. government in response to designated persons or prohibited activities under IFCA.

The following summarises key sections that define the types of sectors, persons and activities subject to sanctions:

- **Section 1** – Implements a blocking provision on the property and interests of foreign financial institutions (FFIs) that knowingly facilitated significant transactions or maintained significant funds in accounts outside of Iran in the currency of Iran (rial); also imposes restrictions on correspondent and payable-through accounts of these FFIs (e.g., prohibited, limiting activity).
- **Section 2 –** Extends sanctions (e.g., blocking provisions) to the property and interests of persons who have materially assisted designated persons on the Specially Designated Nationals and Blocked Persons List (SDN List).
- **Section 3 –** Imposes restrictions on correspondent and payable-through accounts of FFIs that knowingly conducted or facilitated significant transactions on behalf of designated persons on the SDN List or FFIs that knowingly conducted or facilitated significant transactions for the sale, supply or transfer to Iran of significant goods and services used in connection with the automotive sector of Iran.
- **Section 4 –** Exempts from sanctions under the Order activities supporting the Shah Deniz gas project described in Section 603(a) of the Iran Threat Reduction and Syria Human Rights Act of 2012.
- **Section 5 –** Authorises the imposition of the sanctions outlined in Sections 6 and 7 on entities that knowingly engage in significant transactions for the sale, supply or transfer to Iran of significant goods or services used in connection with the automotive sector of Iran.
- **Section 6 –** Authorises the imposition of any of the following sanctions on entities designated under Section 5:
    - Prohibition on the provision of services by the U.S. Export-Import Bank in connection with the export of goods related to designated persons in the Iranian automotive sector;
    - Prohibition on the issuance of licenses by U.S. licensing authorities (e.g., OFAC, BIS) that requires approval by the U.S. government;
    - Prohibition on a financial institution serving as a primary dealer in U.S. government securities or repository of U.S. government funds;
    - Prohibition on U.S. government procurement contracts;
    - Denial of visa and exclusion from entry into the United States of a corporate officer or principal of a sanctioned person; and
    - Extension of sanctions to executives or shareholders with a controlling interest in designated entities.
- **Section 7 –** Imposes a blocking provision on the property and interests of persons engaged in prohibited activities related to Iran's energy, shipping, and shipbuilding sectors; the sale or supply of precious metals; and the provision of underwriting, insurance and reinsurance services. Authorised sanctions include:

  - Prohibiting financial institutions from making loans totalling more than US$10 million;
  - Prohibiting foreign exchange transactions in which the sanctioned person has any interest;
  - Prohibiting transfers of credit or payments between financial institutions involving any interest of the sanctioned person;
  - Blocking property and interests of property of the sanctioned person that come within the United States or in the possession of a U.S. person;
  - Prohibiting U.S. persons from purchasing, investing in or purchasing significant amounts of equity or debt instruments of the sanctioned person;
  - Restricting or prohibiting imports of goods, technology or services from the sanctioned person; and
  - Imposing any of the above sanctions on the principal executives or officers of the sanctioned person.

- **Section 8 –** Imposes a blocking provision on the property and interests of persons engaged in corruption or other activities relating to the diversion or misappropriation of goods intended for the people of Iran (e.g., humanitarian aid).
- **Section 9 –** Prohibits donations of humanitarian goods to persons subject to a blocking provision.
- **Section 10 –** Clarifies that the prohibitions in Sections 1, 2, 7 and 8 extend to any contributions or provisions of funds, goods or services by, to or for the benefit of any person subject to a blocking provision and to receipts of any contribution or provision of funds, goods or services from any such person.
- **Section 11 –** Suspends the entry into the United States of persons who meet one or more of the criteria outlined in Sections 2, 5 and 8.
- **Section 12 –** Authorises the Secretary of the Treasury (in consultation with the Secretary of State) to promulgate rules and enforce this executive order.
- **Section 13 –** Clarifies that prohibited activities include any transaction that evades or avoids, has the purpose of evading or avoiding, causes a violation of, attempts to violate or conspires to violate this executive order.
- **Section 14 –** Provides key definitions (e.g., automotive sector, petroleum, sanctioned person, financial institution, foreign financial institution, Iranian financial institution, government of Iran).
- **Section 15 –** Prohibits notifying sanctioned persons prior to the blocking of property and interests.

- **Section 16 –** Outlines amendments to Executive Order 13622 (e.g., expanding the definition of financial institutions to include dealers in precious metals, stones or jewels).

1070. Where can a list of persons designated under IFCA and Executive Order 13645 be found?

Persons designated under IFCA appear on the SDN List with the [IFCA] program tag. Annotations on the SDN List provide descriptions of the section of IFCA under which the person was designated (e.g., IFCA Determination – Involved in Energy Sector; IFCA Determination – Involved in the Shipbuilding Sector; IFCA Determination – Involved in the Shipping Sector; or IFCA Determination – Port Operator).

Other Executive Orders & Actions

1071. What other measures have been imposed in connection with Syria?

In addition to other broad sanctions imposed against Syria, three executive orders have been issued involving Syria.

On May 18, 2011, Executive Order 13573 was issued, titled "Blocking Property of Senior Officials of the Government of Syria," which imposed the blocking of the property and interests of certain persons and agencies of the government of Syria.

On August 17, 2011, Executive Order 13582 – Blocking Property of the Government of Syria and Prohibiting Certain Transactions With Respect to Syria was issued. The order imposed broad prohibitions on investments with Syria, most exportation and importation, sales or supply from the United States or by a U.S. person wherever located into Syria; or any services to Syria, as well as other actions.

Executive Order 13582 also provides that all property and interests in property that are in the United States, that hereafter come within the United States or that hereafter come within the possession or control of any U.S. person, including any overseas branch of the government of Syria, are blocked and may not be transferred, paid, exported, withdrawn or otherwise dealt in.

Additionally, all property and interests in property are also blocked for any person the Secretary of the Treasury determines has:

- Materially assisted, sponsored or provided financial, material or technological support for, or goods or services in support of, any person whose property and interest in property are blocked pursuant to the order; or
- Are owned, controlled by or have acted or purposed to act for or on behalf of, directly or indirectly, any person whose property and interests are blocked pursuant to this order.

On May 1, 2012, Executive Order 13608 was issued, which, among other things, authorised the U.S. Department of the Treasury to impose broad sanctions on anyone who has violated or attempted to violate certain orders concerning property and interests in property of any person subject to U.S.

sanctions concerning Syria or Iran, or who has facilitated deceptive transactions for or on behalf of any person subject to U.S. sanctions concerning Syria or Iran.

1072. How does Executive Order 13606 (GHRAVITY E.O.) impact the obligations of financial institutions?

On April 22, 2012, the U.S. president signed Executive Order 13606 – Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology (GHRAVITY E.O.).

The GHRAVITY E.O. requires U.S. persons to block all property and interests in property of persons designated by the Secretary of the Treasury, in consultation with or at the recommendation of the Secretary of State, who:

- Have operated, or directed the operation of, information and communications technology that facilitates computer or network disruption, monitoring or tracking that could assist in or enable serious human rights abuses by or on behalf of the government of Iran or the government of Syria;
- Have sold, leased or otherwise provided, directly or indirectly, goods, services or technology to Iran or Syria likely to be used to facilitate such activities;
- Have materially assisted, sponsored or provided financial, material or technological support for, or goods or services to or in support of, the activities described above or any person whose property and interests in property are blocked pursuant to this order; or
- Have been owned or controlled by, or have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to the order.

Entities that are 50 percent or more owned by persons blocked by the GHRAVITY E.O. are also blocked, regardless of whether such entities appear on the Annex or OFAC's SDN List.

1073. Where can a list of persons designated under GHRAVITIY E.O. be found?

Designated entities under GHRAVITY E.O. appear on the SDN List bearing the [HRIT] program tag.

1074. How is "information and communications technology" defined for the purposes of GHRAVITY E.O.?

"Information and communications technology" is defined as "any hardware, software, or other product or service primarily intended to fulfil or enable the function of information processing and communication by electronic means, including transmission and display, including via the internet."

1075. How does Executive Order 13608 – Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria – impact the obligations of financial institutions?

On May 1, 2012, the U.S. president signed Executive Order 13608 – Prohibiting Certain Transactions With and Suspending Entry Into the United States of Foreign Sanctions Evaders With Respect to Iran and Syria (E.O. 13068). E.O. 13608 strengthened U.S. Department of the Treasury's ability to impose

sanctions on foreign persons determined to have violated, attempted to violate, conspired to violate, or caused a violation of sanctions on Iran or Syria.

E.O. 13608 also gives the U.S. Department of the Treasury the authority to impose sanctions on foreign persons who have facilitated deceptive transactions for or on behalf of persons subject to U.S. sanctions. E.O. 13608 empowers the Secretary of the Treasury, in consultation with the Secretary of State, to:

- Impose on a foreign person certain measures upon determining that the foreign person has violated, attempted to violate, conspired to violate or caused a violation of any license, order, regulation or prohibition contained in, or issued pursuant to certain executive orders related to national emergencies, or to the extent such conduct relates to property and interest in property of any person subject to the U.S. sanctions concerning Iran or Syria, or certain national emergencies, as defined in specific executive orders.
- Prohibit, to the extent in or related to either any goods, services or technology in or intended for the United States, or any goods, services or technology provided by or to the U.S. persons, wherever located, all transactions or dealings, whether direct or indirect, involving such persons, including, but not limited to, the following activities:
  - Exporting
  - Re-exporting
  - Importing
  - Selling
  - Purchasing
  - Transporting
  - Swapping
  - Brokering
  - Approving
  - Financing
  - Facilitating
  - Guaranteeing

These prohibitions apply, except to the extent provided by statutes, or in regulations, orders, directives or licenses that may be issued pursuant to this Order, and notwithstanding any contract entered into or any license or permit granted prior to the date of this Order.

Transactions by U.S. persons, or within the United States involving persons sanctioned under this order, are prohibited, effectively cutting the listed persons off from the U.S. marketplace and financial system. By cutting off access to the U.S. marketplace and financial system to such sanction evaders, the order provides the U.S. Department of the Treasury with the power to prevent and deter such behaviour and to hold such persons accountable and to convince them to change their behaviour. Publicly identifying such persons also allows U.S. persons to avoid unwittingly engaging in transactions with identified foreign persons who may expose U.S. persons to the risk of sanctions violations.

If an individual or entity is made subject to the sanctions under this order, U.S. persons generally may no longer provide or procure from such individual or entity any goods, services or technology. Practically speaking, it means that the sanctioned individual or entity will be cut off from the U.S. commercial and financial systems.

Financial institutions must:

- Reject any wire transfer involving a listed person; and
- Restrict the use of accounts owned by a listed person, so that they cannot be operated without an authorisation from OFAC. However, the account is not blocked. In general, a financial institution is prohibited from providing to or procuring from such a sanctioned individual or entity any goods, services or technology.

1076. How is the term "deceptive transaction" defined for the purposes of E.O. 13608?

A "deceptive transaction" is defined as "any transaction where the identity of any person subject to U.S. sanctions concerning Iran or Syria is withheld or obscured from other participants in the transaction or any relevant regulatory authorities."

Foreign persons who have facilitated deceptive transactions will be listed under E.O. 13608 and subject to sanctions. Although these transactions are not subject to blocking under this specific order (although, if they are otherwise subject to blocking under another program, then blocking is required), a U.S. person may not provide or procure goods or services, including financial services, or technology to or from a listed person without authorisation from OFAC, unless the transaction is otherwise exempt from regulation under the International Emergency Economic Powers Act (IEEPA) (e.g., certain travel-related transactions). Wire transfers involving the assets of a listed person under this order must be rejected. A U.S. person is prohibited from dealing with an E.O. 13608-listed person, even where the dealing does not involve Iran or Syria (as well as where it does involve either country).

1077. How is the E.O. 13608 List different from the Denied Persons List maintained by BIS?

The Denied Persons List (DPL) is a list of individuals and entities that have been denied export privileges for violating or presenting an imminent risk of violating the Export Administration Regulations (EAR). E.O. 13608 complements the DPL by addressing two types of sanctions violations outside of the scope of the EAR:

- The prohibition of the provision of services, goods and technology and the prohibition of transactions to or from identified or listed persons; and
- The U.S. Department of the Treasury may prohibit transactions or dealings involving goods and technology not subject to EAR.

However, unlike the U.S. Department of Commerce's authority, the U.S. Department of the Treasury's authority under this order may be implemented only with respect to foreign individuals or entities.

1078. What if a transaction is already under way?

If a transaction is under way at the time of the listing, a U.S. person must cease dealing with the listed person and the U.S. person is prohibited from engaging in transactions or dealings in or related to any goods, services or technology to or from the listed person, unless the transaction is exempt under IEEPA, or until such time that OFAC authorises the transaction pursuant to the order. If the transaction involves a wire transfer, the U.S. financial institution must reject it and file a rejection

report with OFAC within 10 days. Also, a U.S. person may not use a listed person to facilitate personal remittances to or from Iran or Syria without specific authorisation from OFAC.

1079. What is the Joint Comprehensive Plan of Action (JCPOA) and how did it impact Iranian sanctions?

Extending the Joint Plan of Action (JPOA) of 2015, the Joint Comprehensive Plan of Action (JCPOA) of 2016 is an agreement between Iran, China, France, Germany, Russia, the United Kingdom and the United States that ensures Iran's nuclear program remains exclusively peaceful. Under the JCPOA, secondary nuclear-related sanctions were suspended providing Iran sanctions relief on the condition that the International Atomic Energy Agency (IAEA) verifies certain nuclear-related measures have been implemented by Iran as outlined in the JCPOA.

In connection with select activities outlined in the JCPOA, secondary sanctions related to sectors including, but not limited to the following were suspended:

- Financial and banking-related activities;
- Underwriting services, insurance, re-insurance;
- Iran's energy and petrochemical sectors;
- Iran's shipping and shipbuilding sector and port operators;
- Iran's gold and other precious metals;
- Iran's graphite, raw or semi-finished metals (e.g., aluminium, steel, graphite);
- Automotive sector; and
- Commercial passenger aviation.

In addition to the lifting of secondary sanctions, hundreds of designees were removed from the following OFAC Sanctions Listings:

- Specially Designated Nationals and Blocked Persons (SDN) List;
- Foreign Sanction Evaders (FSE) List; and
- Non-SDN Iran Sanctions Act (NS-ISA) List.

Existing sanctions on Iran related to the following activities remain in place:

- Support for terrorism;
- Human rights abuses in Iran and Syria;
- Proliferation of WMDs; and
- Actions that threaten the peace, security or stability of Yemen.

The suspending of sanctions under the JCPOA was accomplished through the issuance of Executive Order 13716, the issuance of contingent waivers of certain statutory sanctions provisions by the U.S. Department of State and the updating of OFAC sanctions designations.

- OFAC has released the following guidance on the impact of the JCPOA on Iranian sanctions: Guidance Relating to the Lifting of Certain U.S. Sanctions Pursuant to the Joint Comprehensive Plan of Action on Implementation Day (2016)
- Frequently Asked Questions Relating to the Lifting of Certain U.S. Sanctions Under the Joint Comprehensive Plan of Action (JCPOA) on Implementation Day (2016)

While many sanctions, as described above, have been suspended, the JCPOA did not revoke the authority of the president to reimpose such sanctions.

1080. What are "secondary sanctions"?

Per the JCPOA, "secondary sanctions" are sanctions "generally directed toward non-U.S. persons for specified conduct involving Iran that occurs entirely outside of U.S. jurisdiction."

1081. How does Executive Order 13716 impact sanctions in connection to Iran?

On July 14, 2015, Executive Order 13716 was issued, which, among other things revoked the following executive orders as they relate to Iran:

- **Executive Order 13574** - Authorizing the Implementation of Certain Sanctions Set Forth in the Iran Sanctions Act of 1996, as Amended (2011)
- **Executive Order 13590** - Authorizing the Imposition of Certain Sanctions With Respect to the Provision of Goods, Services, Technology, or Support for Iran's Energy and Petrochemical Sectors (2011)
- **Executive Order 13622** - Authorizing Additional Sanctions With Respect to Iran (2012)
- **Executive Order 13628** – Authorizing the Implementation of Certain Sanctions Set For in the Iran Threat Reduction and Syria Human Rights Act of 2012 and Additional Sanctions With Respect to Iran (2012) (Sections 5-7 and 15)

1082. What is the "Statement of Licensing Policy" issued by OFAC with respect to Iran?

On January 2016, in conjunction with the JCPOA, OFAC released the "Statement of Licensing Policy for Activities Related to the Export or Re-Export to Iran of Commercial Passenger Aircraft and Related Parts and Services" (SLP) to establish a favourable licensing policy process through which U.S. persons may efficiently request authorisation to engage in Iran's civil aviation industry.

1083. If Iran fails to meet its obligations under the JCPOA, are U.S. persons who have engaged with Iranian entities retroactively liable for sanctions violations?

No. OFAC will not retroactively impose sanctions on activity that was deemed permissible under the JCPOA if Iran fails to meet its obligations. However, U.S. persons could be held liable if they continue to conduct activity after Iranian sanctions have been re-imposed.

1084. If Iran fails to meet its obligations under the JCPOA, will the U.S. grant a "wind-down period" to allow U.S. persons to disengage with Iranian entities?

If Iranian sanctions were to be re-imposed, OFAC may provide guidance on a "wind-down period" to minimise sanctions violations, but there is no guarantee that such period will be provided.

1085. What is the aim of the proposed law Countering Iran's Destabilising Activities of 2017?

Introduced by the U.S. Senate in March 2017, and passed by the U.S. Senate in June 2017, the Countering Iran's Destabilising Activities of 2017 calls for the following with respect to Iran:

- Development of regional strategy to counter Iranian threats in the Middle East and North Africa
- Imposition of additional sanctions with respect to:
    - Iran's ballistic missile program
    - Islamic Revolutionary Guard Corps (IRGC)
    - Human rights abuses
- Review of applicability of sanctions relating to Iran's support for terrorism and its ballistic missile program
- Enforcement of arms embargoes
- Report on coordination of sanctions between the United States and the European Union
- Report on United States citizens detained by Iran
- Exceptions for national security and humanitarian assistance
- Presidential waiver authority (e.g., case-by-case waiver authority, renewal of waivers)

Title II of Countering Iran's Destabilising Activities of 2017 calls for the following with respect to Russia:

- Codification of sanctions relation to the Russian Federations
- Modification of implementation of Executive Order 13662 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine
- Imposition of sanctions with respect to:
    - Activities of the Russian Federation undermining cybersecurity
    - Transfer of arms and related material to Syria
    - Special Russian crude oil projects
    - Development of pipelines in the Russian Federation
    - Investment in or facilitation of the privatisation of state-owned assets by the Russian Federation
    - Significant corruption in the Russian Federation

- Russian and other foreign financial institutions
- Persons engaging with the intelligence or defence sectors of the Government of the Russian Federation
- Foreign sanctions evaders
- Human rights abuses

For further guidance on Russian sanctions, please refer to the Russian and Ukraine-Related Sanctions Program Overview.

Iraqi Sanctions Program Overview

1086. What are the major U.S. government sanctions programs affecting Iraq?

The U.S. government has imposed sanctions on the Republic of Iraq, including, but not limited to, those mandated by the following statutes and executive orders:

- **Immigration and Nationality Act of 1952** (1952)
- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 12722 – Blocking Iraqi Government Property And Prohibiting Transactions With Iraq** (1990)
- **Executive Order 12724 – Blocking Iraqi Government Property And Prohibiting Transactions With Iraq** (1990)
- **Executive Order 12817 – Transfer Of Certain Iraqi Government Assets Held By Domestic Banks** (1992)
- **Executive Order 13290 – Confiscating and Vesting Certain Iraqi Property** (2003)
- **Executive Order 13303 – Protecting the Development Fund for Iraq and Certain Other Property in Which Iraq Has an Interest** (2003)
- **Executive Order 13315 – Blocking Property of the Former Iraqi Regime, Its Senior Officials and Their Family Members, and Taking Certain Other Actions** (2003)
- **Executive Order 13350 – Termination of Emergency Declared in Executive Order 12722 With Respect to Iraq and Modification of Executive Order 13290, Executive Order 13303, and Executive Order 13315** (2004)
- **Executive Order 13364 – Modifying the Protection Granted to the Development Fund for Iraq** (2004)
- **Executive Order 13438 – Blocking Property of Certain Persons Who Threaten Stabilisation Efforts in Iraq** (2007)

- **Executive Order 13668 – Ending Immunities Granted to the Development Fund for Iraq and Certain Other Iraqi Property and Interests in Property Pursuant to Executive Order 13303, as Amended** (2014)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Iraq:

- **UNSCR 661** (1990)
- **UNSCR 670** (1990)
- **UNSCR 687** (1991)
- **UNSCR 706** (1991)
- **UNSCR 778** (1992)
- **UNSCR 986** (1995)
- **UNSCR 1051** (1996)
- **UNSCR 1111** (1997)
- **UNSCR 1129** (1997)
- **UNSCR 1143** (1997)
- **UNSCR 1153** (1998)
- **UNSCR 1158** (1998)
- **UNSCR 1175** (1998)
- **UNSCR 1284** (1999)
- **UNSCR 1293** (2000)
- **UNSCR 1483** (2003)

The following regulation implements Iraqi sanctions:

- **31 C.F.R. Part 575 – Removal of the Iraqi Sanctions Regulations**
- **31 C.F.R. Part 576 –Iraq Stabilisation and Insurgency Sanctions Regulations (ISISR)**

1087. What are the primary objectives of OFAC Sanctions Programs affecting Iraq?

According to OFAC's overview of the Iraq Sanctions Program, the primary objectives of the U.S. government with respect to Iraq are:

- Restrict and eliminate widespread violence, efforts to undermine the economic reconstruction and political reform of Iraq and the blocking of humanitarian assistance;
- Freeze assets of specific individuals and entities associated with the former Saddam Hussein regime; and

- Prohibit trade in or transfer of ownership or possession of Iraqi cultural property or other items of archaeological, historical, cultural, rare scientific and religious importance that were illegally removed (or suspected to be illegally removed) from the Iraq National Museum, the National Library and other locations in Iraq since August 1990.

However, most Iraq sanctions are no longer enforced post-Iraq War.

1088. Where can one find a list of designated entities under the Iraqi Sanctions Program?

Designations are maintained in the appendices of applicable Iraqi regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tags [IRAQ2] and [IRAQ3].

1089. What action must institutions take if a positive "hit" is identified for the Iraqi Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Lebanese Sanctions Program Overview

1090. What are the major U.S. government sanctions programs affecting Lebanon?

The U.S. government has imposed sanctions on Lebanon, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 13441 – Blocking Property of Persons Undermining the Sovereignty of Lebanon or Its Democratic Processes and Institutions** (2007)

The following regulation implemented Lebanese sanctions:

- **31 C.F.R. Part 549 – Lebanon Sanctions Regulations**

1091. What are the primary objectives of OFAC Sanctions Programs affecting Lebanon?

The primary objectives of the U.S. government with respect to the Lebanese Republic (Lebanon) are to restrict and eliminate the breakdown of the rule of law, politically motivated violence and intimidation, reassertion of Syrian control or Syrian interference that threatens the economic or political stability, national security, foreign policy or sovereignty of Lebanon.

According to OFAC's Lebanon Sanctions Program, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions or posing significant risk of taking actions, including acts of violence, that have the purpose or effect of undermining Lebanon's democratic processes or institutions, contributing to

the breakdown of the rule of law in Lebanon, supporting the reassertion of Syrian control or otherwise contributing to Syrian interference in Lebanon or infringing upon or undermining Lebanese sovereignty;

- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned activities; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Lebanese Sanctions Program.

1092. Where can one find a list of designated entities under the Lebanese Sanctions Program?

Designations are maintained in the appendices of applicable Lebanese regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [LEBANON].

1093. What action must institutions take if a positive "hit" is identified for the Lebanon Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Liberian Sanctions Program Overview

1094. What were the major U.S. government sanctions programs affecting Liberia?

The U.S. government had imposed sanctions on the former President Charles Taylor of the Republic of Liberia, including those mandated by the following statutes and executive orders:

- **United Nations Participation Act (UNPA), Section 5** (1945)
- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 13348 - Blocking Property of Certain Persons and Prohibiting the Importation of Certain Goods from Liberia** (2004)
- **Executive Order 13710 - Termination of Emergency With Respect to the Actions and Policies of Former Liberian President Charles Taylor** (2015)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Liberia:

- **UNSCR 1521** (2003)
- **UNSCR 1532** (2004)

The following regulation implemented Liberian sanctions:

- **31 C.F.R. Part 593– Former Liberian Regime of Charles Taylor Sanctions Regulations**

As of November 2015, the U.S. terminated the Liberian Sanctions Program.

1095. What were the primary objectives of OFAC Sanctions Programs affecting Liberia?

The primary objectives of the U.S. government with respect to Liberian sanctions were to restrict and eliminate the unlawful depletion of Liberian resources (e.g., illicit trade of round logs and timber products) by former President Charles Taylor and his regime.

According to OFAC's overview of the Former Liberian Regime of Charles Taylor Sanctions Program, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Being or have been an immediate family member of Charles Taylor;
- Being or have been a senior official of the former Liberian regime headed by Charles Taylor or otherwise to have been or be a close ally or associate of Charles Taylor or the former Liberian regime;
- Materially assisting, sponsoring or providing financial, material or technological support for goods or services in support of the unlawful depletion of Liberian resources, the removal of Liberian resources from that country and the secreting of Liberian funds and property by any person whose property and interest are blocked under the Liberian Sanctions Program;
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Liberian Sanctions Program.

1096. Where can one find a list of designated entities under the Liberian Sanctions Program?

Designations were maintained in the appendices of the Liberian regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [LIBERIA]. As of November 2015, the U.S. terminated the Liberian Sanctions Programs.

Libyan Sanctions Program Overview

1097. What are the major U.S. government sanctions programs affecting Libya?

The U.S. government has imposed sanctions on Libya, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949)

- **Immigration and Nationality Act of 1952** (1952)
- **Executive Order 13566 – Blocking Property and Prohibiting Certain Transactions Related to Libya** (2011)
- **Executive Order 13726 – Blocking Property and Suspending Entry into the United States of Persons Contributing to the Situation in Libya** (2016)

The following regulation implements Libyan sanctions:

- **31 C.F.R. Part 570 – Libyan Sanctions Regulations**

1098. What are the primary objectives of the OFAC Sanctions Program affecting Libya?

The primary objectives of the U.S. government with respect to Libyan sanctions are to restrict:

- Extreme measures taken against the people of Libya including the use of weapons of war, mercenaries, or wanton violence against unarmed civilians;
- Attacks by armed groups against Libyan state facilities, foreign missions in Libya and critical infrastructure;
- Misappropriation of Libyan assets by Qadhafi, members of his government, family and close associates;
- Misappropriation of Libyan natural resources; and
- Violations of the arms embargo imposed by the United Nations Security Resolution (UNSR) 1970 (2011).

According to OFAC's Libya Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions that threaten the peace, security or stability of Libya including the supply of arms or related material;
- Actions or policies that obstruct, undermine, delay, impede or pose significant risk of obstructing, undermining, delaying, or impeding the adoption of or political transition to a Government of National Accord or a successor government;
- Actions that may have led to or resulted in the misappropriation of state assets of Libya;
- Ordering, controlling or otherwise directing or participating in the commission of human rights abuses related to political repression in Libya;
- Threatening or coercing Libyan state financial institutions or the Libyan National Oil Company;
- Planning, directing or committing or to have planned, directed or committed attacks against any Libyan state facility or installation (including oil facilities) against any air, land or sea port in Libya or against any foreign mission in Libya;

- Targeting of women, children or any civilian through the commission of acts of violence (e.g., killing, maiming, torture, rape, abduction, forced displacement) or other conduct that may constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Targeting of schools, hospitals, religious sites or locations where civilians are seeking refuge through the commission of acts of violence or other conduct that may constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Being a senior official of the Government of Libya;
- Being a child of Colonel Muammar Qadhafi;
- Being a leader of an entity that has or whose members have engaged in any of the aforementioned activities;
- Materially assisting, sponsoring or providing financial, material, logistical or technical support for, or goods or services in support of the aforementioned activities;
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Libyan Sanctions Program; or
- Being a spouse or dependent child of any SDN as designated by the Libyan Sanctions Program.

1099. Where can one find a list of designated entities under the Libyan Sanctions Program?

Designations are maintained in the appendices of applicable Libyan regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [LIBYA2].

1100. What action must institutions take if a positive "hit" is identified for the Libyan Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

North Korean Sanctions Program Overview

1101. What are the major U.S. government sanctions programs affecting North Korea?

The U.S. government has imposed sanctions on North Korea, including, but not limited to, those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)

- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949)
- **Antiterrorism and Effective Death Penalty Act (AEDPA)** (1996)
- **North Korea Sanctions and Policy Enhancement Act of 2016 (NKSPEA)** (2016)
- **Executive Order 13466 – Continuing Certain Restrictions with Respect to North Korea and North Korean Nationals** (2008)
- **Proclamation 8271 – Termination of the Exercise of Authorities Under the Trading With the Enemy Act With Respect to North Korea** (2008)
- **Executive Order 13551 – Blocking Property of Certain Persons with Respect to North Korea** (2010)
- **Executive Order 13570 – Prohibiting Certain Transactions with Respect to North Korea** (2011)
- **Executive Order 13687 – Imposing Additional Sanctions with Respect to North Korea** (2015)
- **Executive Order 13722 – Blocking Property of the Government of North Korea and the Workers' Party of Korea and Prohibiting Certain Transactions with Respect to North Korea** (2016)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to North Korea:

- **UNSCR 1718** (2006)
- **UNSCR 1874** (2009)
- **UNSCR 2087** (2013)
- **UNSCR 2094** (2013)
- **UNSCR 2270** (2016)

The following regulation implements North Korean sanctions:

- **31 C.F.R. Part 510 – North Korea Sanctions Regulations**

1102. What are the primary objectives of OFAC Sanctions Programs affecting North Korea?

The primary objective of the U.S. government with respect to the Democratic People's Republic of Korea (DPRK) (North Korea) sanctions is to restrict and eliminate the existence and risk of the proliferation of weapons of mass destruction (WMD) and weapons-usable fissile material on the Korean Peninsula.

All property and interests of the Government of North Korea and the Worker's Party of Korea are blocked. According to OFAC's North Korea Sanctions Program overview, designees have been

identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Activities or transactions that have materially contributed to or pose a risk of materially contributing to the proliferation of WMDs or their means of delivery, including any efforts to manufacture, acquire, possess, develop, transport, transfer or use such items by any person or foreign country of proliferation concern;
- Importing, exporting or re-exporting to, into or from North Korea any arms or related material;
- Importing, exporting, re-exporting, selling or supplying arms or related material from North Korea or the Government of North Korea to Burma or the Government of Burma;
- Providing training, advice or other services or assistance or engaging in financial transactions, related to the manufacture or use of any arms or related material to be imported, exported or re-exported to, into, from North Korea or following their importation, exportation or re-exportation to, into or from North Korea;
- Importing, exporting or re-exporting luxury goods to or into North Korea;
- Engaging in money laundering, the counterfeiting of goods or currency, bulk cash smuggling, narcotics trafficking or other illicit economic activity that involves or supports the Government of North Korea or any senior official thereof;
- Being an agency, instrumentality or controlled entity of the Government of North Korea or the Worker's Party of Korea;
- Being an official of the Government of North Korea;
- Being an official of the Worker's Party of Korea;
- Operating in any industry in the North Korean economy designated by the North Korean Sanctions Program (e.g., transportation, mining, energy, financial services);
- Selling, supplying, transferring or purchasing to or from North Korea or any person acting for or on behalf of the Government of North Korea or the Worker's Party of Korea, metal, graphite, coal or software benefiting the Government of North Korea or the Worker's Party of Korea, including North Korea's nuclear or ballistic missile programs;
- Engaging in, facilitating or being responsible for an abuse or violation of human rights by the Government of North Korea or the Worker's Party of Korea or any person acting for or on behalf of either entity;
- Engaging in, facilitating or being responsible for the exportation of workers from North Korea for the benefit of the Government of North Korea or the Worker's Party of North Korea;
- Engaging in significant activities undermining cybersecurity through the use of computer networks or systems against targets outside of North Korea on behalf of the Government of North Korea or the Worker's Party of North Korea;

- Engaging in, facilitating or being responsible for censorship by the Government of North Korea or the Worker's Party of North Korea;
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the North Korea Sanctions Program; or
- Attempting to engage in the aforementioned activities.

1103. Has the United States issued other AML/CFT measures against North Korea outside of the North Korean Sanctions Program?

Yes. In November 2016, the United States imposed the Fifth Special Measure, the prohibition of opening or maintaining correspondent or payable-through-accounts (PTAs) for North Korean financial institutions, under Section 311 of the USA PATRIOT Act.

In June 2017, the Fifth Special Measure was applied to China's Bank of Dandong for alleged illicit financial ties to North Korea.

For further guidance, please refer to Section 311 – Special Measures.

1104. Why did the United States utilise Special Measures as opposed to its sanctions program to prevent North Korean financial institutions from accessing the U.S. financial system?

One reason may be because of the use of aliases and front companies used by North Korean financial institutions. The extensive use of aliases and front companies makes it difficult to maintain accurate lists of designees and renders interdiction software used to screen for these names ineffective. The Fifth Special Measure not only prohibits the provision of correspondent banking services to North Korean financial institutions, it requires U.S. financial institutions to do the following:

- Conduct due diligence on its correspondent accounts to prevent indirect access by North Korean financial institutions, and
- Notify its foreign respondents of the prohibition on providing North Korean financial institutions access to their correspondent accounts.

1105. Where can one find a list of designated entities under the North Korean Sanctions Program?

Designations are maintained in the appendices of applicable North Korean regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [DPRK].

1106. What action must institutions take if a positive "hit" is identified for the North Korean Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For

guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Russian and Ukraine-Related Sanctions Program Overview

1107. What are the major U.S. government sanctions programs affecting Russia?

The U.S. government has imposed sanctions on Russia, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Sergei Magnitsky Rule of Law Accountability Act of 2012** (2012)
- **Executive Order 13660 – Blocking Property of Certain Persons Contributing to the Situation in Ukraine** (2014)
- **Executive Order 13661 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine** (2014)
- **Executive Order 13662 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine** (2014)
- **Executive Order 13685 – Blocking Property of Certain Persons and Prohibiting Certain Transactions with Respect to the Crimea Region of Ukraine** (2014)
- **Global Magnitsky Human Rights Accountability Act** (2016)

OFAC administers the following sanctions programs related to Russia/Russian individuals and companies:

- The **Magnitsky Sanctions** (initially limited to Russia but now expanded to include acts of corruption and human rights violations conducted by all foreign persons); and
- The **Ukraine-Related Sanctions**, including the Sectoral Sanctions Identifications (SSI) List.

The Cyber-Related Sanctions Program was expanded shortly after the alleged cyber-espionage conducted by Russia in the 2016 presidential election. For further guidance on the Cyber-Related Sanctions Program, refer to the Cyber-Related Sanctions Program section.

The Magnitsky Sanctions

1108. Who was Sergei Magnitsky?

Sergei Magnitsky, a lawyer fighting corruption and criminal conspiracy involving Hermitage Fund companies, was a Russian citizen whose arrest and pre-trial detention were ruled as illegal by then Russian President Dimitry Medvedev's Human Rights Council in July 2011. The Human Rights Council stated that as a result of abuse and neglect, Magnitsky died on November 16, 2009 in Matrosskaya Tishina Prison in Moscow, Russia.

1109. What are the primary objectives of OFAC Sanctions Programs of the Magnitsky sanctions?

The primary objectives of the U.S. government with respect to the initial Magnitsky sanctions were to block the property and interests of:

- Persons responsible for the detention, abuse and death of Sergei Magnitsky, those who benefitted financially from his detention, abuse and death; participated in the efforts to conceal the legal liability of his detention; and those who were involved in the criminal conspiracy uncovered by Magnitsky;
- Persons responsible for extrajudicial killings, torture or other gross violations of internationally recognised human rights committed against individuals seeking to:
  - Expose illegal activity carried out by officials of the Government of the Russian Federation;
  - Obtain, exercise, defend or promote internationally recognised human rights and freedoms (e.g., freedoms of religion, expression, association and assembly) and the rights to a fair trial and democratic elections in Russia
- Persons acting as an agent of or on behalf of a person involved in the aforementioned acts.

The Global Magnitsky Human Rights Accountability Act (2016) expands the Magnitsky Sanctions Program to include foreign persons for gross violations of internationally recognised human rights beyond those related to the detention and death of Sergei Magnitsky. Sanctions can also be imposed on foreign officials involved in "significant corruption."

The U.S. can impose U.S. entry and sanctions against any foreign person (or entity) that has been responsible for or complicit in, or has engaged in, directly or indirectly, any of the following:

- Extrajudicial killings, torture or other gross violations of internationally recognised human rights committed against individuals in any foreign country seeking to expose illegal activity carried out by government officials or to obtain, exercise or promote human rights and freedoms;
- Acting as an agent of or on behalf of a foreign person in such activities;
- Being a government official or senior associate of such official responsible for, or complicit in, ordering or otherwise directing acts of significant corruption, including the expropriation of private or public assets for personal gain, corruption related to government contracts or the extraction of natural resources, bribery or the facilitation or transfer of the proceeds of corruption to foreign jurisdictions; or
- Materially assisting or providing financial, material or technological support for, or goods or services in support of such activities.

1110. Where can one find a list of designated entities under Magnitsky sanctions?

Designations are on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [MAGNIT].

1111. What action must institutions take if a positive "hit" is identified for the Magnitsky sanctions?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Ukraine-Related Sanctions Program Overview

1112. What are the primary objectives of OFAC Sanctions Programs affecting Ukraine?

The primary objectives of the U.S. government with respect to Ukraine-Related sanctions are to restrict and eliminate threats posed by persons who undermined democratic processes and institutions of Ukraine, misappropriated Ukrainian public assets and threatened the peace, security, stability, sovereignty and territorial integrity of Ukraine.

According to OFAC's Ukraine/Russia-Related Sanctions overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions or policies that undermine democratic processes or institutions in Ukraine;
- Actions or policies that threaten the peace, security, stability or territorial integrity of Ukraine (e.g., Crimea);
- Misappropriation of state assets of Ukraine or of an economically significant entity in Ukraine;
- Asserting governmental authority over any part or region of Ukraine without the authorisation of the Government of Ukraine;
- Being a leader of an entity that has or whose members have engaged in of the aforementioned acts;
- Being an official of the Government of the Russian Federation;
- Operating in the arms or related material sector in the Russian Federation;
- Operating in such sectors of the Russian Federation economy as may be determined by the U.S. Secretary of Treasury in consultation with the U.S. Secretary of State;
- Operating in the Crimea region of Ukraine;
- Being a leader of an entity operating in the Crimea region of Ukraine;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned activities; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Ukraine-Related Sanctions Program.

1113. Where can one find a list of designated entities under the Ukraine-Related Sanctions Program?

Designations are maintained in the appendices of Ukraine-Related regulations and on the following lists:

- Specially Designated Nationals (SDN) List administered by OFAC with the program tags [UKRAINE-EO13660] and [UKRAINE-EO13661]; and
- Sectoral Sanctions Identifications (SSI) List with the program tag [UKRAINE-EO13662].

For further guidance on the SSI List, please refer to the Sectoral Sanctions Identification List section.

1114. What action must institutions take if a positive "hit" is identified for the Ukraine-Related Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Additional and Pending Sanctions

1115. Were additional sanctions imposed on Russia for their alleged involvement in the U.S. presidential election of 2016?

Yes. The Obama administration expelled Russian diplomats who were suspected of cyber-espionage during the U.S. presidential election of 2016. The administration also placed several Russian intelligence agencies and officials on the SDN List. This was accomplished under the Cyber-Related Sanctions Program which was expanded through Executive Order 13757 – Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, to address the alleged cyber-related activities committed by the Russians. For further guidance, please refer to the Cyber-Related Sanctions Program section.

Additionally, in January 2017, the U.S. Congress proposed bills to establish an independent commission to examine Russian attempts to interfere in the 2016 U.S. presidential election via cyber operations or other means (Commission to End Russian Interference in the United States Election) and to codify existing sanctions (e.g., Executive Order 13694 – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities, Executive Order 13660 – Blocking Property of Certain Persons Contributing to the Situation in Ukraine) and impose further sanctions on Russia (Counteracting Russian Hostilities Act of 2017 [CRHA]) for other aggressive acts. The CRHA proposed sanctions on the following types of activities:

- On persons engaged in significant activities undermining cybersecurity and democratic institutions:
  - Asset blocking;
  - Exclusion from the United States; and

  - Revocation of visas (or other documentation).

- On persons engaging in transactions with the intelligence or defence sectors of the government of the Russian Federation; on persons engaged in specified aggressive acts relating to Ukraine, the annexation of Crimea, the occupation of South Ossetia and Abkhazia; on persons engaged in specified acts with respect to the development and production of petroleum and natural gas resources, pipelines and civil nuclear projects in the Russian Federation; on persons who facilitate the issuance of sovereign debit of the Russian Federation; on persons who invest or facilitate the privatisation of state-owned assets by the Russian Federation; or persons engaged in recognised human rights abuses:
  - Restrict/limit Export-Import Bank Assistance and licensing (or other permission) for exports;
  - Prohibit/discourage loans from domestic international financial institutions;
  - Prohibit transfers of credit or payments between financial institutions;
  - Prohibit/restrict transactions relating to designated property;
  - Prohibit designated financial institutions from acting as a primary dealer of United States Government debt instruments or as a repository of United States Government funds;
  - Prohibit procurement contracts with the United States Government;
  - Prohibit transactions in foreign exchange subject to the jurisdiction of the United States;
  - Prohibit investment in equity or debt;
  - Exclusion of designated corporate officers from the United States; and
  - Imposition of aforementioned sanctions on principal executive officers or persons performing similar functions and with similar authorities.

The CRHA also addressed corrupt practices committed by Russia in Europe and Eurasia to exert malign influence and undermine democratic institutions and European unity.

Pursuant to CRHA, notification(s) of termination(s) of sanctions must be submitted by the President to the chairperson and ranking member of the appropriate congressional committee. Termination of sanctions under CRHA may occur only upon submission of a certification that the Government of the Russian Federation has done the following:

- Ceased cyber-attacks against United States officials and unofficial entities;
- Ceased ordering, controlling or otherwise directing, supporting or financing significant acts intended to undermine the peace, security, stability, sovereignty or territorial integrity of Ukraine; or
- Halted military operations in Syria.

1116. Were additional sanctions proposed against Russia for their alleged cybersecurity activities and other corrupt acts?

Introduced by the U.S. Senate in March 2017, and passed in June 2017, the Countering Iran's Destabilising Activities of 2017 called for the development of a regional strategy to counter Iranian threats in the Middle East and North Africa and the imposition of sanctions with respect to Iran's ballistic missile program, among other actions. Title II called for the following with respect to Russia:

- Codification of sanctions relation to the Russian Federations
- Modification of implementation of Executive Order 13662 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine
- Imposition of sanctions with respect to:
    - Activities of the Russian Federation undermining cybersecurity
    - Transfer of arms and related material to Syria
    - Special Russian crude oil projects
    - Development of pipelines in the Russian Federation
    - Investment in or facilitation of the privatisation of state-owned assets by the Russian Federation
    - Significant corruption in the Russian Federation
    - Russian and other foreign financial institutions
    - Persons engaging with the intelligence or defence sectors of the Government of the Russian Federation
    - Foreign sanctions evaders
    - Human rights abuses

In May 2017, the U.S. Senate introduced Countering Russian Influence in Europe and Eurasia Act of 2017, which acknowledged the Russian Government's attempt to exert influence by "providing resources to political parties, think tanks and civil society groups [to] sow distrust in democratic institutions," disseminating anti-Western disinformation, violating previous agreements in other regions (e.g., Ukraine, Georgia) and other corrupt practices.

Somalian Sanctions Program Overview

1117. What are the major U.S. government sanctions programs affecting Somalia?

The U.S. government has imposed numerous sanctions on the Federal Republic of Somalia, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)

- **United Nations Participation Act (UNPA)** (1945; amended by the United Nations Participation Act, 1949)
- **Executive Order 13536 – Blocking Property of Certain Persons Contributing to the Conflict in Somalia** (2010)
- **Executive Order 13620- Taking Additional Steps to Address the National Emergency With Respect to Somalia** (2012)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Somalia:

- **UNSCR 733** (1992)
- **UNSCR 1356** (2001)
- **UNSCR 1725** (2006)
- **UNSCR 1744** (2007)
- **UNSCR 1772** (2007)
- **UNSCR 1816** (2008)
- **UNSCR 1844** (2008)
- **UNSCR 1846** (2008)
- **UNSCR 1851** (2008)
- **UNSCR 1872** (2009)
- **UNSCR 1897** (2009)

The following regulation implements Somalia sanctions:

- **31 C.F.R. Part 551 – Somalia Sanctions Regulations**

1118. What are the primary objectives of OFAC Sanctions Programs affecting Somalia?

The primary objectives of the U.S. government with respect to Somalia sanctions are to restrict and eliminate violent acts which are the subject of United Nation Security Resolutions (UNSR) (e.g., acts of piracy and armed robbery at sea), violence against Somalian citizens, export of charcoal that funds terrorist activity and misappropriation of public assets of Somalia.

According to OFAC's Somalia Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Acts that threaten the Djibouti Agreement of August 18, 2008 or the political process including, but not limited to, the following:
  - Transitional Federal Institutions;
  - Future Somali governing institutions; or

  - African Union Mission in Somalia (AMISOM);
  - Other future international peacekeeping operations related to Somalia; or
  - Misappropriation of Somali public assets.
- Obstruction of the delivery, access or distribution of humanitarian assistance to Somalia;
- Having supplied, sold or transferred to Somalia or to have been the recipient in the territory of Somalia of arms or any related material, technical advice, training or assistance, including financing and financial assistance, related to military activities;
- Ordering, controlling or directing or participated in the commission of acts of violence targeting Somalian citizens (e.g., killing, maiming, sexual and gender-based violence, attacks on schools, hospitals, taking hostages, forced displacement);
- Being a political or military leader recruiting or using children in conflict in Somalia;
- The import or export of charcoal into/out of Somalia on or after February 22, 2012;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned activities; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Somalian Sanctions Program.

1119. Where can one find a list of designated entities under Somalia Sanctions Program?

Designations are maintained in the appendices of Somalia regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [SOMALIA].

1120. What action must institutions take if a positive "hit" is identified for the Somalia Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Sudanese Sanctions Program Overview

1121. What are the major U.S. government sanctions programs affecting Sudan?

The U.S. government has imposed numerous sanctions on the Republic of Sudan, including those mandated by the following statutes and executive orders:

- **United Nations Participation Act (UNPA), Section 5** (1945)
- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)

- **Antiterrorism and Effective Death Penalty Act of 1996** (AEDPA) (1996)
- **Trade Sanctions Reforms and Export Enhancement Act of 2000 (TSRA)** (2000)
- **Darfur Peace and Accountability Act of 2006 (DPAA)** (2006)
- **Executive Order 13067 – Blocking Sudanese Government Property and Prohibiting Transactions With Sudan** (1997)
- **Executive Order 13400 – Blocking Property of Persons in Connection with the Conflict in Sudan's Darfur Region** (2006)
- **Executive Order 13412 – Blocking Property and Prohibiting Transactions with the Government of Sudan** (2006)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Sudan:

- **UNSCR 1591** (2005)
- **UNSCR 1672** (2006)

The following regulations implement Sudan sanctions:

- **31 C.F.R. Part 538 – Sudanese Sanctions Regulations**
- **31 C.F.R. Part 538 – Darfur Sanctions Regulations**

As of January 2017, the U.S. terminated the Sudanese Sanctions Program.

1122. What were the primary objectives of OFAC Sanctions Programs affecting Sudan?

The primary objectives of the U.S. government with respect to Sudanese sanctions were to restrict and eliminate Sudanese support of international terrorism and human rights violations (e.g., slavery, denial of religious freedom, gender-based sexual violence) of Sudanese citizens. Subsequent Executive Orders narrowed the scope of Sudanese sanctions by eliminating the Republic of South Sudan, recognised as independent from Sudan on July 2011, and exempting the following regions from certain sanctions:

- Kordofan/Nuba Mountains State
- Blue Nile State
- Abyei
- Darfur
- Certain areas around Khartoum

All property and interests of the Government of Sudan were blocked. Additionally, according to OFAC's Sudan Sanctions Program overview, designees were identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following acts contributing to the conflict in Darfur:

- Threatened the peace process in Darfur;
- Threatened the stability of Darfur and the region;
- Responsible for conduct related to the conflict in Darfur that violates international law;
- Responsible for heinous conduct with respect to human life or limb related to the conflict in Darfur;
- Directly or indirectly, supplied, sold or transferred arms or any related material, assistance, advice or training related to military activities of the following:
    - Government of Sudan
    - Sudan Liberation Movement/Army
    - Justice and Equality Movement
    - Janjaweed
    - Any person operating in the states of North Darfur, South Darfur or West Darfur that is a belligerent, a nongovernmental entity or an individual
- Responsible for offensive military overflights in and over the Darfur region;
- Materially assisted, sponsored or provided financial, material or technological support for, or goods or services in support of, the aforementioned activities; or
- Owned, controlled by or acting or purporting to act for or on behalf of, directly or indirectly, any person listed or designated in the Sudanese Sanctions Program.

Pursuant to those objectives, OFAC implemented a full-scale country embargo involving Sudan, including broad prohibitions on U.S. persons importing or exporting goods and services to or from Sudan. While the United States lifted these sanctions in January 2017, it did so only as long as the Government of Sudan sustains the positive actions that it had taken in the six months prior to January 2017, as judged by the United States. That is, the United States may re-impose the Sudanese sanctions if the Sudanese Government does not sustain those positive actions.

Finally, due to the interdependence between Sudan and South Sudan, certain activities of the Republic of South Sudan continued to be subject to Sudanese sanctions. For further guidance on sanctions affecting South Sudan, please refer to the South Sudanese Sanctions Overview.

1123. Where can one find a list of designated entities under the Sudanese Sanctions Program?

Designations were maintained in the appendices of Sudanese regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tags [SUDAN] and [DARFUR].

1124. What action must institutions take if a positive "hit" is identified for the Sudanese Sanctions Program?

When active, institutions were obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

South Sudanese Sanctions Program Overview

1125. What are the major U.S. government sanctions programs affecting South Sudan?

The U.S. government has imposed numerous sanctions on South Sudan, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 13664 – Blocking Property of Certain Persons with Respect to South Sudan** (2014)

The following regulation implements South Sudanese sanctions:

- **31 C.F.R. Part 558 – South Sudan Sanctions Regulations**

1126. What are the primary objectives of OFAC Sanctions Programs affecting South Sudan?

The primary objectives of the U.S. government with respect to South Sudanese sanctions are to restrict and eliminate the widespread violence and human rights abuses against South Sudanese citizens, recruitment and use of child soldiers, attacks on peacekeepers and the obstruction of humanitarian operations in South Sudan. As of July 2011, the Republic of South Sudan was recognised as independent from Sudan, but due to the interdependence between certain sectors of their economies, certain activities are still subject to Sudanese sanctions.

According to OFAC's South Sudan Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions or policies that threaten the peace, security or stability of South Sudan;
- Actions or policies that threaten transitional agreements or undermine democratic processes or institutions in South Sudan;
- Actions or policies that have the purpose or effect of expanding or extending the conflict in South Sudan or obstructing reconciliation or peace talks or processes;
- Commission of human rights abuses against persons in South Sudan;

- Targeting of women, children or any civilian through the commission of acts of violence (e.g., killing, maiming, torture, rape), abduction or forced displacement that would constitute a serious abuse or violation of human rights or a violation of international humanitarian law;
- Attacks on schools, hospitals, religious sites or locations where civilians are seeking refuge;
- The use or recruitment of children by armed groups or armed forces in the context of the conflict in South Sudan;
- Obstruction of activities of international peacekeeping, diplomatic or humanitarian missions in South Sudan or the delivery, distribution or access to humanitarian assistance;
- Attacks against United Nations missions, international security presences or peacekeeping operations;
- Being a leader of an entity (e.g., government, rebel militia) that has or whose members have engaged in any of the aforementioned acts;
- Materially assisting, sponsoring or providing financial, material or technological support for, or goods or services to or in support of the aforementioned activities; or
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the South Sudanese Sanctions Program.

For further guidance on Sudanese sanctions, please refer to the Sudanese Sanctions Program Overview section.

1127. Where can one find a list of designated entities under the South Sudanese Sanctions Program?

Designations are maintained in the appendices of South Sudanese regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [SOUTH SUDAN].

1128. What action must institutions take if a positive "hit" is identified for the South Sudanese Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Venezuelan Sanctions Program Overview

1129. What are the major U.S. governments sanctions programs affecting Venezuela?

The U.S. government has imposed numerous sanctions on the Bolivarian Republic of Venezuela, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)

- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Immigration and Nationality Act of 1952** (1952)
- **Venezuela Defense of Human Rights and Civil Society Act of 2014** (2014)
- **Executive Order 13692 – Blocking Property and Suspending Entry of Certain Persons Contributing to the Situation in Venezuela** (2015)

The following regulation implements Venezuelan sanctions:

- **31 C.F.R. Part 591 – Venezuela Sanctions Regulations**

1130. What are the primary objectives of OFAC Sanctions Programs affecting Venezuela?

The primary objectives of the U.S. government with respect to the Venezuela are to restrict and eliminate:

- The erosion of human rights guarantees;
- Persecution of political opponents;
- Curtailment of press freedoms;
- Use of violence and human rights violations in response to anti-government protests;
- Arbitrary arrests and detention of anti-government protestors; and
- Public corruption.

According to Executive Order 13692, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Actions or policies that undermine democratic processes or institutions;
- Significant acts of violence or conduct that constitutes a serious abuse or violation of human rights, including against persons involved in anti-government protests in Venezuela in or since February 2014;
- Actions that prohibit, limit or penalise the exercise of freedom of expression or peaceful assembly;
- Public corruption by senior officials within the Government of Venezuela;
- Being a current or former leader of an entity that has or whose members have engaged in the aforementioned activities;
- Being a current of former official of the Government of Venezuela;
- Materially assisting, sponsoring or providing financial, material or technological support for goods or services to or in support of the aforementioned activities;
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Venezuelan Sanctions Program.

1131. Where can one find a list of designated entities under the Venezuelan Sanctions Program?

Designations are maintained in the appendices of Venezuelan regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [VENEZUELA].

1132. What action must institutions take if a positive "hit" is identified for the Venezuelan Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Yemeni Sanctions Program Overview

1133. What are the major U.S. government sanctions programs affecting Yemen?

The U.S. government has imposed sanctions on the Republic of Yemen, including those mandated by the following statutes and executive orders:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 13611 – Blocking Property of Persons Threatening the Peace, Security or Stability of Yemen** (2012)

The following United Nations Security Council Resolutions (UNSCR) have been issued with respect to Yemen:

- **UNSCR 2140** (2014)
- **UNSCR 2201** (2015)
- **UNSCR 2204** (2015)
- **UNSCR 2216** (2015)

The following regulation implements Yemeni sanctions:

- **31 C.F.R. Part 552 – Yemen Sanctions Regulations**

1134. What are the primary objectives of OFAC Sanctions Programs affecting Yemen?

The primary objectives of the U.S. government with respect to Yemen sanctions are to restrict and eliminate obstructions to the political process that threaten the peace, security and stability of Yemen.

According to Executive Order 13611, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Acts that directly or indirectly threaten the peace, security or stability of Yemen (e.g., obstructions to the November 23, 2011 agreement between the Government of Yemen and those in opposition to it, which provides for a peaceful transition of power in Yemen) or that obstruct the political process in Yemen;
- Being a political or military leader of an entity that has engaged in the aforementioned acts;
- Materially assisting, sponsoring or providing financial, material or technological support for or goods or services to or in support of the aforementioned acts
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Yemen Sanctions Program.

1135. Where can one find a list of designated entities under the Yemen Sanctions Program?

Designations are maintained in the appendices of Yemen regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [YEMEN].

1136. What action must institutions take if a positive "hit" is identified for the Yemen Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Zimbabwe Sanctions Program Overview

1137. What are the major U.S. government sanctions programs affecting Zimbabwe?

The U.S. government has imposed numerous sanctions on the Republic of Zimbabwe, including those mandated by the following statutes and executive orders, which are listed in chronological order:

- **National Emergencies Act (NEA)** (1976)
- **International Emergency Economic Powers Act (IEEPA)** (1977)
- **Executive Order 13288 – Blocking Property of Persons Undermining Democratic Processes or Institutions in Zimbabwe** (2003)
- **Executive Order 13391 – Blocking Property of Additional Persons Undermining Democratic Processes or Institutions in Zimbabwe** (2005)
- **Executive Order 13469 – Blocking Property of Additional Persons Undermining Democratic Processes or Institutions in Zimbabwe** (2008)

The following regulation implements Zimbabwe sanctions:

- **31 C.F.R. Part 541 – Zimbabwe Sanctions Regulations**

1138. What are the primary objectives of OFAC Sanctions Programs affecting Zimbabwe?

The primary objectives of the U.S. government with respect to Zimbabwe sanctions are to restrict and eliminate actions of certain persons who continually undermined the democratic processes and institutions of Zimbabwe.

According to OFAC's Zimbabwe Sanctions Program overview, designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following:

- Being a senior official of the Government of Zimbabwe;
- Being owned or controlled by, directly or indirectly, the Government of Zimbabwe or an official or officials of the Government of Zimbabwe;
- Engaging in actions or policies to undermine Zimbabwe's democratic processes or institutions;
- Responsible for or having participated in human rights abuses related to political repression in Zimbabwe;
- Engaging in activities facilitating public corruption by senior officials of the Government of Zimbabwe;
- Being a spouse or dependent child of any person whose property and interests in property are blocked pursuant to the Zimbabwe Sanctions Program;
- Materially assisting, sponsoring or providing financial, material or technological support for or goods or services to or in support of the aforementioned acts;
- Owning or controlling property or interests, acting or purporting to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Zimbabwe Sanctions Program.

1139. Where can one find a list of designated entities under Zimbabwe Sanctions Program?

Designations are maintained in the appendices of Zimbabwe regulations and on the Specially Designated Nationals (SDN) List administered by OFAC with the program tag [ZIMBABWE].

1140. What action must institutions take if a positive "hit" is identified for the Zimbabwe Sanctions Program?

Institutions are obligated to block or reject a transaction, depending on the requirements of the specific sanctions program involved, and file a Blocked or Rejected Transaction Report with OFAC. For guidance, contact OFAC. For additional guidance, please refer to the sections: Investigating Potential Matches and OFAC Reporting Requirements.

Other U.S. and International Sanctions Programs

1141. Should institutions include other U.S. sanctions program lists as part of their OFAC Compliance Programs?

U.S. government agencies, such as the U.S. Department of the Treasury, the U.S. Bureau of Industry and Security (BIS), the U.S. Department of Commerce, the U.S. Department of Labor and the U.S. State Department, have independent prohibitions on transactions with certain individuals or entities beyond those included in OFAC Sanctions Listings, including, but not limited to, the following:

- **Denied Persons List (DPL)** – A list of individuals and entities that have been denied export privileges that is administered by the Bureau of Industry and Security (BIS). No exporter may participate in an export or re-export transaction involving items subject to the Export Administration Regulations (EAR) with a person or entity whose export privilege has been denied by the BIS.
- **Unverified List** – A list of names and countries of foreign persons who in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check or a post shipment verification for reasons outside of the U.S. government's control. The presence of a party on this list in a transaction is a red flag that should be resolved before proceeding with the transaction.
- **The Entity List** – A list of names of certain foreign parties that are prohibited from receiving items subject to the EAR unless the exporter obtains a license that is administered by BIS. The Entity List can include businesses, research institutions, government and private organisations, individuals and other types of legal persons who are subject to specific license requirements for the export, re-export and/or transfer (in-country) of specified items.
- **The AECA Debarred List** – A list of names of persons who have been convicted of violations in court (or conspiracy to violate) (statutory debarment) or have violated (or conspired to violate) the Arms Export Control Act of 1976 (AECA) during an administrative proceeding (administrative debarment).
- **BIS General Orders** – A list of persons and businesses with restricted export privileges administered by the Department of Commerce.

Persons on the aforementioned lists are included generally due to concerns with export privileges and licensing and may not be subject to sanctions, unlike those designated on the SDN List.

Institutions that operate internationally also should consider other sanctions lists as part of an OFAC Compliance Program. This would depend on the institution's internal risk assessment.

1142. What is the Consolidated Screening List, and who should screen against it?

The Consolidated Screening List consolidates export screening lists administered by the Departments of Commerce, State and Treasury to use as an aid to detect prohibited parties and/or activities in export transactions. The Consolidated Screening List includes the following:

- Denied Persons List (Department of Commerce)

- Unverified List (Department of Commerce)
- Entity List (Department of Commerce)
- Nonproliferation Sanctions List (Department of State)
- AECA Debarred List (Department of State)
- Specially Designated Nationals and Blocked Persons List (SDN List) (Department of the Treasury, OFAC)
- Foreign Sanctions Evaders List (FSE List) (Department of the Treasury, OFAC)
- Sectoral Sanctions Identifications (SSI) List (Department of the Treasury, OFAC)
- Palestinian Legislative Council (PLC) List (Department of the Treasury, OFAC)
- The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List) (Department of the Treasury, OFAC)
- Non-SDN Iranian Sanctions Act List (NS-ISA) (Department of the Treasury, OFAC)

Exporters and importers should screen against the Consolidated Screening List. Financial institutions with a significant customer population of exporters and importers may consider incorporating the Consolidated Screening List into their overall OFAC Compliance Programs.

1143. Is the Consolidated Screening List the same as OFAC's Consolidated Sanctions List?

No. The Department of Commerce administers the Consolidated Screening List, which is separate from OFAC's Consolidated Sanctions List. Although designees may overlap, the lists are independent of each other.

1144. What are "antiboycott laws," and which agency is responsible for administering and enforcing them?

According to the BIS' Office of Antiboycott Compliance (OAC), antiboycott laws refers to the "1977 amendments to the Export Administration Act (EAA) and the Ribicoff Amendment to the 1976 Tax Reform Act (TRA)" that sought to "counteract the participation of U.S. citizens in other nation's economic boycotts or embargoes" (e.g., Arab League boycott of Israel) by prohibiting the following:

- "Agreements to refuse or actual refusal to do business with or in Israel or with blacklisted companies.
- Agreements to discriminate or actual discrimination against other persons based on race, religion, sex, national origin or nationality.
- Agreements to furnish or actual furnishing of information about business relationships with or in Israel or with blacklisted companies.
- Agreements to furnish or actual furnishing of information about the race, religion, sex, or national origin of another person."

Antiboycott laws essentially prevent "U.S. firms from being used to implement foreign policies of other nations which run counter to U.S. policy."

The OAC office of the BIS administers and enforces antiboycott laws by requiring U.S. firms to report receipts of boycott requests (e.g., through quarterly reports, tax returns) and violations of antiboycott laws through voluntary self-disclosure).

1145. Are sanctions lists maintained by jurisdictions and bodies other than OFAC?

There are several sanctions lists maintained by other countries that include, but are not limited to, the following:

- **U.N. Consolidated Lists:** The Security Council of the United Nations is empowered to take enforcement measures to maintain or restore international peace and security under Chapter VII of its charter. One such enforcement measure is the imposition of sanctions, including economic and trade sanctions, arms embargoes, travel bans, and other financial or diplomatic restrictions. The Security Council has imposed sanctions on individuals and organisations through a variety of resolutions; each list is maintained by the relevant Security Council Committee. Examples include the Al-Qaida Sanctions List, Taliban Sanctions Lists, Resolutions related to the proliferation of weapons of mass destruction (WMDs).
- **Bank of England (BOE) List:** The BOE, the central bank of the United Kingdom, publishes lists of individuals and organisations against which financial sanctions have been imposed.
- **Australian Department of Foreign Affairs and Trade (DFAT) List:** The purpose of this list is to freeze assets of terrorists by making it a criminal offense for persons to hold, use or deal with assets that are owned or controlled by persons or entities on the list.
- **European Union (EU) Consolidated List:** The EU maintains a list of persons, groups and entities subject to Common Foreign Security Policy-related financial sanctions.
- **The Hong Kong Monetary Authority (HKMA) List:** Institutions that find they have done business with individuals or entities on the HKMA List are required to report such activity to the HKMA and Hong Kong's Joint Financial Intelligence Unit (JFIU).
- **Monetary Authority of Singapore (MAS) List:** The MAS issues a list of individuals who and organisations that have been sanctioned by the government of Singapore. Dealing with any of those cited on the MAS List can lead to fines, criminal penalties and increased regulatory scrutiny for financial institutions operating in that country.
- **New Zealand Police (NZP) List:** The NZP maintains the list of terrorist entities designated by the UN Security Council Regulations against the Taliban and al-Qaida, as well as those designated under the Terrorism Suppression Act 2002.
- **Canadian Government's Office of the Superintendent of Financial Institutions (OSFI) List:** Regulations mandate that every Canadian financial institution and foreign branch operating in Canada review their records on a continuing basis for the names of individuals listed in OSFI's Schedule to the Regulations.

- **Reserve Bank of Australia (RBA) List:** The RBA administers sanctions as specified in the Banking (Foreign Relations) Regulations 1959. The responsibility of DFAT is to maintain and publish the Australian government's list of terrorists and their sponsors, those in the former Iraqi regime, and the sanctions lists of those in the former government of the Federal Republic of Yugoslavia, ministers and senior officials of the government of Zimbabwe, and entities associated with the Democratic People's Republic of Korea (North Korea).

1146. Is there overlap between these international sanctions lists and the OFAC Sanctions Listings?

As international efforts to combat drug trafficking, terrorism and the proliferation of WMDs continue to converge, there may be significant overlap between the sanctions lists maintained by different countries, especially by those countries that have ratified the same international instruments to combat transnational crimes.

Screening Customers and Transactions

Basics

1147. What parties, activities and transactions are subject to OFAC sanctions?

All activities, including all trade or financial transactions, regardless of the amount, and all relationships, whether direct or indirect (e.g., customer, noncustomer), are subject to OFAC sanctions. This includes, but is not limited to, the following:

- **Account types:** deposits, loans, trusts, safety deposit boxes;
- **Transaction types:** wire transfers, ACH transfers, letters of credit, currency exchanges, deposited/cashed checks, purchases of monetary instruments, loan payments, security trades, retail purchases; and
- **Individuals/entities:** account holders, authorised signers, guarantors, collateral owners, beneficiaries, nominee shareholders, noncustomers, employees, vendors.

It is important to note that persons who are not listed on OFAC Sanctions Listings can also be subject to sanctions if they provide material assistance to a designated target or assist the target to evade OFAC sanctions.

As a practical matter, however, institutions must decide, based on their assessment of OFAC compliance risk, which parties, activities and transactions will be screened against the OFAC Sanctions Listings, as well as how often, since 100 percent screening is not a viable option for most institutions. For further guidance on screening, please refer to the sections: Screening Customers and Transactions and Interdiction Software.

1148. When should customers be screened against the OFAC Sanctions Listings?

Customers should be screened under several circumstances. Examples include, but are not limited to, before account opening (although some institutions screen at the end of the day and choose to take the

risk), upon changes to the existing information (e.g., amendments to beneficiaries, signers, change of address), entire existing customer population periodically (frequency based on OFAC risk assessment) and upon distribution of funds (e.g., incoming/outgoing wire transfers, payees on monetary instruments).

1149. Is a financial institution in violation of OFAC regulations if it establishes an account for an SDN designee?

Opening an account for an SDN designee is considered the provision of a prohibited service and is subject to sanctions. Accordingly, if a financial institution does not conduct OFAC screening before the opening of an account, it is taking a risk and thus the financial institution should implement controls on the account to ensure transactions are not conducted until the customer has been screened against OFAC Sanctions Listings to ensure that, if required, any funds obtained by the financial institution are appropriately blocked.

1150. How often should an institution's existing customer base be checked against the continuously updated OFAC Sanctions Listings?

The existing customer base should, ideally, be checked against the OFAC Sanctions Listings at each update. If this is not possible, the frequency of OFAC screens should be based on the institution's risk profile, recognising that as soon as a name is added to the OFAC Sanctions Listings, OFAC expects compliance. If the institution fails to identify and block/reject a transaction/trade conducted by an individual or entity on the OFAC Sanctions Listings, consequences can include enforcement actions and negative publicity.

1151. Should the names of account parties (e.g., beneficiaries) who are not account holders be included in the OFAC screening process?

Yes. Account parties who are not account holders (e.g., beneficiaries, guarantors, principals, beneficial owners, nominee shareholders, directors, signatories and powers of attorney) should be screened for possible matches. However, the extent to which an institution can include these account parties will depend on the institution's risk profile, CIP, KYC programs and available technology.

Since account beneficiaries have a "property interest" in products, financial institutions should screen account beneficiaries upon account opening, while updating account information, when performing periodic screening and upon disbursing funds. Beneficiaries include, but are not limited to, trustees, children, spouses, nonspouses, entities and powers of attorney.

1152. Since many financial institutions perform OFAC screens post account opening, are they in violation if the next-day verification results in a positive "hit"?

If an institution is aware that a potential customer is on the OFAC Sanctions Listings, it is prohibited from opening the account.

If the account is already open, the important thing is not to allow any transactions to be conducted. If an initial deposit was made in the account of a positive match to the OFAC Sanctions Listings, the institution is obligated to freeze/reject the assets.

1153. Do OFAC regulations apply only to accounts of and transactions by those customers that transact business through the institution?

No. OFAC regulations apply to all financial transactions performed or attempted by a financial institution, and this would include, for example, transactions of noncustomers, payments made to vendors and compensation paid to employees. However, the extent to which an institution includes such parties in its screening process will depend on the institution's risk profile and available technology.

1154. If a transaction is sent and/or received on behalf of a third party, should the institution include the third party in its OFAC screening process?

Yes. If the institution is aware that the transaction is being sent or received on behalf of a third party, it should include the third party in its OFAC screening process.

1155. Does an institution need to check the OFAC Sanctions Listings when selling cashier's checks and money orders?

In theory, every transaction and every activity that a U.S. institution engages in is potentially subject to OFAC sanctions. If an institution knows or has reason to know that a target is party to a transaction, the institution's processing of the transaction would be unlawful. However, a financial institution, depending upon its risk profile and available technology, may decide to screen only some cashier's checks and money orders (e.g., higher-dollar thresholds).

1156. In the instance of a wire transfer, if a "hit" is found after the payment has been completed, who has ultimate liability?

Each U.S. person who handled or permitted the transaction may be found to have violated the sanctions program. For example, the originating financial institution, the correspondent bank and the beneficiary bank could each be fined by OFAC.

1157. Is an institution obligated to report a possible match with the name of someone who is not a customer of the financial institution (e.g., beneficiary of a funds transfer originated by its own customer)?

Yes. After a diligent effort is made to rule out a false hit, which may include a call to OFAC to discuss whether the name of the possible match is a party subject to the sanctions, the institution should report the hit regardless of its relationship with the individual or entity in question.

1158. If a loan is approved but involves a true OFAC "hit" on the Sanctions Listings, what should the customer be told as a denial reason?

If a true OFAC "hit" is confirmed, there is no reason not to explain the reason for the blocked/rejected transaction to the customer. The customer can contact OFAC directly for further information.

1159. How should institutions screen information not maintained in an electronic format?

Unless previous authorisation was granted by OFAC or exclusion is expressly exempted by statute, all customers and other account/transaction party names should be screened, regardless of the form in which the information is maintained. The scope and frequency of the screenings should be based on the institution's risk profile and available technology. For example, a possible risk-based approach could include screening payees of checks greater than US$10,000.

1160. Can an individual send money to a sanctioned country using a third-country company's website?

Although a website may say it is permissible to send funds to a sanctioned country, it would be in violation of OFAC laws and regulations to do something indirectly that is not permissible to do directly. The use of websites by U.S. persons who may be used to facilitate unauthorised transactions would be a violation of U.S. law.

1161. How can institutions effectively screen customers and transactions against multiple sanctions lists?

Many institutions use interdiction software to screen customers and transactions against multiple lists simultaneously. For additional guidance on the various types of software available, please refer to the AML/CFT Technology, KYC Process and Customer and Transaction List Screening sections.

1162. What does "stripping" mean?

"Stripping" is when information is removed from payment information in order to prevent the funds transfer from being blocked or rejected when being screened for possible sanctions violations.

1163. What steps can financial institutions take to mitigate the risks of stripping?

To mitigate the risks associated with "stripping," a financial institution can do the following:

- Implement a stringent OFAC training program that includes OFAC requirements and the penalties for noncompliance for all branches and operations, both foreign and domestic.
- Implement a review process of potential OFAC hits to ensure wires were not "stripped."
- Implement a review process of funds transfers with the same sender/amount coming back in a short time.

Cover Payments

1164. What are cover payments?

"Cover payments" are used in correspondent banking as a cost effective method of sending international transactions on behalf of customers. A cover payment involves several actions by financial institutions:

- Obtaining a payment order from the customer;

- Sending of a credit transfer message for an aggregate amount through a messaging network (e.g., Society for Worldwide Interbank Financial Telecommunication [SWIFT]) that travels a direct route from the originating bank to the ultimate beneficiary's bank;
- Execution of a funds transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message; and
- Disbursement of funds to the ultimate beneficiary in accordance with the credit transfer message.

1165. What challenges have cover payments posed?

Previous messaging standards did not include information on the ultimate originators and beneficiaries of cover payments. The lack of information posed a challenge for recordkeeping, suspicious activity monitoring and sanctions screening.

1166. What is SWIFT's role in the international payments system?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) is the infrastructure supporting both global correspondent banking and most domestic payment systems and Real-Time Gross Settlement (RTGS) networks involving over 11,000 financial institutions (e.g., banks, broker-dealers, investment managers) in more than 200 countries and territories. Participants also include corporate as well as market infrastructures (settlement and clearing organisations) in payments, securities, treasury and trade.

Message types (MTs) are used to transmit financial information and instructions from one participating financial institution to another, also referred to as SWIFT FIN messages.

Oversight is provided by central banks including the National Bank of Belgium, the Bank of England, the Bank of Japan and the U.S. Federal Reserve.

For further guidance on SWIFT, please refer to the Cover Payments and SWIFT section.

1167. What enhancements were made to SWIFT's messaging with regard to cover payments?

MT 202s were often used in lieu of the MT 103s, in part, because MT 202s were more cost-effective. Regardless of the reason, however, the substitution of an MT 202 for an MT 103 in a commercial transaction masked the underlying parties to a transaction, thereby frustrating attempts to comply with recordkeeping, monitoring and sanctions requirements.

To address this lack of transparency, in 2009, SWIFT developed a variant of the MT 202 payment message type, MT 202 COV, which allows all information contained in certain fields (e.g., originator and beneficiary information) of the MT 103 to be transmitted in the MT 202 COV and is to be used for cover payments in lieu of MT 202s. The MT 202 COV provides intermediary banks with additional originator and beneficiary information to perform sanctions screening and suspicious activity monitoring.

To further improve efficiency and transparency of cross-border payments, SWIFT developed a global payments innovation (GPI), a cloud-based payments tracking service that allows correspondents to see

payments end-to-end throughout all legs of the transaction and meet regulatory requirements (e.g., KYC rules, sanctions screening, audit requests).

1168. How can SWIFT messages be used to support sanctions screening?

SWIFT messages contain payment information such as originators, intermediate beneficiaries, ultimate beneficiaries and multiple banks involved in the transfers. It is important that these fields be screened against sanctions lists (e.g., OFAC Sanctions Listings, U.N. Consolidated Lists).

For further guidance on screening software, please refer to the AML/CFT Technology section.

1169. Do all SWIFT messages need to be screened as part of a sanctions program?

When implementing a risk-based sanctions compliance program, financial institutions may elect to include only SWIFT messages that constitute payment instructions. For example the message MT 950 Statement Message provides balance and transaction details of an account to the account owner and is widely used for account reconciliation within a bank, but does not constitute a payment instruction.

The decision to limit SWIFT messages may be restricted by the type of screening system used by a financial institution. For example, some systems have the ability to screen all messages, while others can only screen those messages that constitute payment instructions.

1170. How are SWIFT messages used by the U.S. Department of Treasury to combat terrorist financing?

Following the terrorist activity on September 11, 2001, the U.S. Department of Treasury established the Terrorist Finance Tracking Program (TFTP) to identify, track and pursue terrorists by conducting targeted searches on data provided by SWIFT. The U.S. Department of Treasury submits subpoenas to the U.S. and European operating centres of SWIFT for financial messaging data related to specific terrorism investigations.

For further guidance on counter-terrorism efforts, please refer to the Counter-Terrorism Sanctions Programs section.

1171. Is the TFTP limited to SWIFT messages from U.S. financial institutions?

No. In 2010, the United States and the European Union signed an international agreement authorising the transfer of financial messaging data from SWIFT's European operating centre to the U.S. Department of Treasury specifically for counter-terrorism efforts.

1172. Are all SWIFT messages made available to the TFTP?

No. SWIFT provides messages requested through a subpoena from the U.S. Department of Treasury.

However, in 2010, FinCEN issued a proposed rule that would impose additional reporting requirements of transmittal orders (e.g., SWIFT messages) associated with "cross-border electronic transmittals of funds" (CBETFs). For further guidance, please refer to the Cross-Border Electronic Transmittal of Funds section below.

U-Turn Payments

1173. What is a "U-Turn payment"?

A "U-Turn payment" is a payment originating at a non-U.S. bank going through a U.S. bank destined for a payment to another non-U.S. bank, provided the payments do not directly credit or debit a sanctioned account holder (e.g., an account of a person/business who is a designee on the SDN List). The originator, beneficiary, originating bank or beneficiary bank could all be from the sanctioned country (e.g., Iran, Cuba) as long as there are third-country banks on both sides of the transaction.

1174. What is the purpose of a U-Turn payment?

For many years, OFAC, under Iranian Sanctions and Cuban Sanctions, prohibited U.S. financial institutions from directly sending funds to Iran and Cuba, but allowed U-Turn payments in some instances. A U-Turn payment is designed to allow international financial institutions, in the wake of heavy economic sanctions against certain countries (e.g., Iran, Cuba), to still clear payments through their U.S. correspondent accounts under limited circumstances.

1175. Are U-Turn payments allowed under the Iranian Sanctions Program?

As of November 10, 2008, Iranian U-Turn payments are no longer allowed.

1176. What are the limited circumstances that make U-Turn Payments permissible under the Cuban Sanctions Program?

As of March 16, 2016, Cuban U-Turn payments are permissible provided that neither the originator nor the beneficiary is a person subject to OFAC sanctions.

Automated Clearing House Transactions and IATs

1177. Are Automated Clearing House (ACH) transactions subject to OFAC sanctions?

Yes. ACH transactions, just as is the case with all other financial transactions, are subject to OFAC sanctions. With the growth in ACH transactions going beyond direct deposits of payroll, government benefits and consumer bill payments to include one-time debits and check conversions, which can include cross-border transactions, the overall OFAC compliance risk associated with ACH transactions has increased.

1178. Which participants in an ACH transaction are subject to OFAC sanctions?

All ACH participants, including originators, originating depository financial institutions (ODFIs), receiving depository financial institutions (RDFIs), receivers, ACH operators and third-party service processors are subject to OFAC sanctions. ACH participants generally include the following:

- An originator is an organisation or person that/who initiates an ACH transaction, either as a debit or credit.
- An ODFI is the originator's depository financial institution that initiates the ACH transaction into the ACH network at the request of and by agreement with its customers.

- An RDFI is the receiver's depository institution that receives the ACH transaction from the ACH operators (which may be the ODFI, another bank or a third party) and credits or debits funds to or from their receiver's accounts.
- A receiver is a person, corporation or other entity who has authorised the originator to initiate an ACH transaction, either as a debit or credit to an account held at the RDFI.
- An ACH operator processes ACH transactions that flow between different financial institutions and serves as a clearing facility that receives entries from the ODFIs and distributes the entries to the appropriate RDFI (e.g., Fed ACH, Electronic Payments Network [EPN]).
- A third-party service provider (TPSP) is an entity other than an originator, ODFI or RDFI that performs any functions on behalf of the originator, the ODFI or the RDFI with respect to the processing of ACH entries. The functions of these TPSPs can include, but are not limited to, the creation of ACH files on behalf of the originator or ODFI, or acting as a sending point of an ODFI (or receiving point on behalf of an RDFI).

For international ACHs, the NACHA operating rules define the following two new participants:

- A foreign correspondent bank is defined as a participating depository financial institution (DFI) that holds deposits owned by other financial institutions and provides payment and other services to those financial institutions.
- A foreign gateway operator (FGO) acts as an entry point to or exit point from a foreign country.

1179. How is a cross-border or international ACH transaction defined by OFAC?

OFAC defines a cross-border or international ACH transaction as an ACH transaction in which at least one of the ACH participants (e.g., originator, ODFI, receiver, RDFI) is outside of the United States or a U.S. jurisdiction and at least one of the processing institutions is subject to OFAC sanctions (i.e., within the United States or a U.S. jurisdiction).

For example, an international ACH transaction can include a domestic ODFI and a domestic RDFI that was initiated by a foreign originator.

1180. What is an IAT?

The international automated clearing house transaction (IAT) is a new Standard Entry Class (SEC) code that is required for all international ACH debits and credits as of September 18, 2009. Additional information is required to be sent with the ACH transaction to facilitate sanctions filtering and monitoring for potentially suspicious activity. These new fields include the following:

- Originator's name/address
- Beneficiary's name/address
- Originating bank name/ID/branch code
- Foreign correspondent bank name/ID/branch code
- Receiving bank name/ID/branch code

- Reason for payment

1181. What should an ODFI do to comply with OFAC sanctions?

In general, the ODFI must verify the originator is not a blocked party and make a good-faith effort to determine the originator is not transmitting blocked funds.

For cross-border ACH transactions, the ODFI is required to code the transaction as an IAT and provide the required information as detailed above.

In addition to screening the originator against OFAC Sanctions Listings, ODFIs should consider including the following in agreements with originators:

- Acknowledgement that originators and the ODFI are subject to OFAC sanctions (for certain types of ACH instructions, such an acknowledgement is required)
- Reference to possible delays in processing, settlement and/or availability for screening or investigating possible hits against the OFAC Sanctions Listings

1182. What should an RDFI do to comply with OFAC regulations?

An RDFI should screen its receivers against OFAC Sanctions Listings. Additionally, RDFIs are obligated to unbatch ACH transactions containing IATs and screen against OFAC Sanctions Listings.

1183. Is additional screening required for third-party service providers (TPSPs)?

As financial institutions can be held responsible in some situations for the acts of TPSPs, the financial institution should assess these relationships and ACH transactions to determine OFAC compliance risk and develop appropriate policies, procedures and processes to mitigate such risks. For further guidance on managing third-party risk, please refer to the sections: Know Your Third Parties and Third-Party Payment Processors.

1184. Can ODFIs and RDFIs rely on each other for OFAC compliance?

Domestic ODFIs and RDFIs can rely on each other for OFAC compliance to screen the originator and receiver as described above. This reliance, however, cannot be placed upon international ODFIs and RDFIs.

1185. Is an ODFI obligated to unbatch domestic ACH transactions in order to screen against OFAC Sanctions Listings?

No. If an ODFI receives domestic ACH transactions that its customer already has batched, the ODFI is not responsible for unbatching those transactions to screen against OFAC Sanctions Listings.

1186. If an ODFI unbatches domestic ACH transactions, is it obligated to screen against OFAC Sanctions Listings?

Yes. If an ODFI unbatches a file originally received from the originator in order to process "on-us" transactions, then it is obligated to screen against OFAC Sanctions Listings because it is acting as both the ODFI and RDFI for these transactions.

Financial institutions should determine the level of OFAC compliance risk of the remaining unbatched transactions that are not "on-us" and develop appropriate policies and controls to address the associated risks (e.g., screening each unbatched ACH record) through its OFAC/sanctions risk assessment. For additional guidance on OFAC/sanctions risk assessments, see the Risk Assessments section.

1187. How should ACH transactions that violate OFAC sanctions be handled?

If an ODFI processes an ACH credit for a receiver that is in violation of OFAC regulations, the RDFI should post the credit to the receiver's account, freeze the funds and report the transaction to OFAC.

If an ODFI processes a violative ACH debit, the RDFI should return the funds to the ODFI with the Return Reason Code R16 (Account Frozen) in accordance with NACHA Operating Rules. The ODFI should then freeze the funds and report the transaction to OFAC.

All transactions that have not yet been processed by the ODFI but are believed to be in violation of OFAC sanctions should be reported to OFAC for further review.

For additional guidance on ACHs, please refer to the Automated Clearing House Transactions section.

Trade Finance Transactions

1188. Are trade finance transactions subject to OFAC regulations?

Yes. Trade finance transactions, just as is the case with all other financial transactions, are subject to OFAC regulations. Each institution should establish a risk-based approach to screening the following trade finance participants for possible sanctions violations related to:

- Traders (e.g., importers, exporters)
- Financial institutions facilitating trade finance transactions (e.g., in the case of letters of credit, issuing bank, confirming bank, nominated bank, accepting bank, discounting bank, reimbursing bank, paying bank)
- Insurers
- Shipping agents/couriers

1189. What have been some challenges to complying with OFAC sanctions with respect to trade finance?

The major challenges of complying with OFAC sanctions with respect to trade finance include, but are not limited to, the following:

- Numerous parties located in foreign jurisdictions
- Frequent amendments (e.g., changes to involved parties, ports)
- Documentary-based transactions that require manual screening

For additional guidance on the money laundering and terrorist financing risks of trade finance, please refer to the Trade Finance Activities section.

Investigating Potential Matches

1190. What is the most effective way of monitoring transactions for OFAC?

More institutions are beginning to appreciate the challenge of dealing with long and frequently changing OFAC Sanctions Listings and, as such, are turning to interdiction software solutions to strengthen their OFAC Compliance Programs. Given the increasing use and complexity of international wire transactions, using interdiction software is a necessity for some institutions.

However, institutions cannot lose sight of the fact that a system is a tool, not the only solution. In the end, there can be no substitute for experienced and well-trained staff.

For smaller institutions with relatively few wire transactions, a simple in-house system using existing database software can be designed to perform the OFAC screening. This can be an effective and more cost-efficient alternative to purchasing OFAC interdiction software.

For additional guidance on interdiction software, please refer to the Customer and Transaction List Screening section.

1191. What are some tips for clearing an OFAC "hit"?

Tips for clearing OFAC "hits" include, but are not limited to, the following:

- Utilisation of primary factors that by themselves provide a high probability of a false positive, including, but not limited to, the following:
  - General false positive (e.g., SDN is individual and potential match is a vessel)
  - Identification number
  - Date of birth
- When unable to clear OFAC "hits" based on primary factors, utilisation of secondary factors that may not individually clear a match but together provide a high probability of a false positive, including, but not limited to, the following:
  - Not an exact name match (e.g., only one name matches the two or more names of the individual)
  - Country of origin
  - Address

If unable to clear based on primary or secondary factors, institutions should contact OFAC for further guidance.

1192. What should an institution do if it confirms a positive OFAC "hit"?

Finding a "hit" may necessitate blocking or rejecting a transaction and, if it is ultimately determined to be a positive hit, it will require the filing of a Blocked Transaction or Rejected Transaction report with OFAC. An institution is required to file the OFAC report within 10 business days of the blocked/rejected transaction. However, many possible hits turn out to be "false positives," which the institution should identify and clearly document the rationale and decision during its investigation process.

1193. What should an institution do when it is not comfortable that it has sufficient dispositive information to conclude the name is not a true match?

The institution should contact OFAC directly by telephone (1.800.540.OFAC) or email hotlines for further guidance. The investigation should be documented and maintained in the event questions arise in the future.

1194. Should a financial institution permanently suppress names causing frequent "false positives" in order to reduce the volume of transactions to be reviewed?

Financial institutions must carefully consider the risk of suppressing a name permanently. Since the OFAC Sanctions Listings are dynamic, it may be best to suppress a name until the OFAC Sanctions Listings are updated. A false positive at a certain time may become a true hit when the OFAC Sanctions Listings are updated.

1195. Is it necessary to file a SAR for an OFAC hit?

If the only "suspicious" activity was the OFAC hit, the blocked/rejected report satisfies a financial institution's reporting obligation. If the OFAC hit served as an alert generator to other suspicious activity in the customer's account, both a blocked/rejected report and a SAR are warranted, in which case the SAR should be sent promptly to FinCEN.

For further guidance on conducting investigations and filing SARs, please refer to the sections: Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Reports.

Blocking and Rejecting Transactions

1196. What is the difference between "blocking" and "rejecting"?

"Blocking" simply means freezing property. It is an across-the-board prohibition against transfers or dealings of any kind with regard to the property.

For example, a U.S. bank receives instructions to wire US$2,000 to a customer's relative in a country subject to OFAC Sanctions. The U.S. bank interdicts the payment, blocks it and reports it because it qualifies under the OFAC Sanctions Programs as a transaction to be blocked.

"Rejecting" means, simply, to not process a transaction. In some cases, an underlying transaction may be prohibited, but there is no blockable interest in the transaction. In these cases, the transaction is simply rejected or not processed.

For example, a U.S. credit union receives instructions from its customer to send US$4,000 to a country subject to OFAC sanctions. The credit union forwards the payment instructions to its correspondent that processes its wire transfers. The correspondent interdicts the payment, rejects it and reports it because it qualifies under the OFAC Sanctions Program as a transaction to be rejected.

Financial institutions should consult the specific economic sanction and follow the instructions exactly as written; requirements differ among the sanctions. In most cases, blocking is required; rejections are permitted only under very limited circumstances. The financial institution should, however, contact OFAC with questions.

1197. How will an institution know whether to block or reject a transaction?

An institution's obligation to block or reject a transaction depends on the requirements of the specific sanctions program involved.

1198. Does the requirement to block property apply to property and interests jointly owned by the designee with a third party?

Yes. If the designee is subject to a blocking provision, property and interests in which the designee owns 50 percent or more in aggregate is subject to being blocked.

1199. Can a blocking provision be applied to property and interests of persons associated with the designee?

If the associate provides material assistance, helps the designee evade sanctions or conspires to evade sanctions with the designee, the property and interests of the associate may be blocked.

1200. If a transaction to/from a designated target with a blockable interest is aborted by the customer, should it still be reported to OFAC?

Yes. OFAC prohibits evasion of and attempts to evade sanctions.

Financial institutions may also consider filing a Suspicious Activity Report (SAR).

FinCEN has established a hotline, 1.866.556.3974, for institutions to report to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States.

1201. With whom does title to blocked property rest?

Title to blocked property remains with the sanctioned target (designated country, national or blocked person), but the exercise of rights normally associated with ownership is relegated to the U.S. Department of the Treasury and controlled by OFAC-specific licenses or other authorisation by OFAC.

1202. What should be done with blocked funds?

Depository institutions must hold blocked funds in an individual account or an omnibus account (as long as an audit trail will allow specific funds to be unblocked with interest at any point in the future) that earns interest at a commercially reasonable rate. Only OFAC-authorised debits (including some

normal banking service charges) can be made in these accounts. OFAC can be contacted directly for further assistance on what types of transactions or service fees are permissible.

For nondepository institutions, the same requirements apply except for one. The nondepository institution will have to engage a depository institution to open a blocked account and hold the funds. The nondepository institution maintains the account on its books in the name of the individual or entity whose funds were blocked, but it should ensure the account is designated as a blocked account by the depository institution.

1203. Can an institution inform its customers that their funds have been blocked?

Yes. Unlike with Suspicious Activity Reports (SARs), an institution can inform customers of their blocked funds, but only after the funds have been frozen. Institutions can also inform customers of their right to apply for the unblocking and release of their funds through OFAC. However, if a SAR is also filed on the customer, then the customer may not be told of the SAR.

1204. When can an institution release blocked funds?

Funds can be released by the institution only upon receipt of a license or the issuance of an executive order allowing payment of the blocked funds. Usually, the customer who owns the blocked funds must apply for a license at OFAC to allow for such a payment. For additional guidance on licensing, please refer to the OFAC Licensing section.

1205. Does informing a customer of the potential blocking of funds constitute assisting the customer in evading OFAC Sanctions?

It is not advisable for an institution to inform a customer that a transaction is subject to blocking, as some of the sanctions programs prohibit aiding or abetting. Institutions may want to seek legal counsel before providing a response and/or referring the customer to OFAC. In any event, if the institution receives instructions from its customer for a wire transfer to a sanctioned country or designee, the institution must act on the instructions by blocking/rejecting the funds.

1206. How much has been blocked/rejected?

Based on the recent Terrorist Assets Report issued by OFAC, the United States has blocked over US$2.0 billion relating to state sponsors of terrorism, of which more than 80 percent was related to Iran.

1207. Can an institution allow a third party to conduct its screenings against the OFAC Sanctions Listings?

Yes. However, ultimate responsibility for OFAC compliance still lies with the institution, not the third party.

1208. How can customers request the release of blocked funds?

Customers must complete an Application for the Release of Blocked Funds. Upon approval by OFAC, the application becomes a specific license authorising the unblocking and release of funds. Funds can

be released to the originator or originating bank, or in accordance with OFAC's instructions in the specific license, which usually allow payment in accordance with the original payment instructions.

OFAC Reporting Requirements

Blocked/Rejected Transaction Reports

1209. What are the reporting requirements for blocked and/or rejected transactions?

The following reports must be filed with OFAC:

- Report of Blocked Transactions
- Report of Rejected Transactions
- Annual Report of Blocked Property
- Reports on Litigation, Arbitration and Dispute Resolution Proceedings

A Report of Blocked Transactions must be filed for blocked transactions within 10 business days of the blocked transaction. A Report of Rejected Transactions must be filed for rejected transactions within 10 business days of the rejected transaction. If the institution is holding funds in a blocked account on June 30, it is required to file an Annual Report of Blocked Property by September 30 of that year. U.S. persons involved in litigation, arbitration or other binding alternative dispute resolution proceedings regarding blocked property must provide notice of such proceedings to the OFAC Chief Counsel and submit copies of all documents associated with such proceedings within 10 business days of their filing.

1210. What is the time frame for filing a report to OFAC?

Blocked and Rejected Transaction reports must be filed within 10 business days after the date of detection of the "hit." All submissions must be received in writing and be kept on file with supporting documentation at the financial institution for five years. An Annual Report of Blocked Property must be filed by September 30 each year.

1211. What does the term "date of detection" mean for OFAC purposes?

The term "date of detection" is the date of the blocked/rejected transaction.

1212. Where are OFAC reports filed?

Institutions are required to submit Blocked Transactions, Rejected Transactions and Blocked Property reports to the Compliance Programs Division, OFAC, Department of the Treasury, Washington, DC, 20220.

1213. Can OFAC reports be filed electronically?

Yes. The Report of Blocked Transactions and Report of Rejected Transactions can be submitted via regular mail, fax or through OFAC's E-Filing system, the Automated Blocking & Reject Reporting System (ABaRRS). The Annual Report of Blocked Property can be submitted via regular mail.

1214. Should supporting documentation be sent with Blocked Transactions and Rejected Transactions reports to OFAC?

Blocked Transactions and Rejected Transactions reports must include a copy of the original payment instructions and specific transaction detail. All supporting documentation should be sent to OFAC with the Blocked Transactions and Rejected Transactions reports. It may be prudent to check with OFAC at the time of filing to see if any additional documentation is needed.

1215. How long should institutions retain OFAC reports and supporting documentation?

OFAC reports and supporting documentation must be retained for a minimum of five years from the date of the filing to OFAC. The retention period may be longer than five years, depending on the state or self-regulatory organisation (SRO).

1216. If multiple institutions are involved in processing the transaction, who ultimately is responsible for filing the appropriate reports with OFAC?

The institution that blocks or rejects the prohibited transaction is responsible for filing the required reports. However, other individuals or institutions involved in the transaction who failed to block, reject and/or report the prohibited transaction may be subject to penalties.

1217. Does the filing of Blocking/Rejecting Reports obviate the need for institutions to file a Suspicious Activity Report?

If no further suspicious activity is detected other than the confirmed OFAC match, the filing of a Report of Blocked Transactions or Report of Rejected Transactions satisfies the Suspicious Activity Report (SAR) filing requirement. For further guidance on reporting potentially suspicious activity, please refer to the Suspicious Activity Reports section.

Annual Report of Blocked Property

1218. What is the Annual Report of Blocked Property?

If the institution is holding funds in a blocked account on June 30, it is required to file an Annual Report of Blocked Property by September 30 of that year.

OFAC Licensing

1219. Are there exceptions to the OFAC Sanctions Programs?

Yes. OFAC can issue general licenses authorising the performance of certain categories of transactions, as well as specific licenses, on a case-by-case basis. Additional information on how to request a license can be found in the regulations for each sanctions program on OFAC's website.

1220. What is a general license?

A general license is defined by OFAC as an authorisation from OFAC that allows certain transactions for a class of persons without the filing of a license application with OFAC. The terms of a general license are provided in the relevant embargo or sanctions program.

1221. What is a specific license?

A specific license is defined by OFAC as a "permit issued by OFAC on a case-by-case basis to a specific individual or company allowing an activity that would otherwise be prohibited by the embargo or sanctions program."

1222. How is a specific license obtained?

Individuals or entities must submit an application for specific licenses to OFAC. Application requirements are specific to the particular embargo or sanctions program. For additional details, refer to OFAC's website: www.ustreas.gov/ofac.

1223. What information must be provided on an application for a specific license?

Most license programs do not have a specific application form. However, a detailed letter should be remitted to OFAC that should include all necessary information as required in the application guidelines or regulations for the specific embargo program. A detailed description of the proposed transaction, including the names and addresses of any individuals or companies involved, should be included in the letter. In many cases, OFAC's licensing division will be able to guide further through a phone consultation what is best included in the letter, as every sanctions program has different nuances for licensing.

1224. Is there a formal process of appeal if an application for a specific license is denied by OFAC?

No. There is no formal process of appeal; however, OFAC will reconsider its decision for good cause, such as where the applicant can demonstrate changed circumstances or submit additional relevant information that was not presented previously.

1225. How can specific licenses be verified by institutions?

Each specific license has a control number that can be verified by contacting the OFAC Licensing Division. If a customer claims it has a specific license, the institution should verify the transaction conforms to the terms of the license before processing the transaction and retain a copy of the authorising license.

1226. Are specific licenses transferable?

In general, specific licenses are not transferable.

1227. Do specific licenses expire/require renewal?

Specific licenses expire on the expiration date set forth in the license. If no expiration date is included, the institution should check with OFAC to see if the license is still valid.

1228. Can specific licenses be revoked?

Yes. Specific licenses can be revoked or modified at any time at the discretion of the Secretary of the Treasury.

1229. Do specific licenses provide protection from civil or criminal liability for violations of any laws or regulations?

No. A specific license is only good to conduct such transactions or activities as it is approved for, and in no way prevents penalties for violations of laws or regulations.

1230. Are licenses issued only by OFAC?

No. In some instances, applicants may apply for licenses with the U.S. Bureau of Industry and Security (BIS).

1231. What is the U.S. Bureau of Industry and Security (BIS)?

BIS is an agency of the U.S. Department of Commerce. The mission of BIS is to advance U.S. national security, foreign policy and economic objectives by ensuring an effective export control and treaty compliance system and promoting continued U.S. strategic technology leadership. BIS achieves this by controlling the dissemination of dual-use products and technology to destinations and end users throughout the world. BIS expertise includes engineering and product knowledge used for product classification.

1232. Does the BIS issue any lists similar to OFAC's SDN List?

The BIS publishes the following lists:

- **Denied Persons List (DPL)** – A list of individuals and entities that have been denied export privileges. No exporter may participate in an export or re-export transaction subject to an Export Administration Regulation (EAR) with a person or entity whose export privilege has been denied by the BIS.
- **Entity List** – A list of names of certain foreign parties that are prohibited from receiving some or all items subject to the EAR unless the exporter secures a license. The Entity List can include businesses, research institutions, government and private organisations, individuals and other types of legal persons, who are subject to specific license requirements for the export, re-export and/or transfer (in-country) of specified items.
- **Unverified List** – A list of names and countries of foreign persons who in the past were parties to a transaction with respect to which BIS could not conduct a pre-license check or a post shipment verification for reasons outside of the U.S. government's control. The presence of a party on this list in a transaction is a red flag that should be resolved before proceeding with the transaction.

- **BIS General Orders** – A list of persons and businesses with restricted export privileges.

The Consolidated Screening List administered by the Department of Commerce includes the above lists as well as the following:

- **Nonproliferation Sanctions List** (Department of State)
- **AECA Debarred List** (Department of State)
- **Specially Designated Nationals and Blocked Persons List (SDN List)** (Department of the Treasury, OFAC)
- **Foreign Sanctions Evaders List (FSE List)** (Department of the Treasury, OFAC)
- **Sectoral Sanctions Identifications (SSI)** List (Department of the Treasury, OFAC)
- **Palestinian Legislative Council (PLC)** List (Department of the Treasury, OFAC)
- **The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)** (Department of the Treasury, OFAC)
- **Non-SDN Iranian Sanctions Act List (NS-ISA)** (Department of the Treasury, OFAC)

1233. Who is required to screen against the BIS lists?

Exporters are required to screen against the BIS lists. No exporter may participate in an export or re-export transaction subject to an Export Administration Regulation (EAR) with a person or entity whose export privilege has been denied by the BIS.

1234. Are financial institutions required to screen against the BIS lists?

No. It is the responsibility of the exporter to ensure that it is not transacting with an individual or entity listed on the BIS lists; however, a financial institution is still liable if it facilitates a transaction with a listed individual or entity. As a prudent measure, although not required, some financial institutions opt to screen against the DPL in addition to the OFAC Sanctions Listings.

1235. What action must institutions take if a positive "hit" is identified on the BIS lists?

Follow-up actions may involve restrictions on shipping to certain countries, companies, organisations and/or individuals. Unlike with OFAC, there are no reporting requirements when a positive hit is identified. For additional guidance, contact BIS's Office of Enforcement Analysis (OEA).

1236. What is the interrelation between BIS and OFAC?

BIS and OFAC both work toward a common national security goal, with different functions. With regard to licensing, both BIS and OFAC can have overlapping authority. For some sanctions programs, only one of the agencies may provide a license.

1237. Are there other U.S. agencies with licensing and export prohibition responsibilities beyond OFAC and BIS?

Yes. The Commerce, State, Defense and Energy Departments administer the following licensing and export prohibition programs:

- **The Commerce Control List (CCL)**, administered by the Commerce Department pursuant to the Export Administration Act of 1979 (EAA) (as amended), is used to regulate the export and re-export of items that have commercial uses but also have possible military applications (dual-use items). Examples of items on the CCL include, but are not limited to, the following:
    - Nuclear materials, chemicals, microorganisms and, toxins
    - Computers
    - Telecommunications
    - Information security
    - Navigation and avionics
    - Aerospace and propulsion
- The **U.S. Munitions List (USML)**, administered by the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs within the State Department pursuant to the Arms Export Control Act of 1976 (AECA) and the International Traffic in Arms Regulations (ITAR), is used to control the export of defence articles, services and related technologies. Examples of items on the USML list include, but are not limited to, the following:
    - Firearms, such as close assault weapons, combat shotguns, guns over calibre 0.50 and flamethrowers
    - Launch vehicles, guided missiles, ballistic missiles, rockets, torpedoes, bombs and mines
    - Explosives, propellants and incendiary agents
    - Armored combat ground vehicles, special naval equipment, fighter bombers, attack helicopters, unmanned aerial vehicles (UAV)
    - Military training equipment
    - Personal protective equipment, such as body armour, helmets and select face paints
    - Military electronics, such as radios and radar systems
- The Defense Department is actively involved in the interagency review of those items controlled on both the CCL and the USML. The agencies work together when there is a question about whether a proposed export is controlled on the CCL or the USML.
- The **AECA Debarments list**, also administered by the Directorate of Defense Trade Controls within the State Department pursuant to AECA and ITAR, includes persons who have been convicted for violations (or conspiracy to violate) the AECA in court (statutory debarments) or

have violated (or conspired to violate) the AECA during an administrative proceeding (administrative debarment). The Energy Department, through the National Nuclear Security Administration (NNSA) is responsible for the security of the U.S. nuclear weapons, nuclear proliferation and naval reactor programs. This includes controlling nuclear technology and technical data for nuclear power.

Administrative Subpoena or 602 Letter and Prepenalty Notice

1238. What is a "602 Letter"?

If OFAC needs additional information from a financial institution, it may send an administrative subpoena, also called a 602 Letter, to the institution (e.g., requesting an explanation regarding how a prohibited transaction was processed and/or actions taken by an institution to prevent future violations).

1239. What is a Prepenalty Notice?

OFAC may issue a Prepenalty Notice in response to information provided in a 602 Letter response. The Prepenalty Notice cites the violation and states the amount of the proposed penalty.

1240. What is the allotted time frame for responding to a Prepenalty Notice?

An institution has 30 days to make a written presentation on why a penalty should not be imposed, or if imposed, why the proposed civil money penalty should be reduced.

1241. What are the consequences of not responding to a Prepenalty Notice?

Failure to respond to a Prepenalty Notice may result in default judgments levying maximum fines.

Voluntary Disclosure

1242. What is meant by "voluntary self-disclosure"?

"Voluntary self-disclosure (VSD)" is defined by OFAC as notification to OFAC of an apparent sanctions violation by the institution that has committed the violation.

1243. Are there instances in which a disclosure may not be considered voluntary?

There are a few instances in which a notification may not be considered by OFAC to be voluntary. The first is if OFAC has previously received information concerning the conduct from another source, such as another regulatory or law enforcement agency, or if another person's Blocked Transactions and Rejected Transactions reports detail information that would show a violation. Similarly, responding to an administrative subpoena or another inquiry from OFAC would not be deemed voluntary. In addition, the submission of a license application may not be deemed a voluntary disclosure.

1244. Should institutions voluntarily self-disclose past undetected violations of OFAC regulations?

Self-disclosure may be considered a mitigating factor by OFAC in civil penalty proceedings. Voluntary self-disclosure will be considered when determining an enforcement response. It is advisable that institutions seek legal counsel's advice before self-disclosing.

1245. In what form should the voluntary self-disclosure be?

Self-disclosure should be in the form of a detailed letter to OFAC, with supporting documentation, as appropriate.

1246. What guidance has been issued on voluntary disclosures of sanctions violations?

The Department of Justice (DOJ) issued Guidance Regarding Voluntary Self-Disclosures, Cooperation and Remediation in Export Control and Sanctions Investigations Involving Business Organisations in 2016. While the guidance explicitly stated that it did not apply to financial institutions, only corporate entities engaged in export activity and their employees, much of the guidance could be applied to financial institutions. The guidance discussed how the following activity could impact the "credit" of the VSD:

- Timing and accuracy (e.g., full disclosure of relevant facts) of initial VSD;
- Subsequent cooperation with investigations (e.g. proactive versus reactive); and
- Remediation efforts of flawed sanctions/export control programs (e.g., timeliness, disciplinary actions of responsible employees).

The guidance discussed the following aggravating factors:

- Exports involving nuclear non-proliferation or missile technology to a proliferator country;
- Exports involving items to be used in weapons of mass destruction (WMDs);
- Exports to a terrorist organisation;
- Exports of military items to a hostile foreign power;
- History of repeated sanctions violations;
- Degree of knowledge of involvement of senior management in the sanctions violation(s); and
- Amount of profits earned from sanctions violations, intended or realised.

The guidance also discussed the following types of impact on benefits or "credits" for the self-disclosing entity:

- Reduced fine and/or forfeiture;
- Non-prosecution agreement (NPA) as opposed to a deferred prosecution agreement (DPA);
- Reduced period of supervised compliance; and
- No requirement for a monitor.

Whether self-disclosing for sanctions violations, tax evasion or other laws, it is advisable that institutions seek legal counsel's advice before self-disclosing. For guidance on developing a comprehensive sanctions compliance program, please refer to the OFAC Basics section.

Independent Testing

1247. What should be considered with respect to independent testing of an OFAC program?

Although OFAC audit programs will vary depending on the company's nature of business and operations, there are certain basic considerations that should be included in all OFAC audits, such as:

- Confirming that the institution's compliance policy or operating procedures detail OFAC restrictions and the roles and responsibilities of company personnel in ensuring compliance;
- Confirming that the institution has provided appropriate training on OFAC sanctions and Compliance Program requirements;
- Reviewing the institution's procedures for screening new customer and other third-party relationships against the OFAC list and existing customer/third-party relationships against updates to the OFAC Sanctions Listings;
- Determining whether the institution's personnel understand how OFAC screening software works and its level of reliability (e.g., what degree of confidence can be expected from the algorithms used by the software);
- Determining whether any modifications have been made to the OFAC screening software and, if so, whether these are properly supported and documented;
- Testing the effectiveness of the institution's monitoring procedures: where screening is manual, reviewing the company's transaction records to determine whether any OFAC transactions may have gone undetected; where screening is automated, constructing "dummy tests" of actual OFAC names to ensure that they are identified by the system;
- Reviewing the institution's procedures for clearing "hits" and related documentation;
- Determining whether true "hits" are reported to OFAC, according to the requirements;
- Determining that the institution has effective controls for not releasing frozen assets until permitted by OFAC;
- Following up on any previously identified problems or issues in past audit reports or regulatory examination reports; and
- Sampling transactions with missing information (e.g., country fields) and related payment orders for potential indicators of stripping.

1248. Is there a requirement that OFAC Compliance Programs be subject to periodic independent testing?

Performing independent testing of an institution's OFAC Compliance Program is not mandated by regulation, but is prudent given the risks of noncompliance and financial institution regulators do expect OFAC Sanctions Compliance Programs to be tested. Some institutions may find it beneficial to conduct a review of the OFAC Sanctions Compliance Program simultaneously with the review performed of the AML/CFT Compliance Program. When the reviews are not performed in conjunction with one another, the time frame for performing a review should be risk-based. For institutions that have determined they are high-risk pertaining to OFAC (for additional information on determining whether an institution is high risk for OFAC consideration, please refer to the Risk Assessments section), it may be more appropriate to conduct a review more frequently (every 12 to 18 months) to ensure that potential gaps and deficiencies, which may lead to potential sanctions violations, are identified.

1249. Should independent testing of an OFAC Sanctions Compliance Program be risk-based?

Yes. Just as with the independent testing of the AML/CFT Compliance Program, the testing of the OFAC Sanctions Compliance Program should be risk-based. As not every institution experiences the same level of OFAC compliance risk, the depth of review performed may be more or less rigorous to be in line with evaluating whether the OFAC Sanctions Compliance Program is adequately designed and operating effectively in order to mitigate the institution's unique level of risk.

1250. Are compliance officers required to certify that sanctions screening programs are in compliance with AML/CFT and sanctions laws and regulations?

Federal AML/CFT and sanctions laws and regulations do not require "certifications." Due to identified serious shortcomings in AML/CFT programs, the New York State Department of Financial Services (DFS) enacted a rule in 2016 requiring annual certifications of transaction monitoring and filtering programs by the board of directors or senior official(s) responsible for the management, operations, compliance and/or risk management of a covered institution.

For more guidance, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications.

1251. Should OFAC screening systems be validated?

Typically, a sanction screening system is considered a model that should be subject to validation. The model validation should be performed by a party independent of the model developer and owner, who has the requisite technical and subject matter expertise to be able to perform the necessary tasks.

For further guidance on model validation, please refer to the Model Validation section.

Consequences of Noncompliance with OFAC Laws and Regulations

1252. What are the consequences of noncompliance?

Pursuant to the Federal Civil Penalties Inflation Adjustment Act Improvements Act of 2015 (Inflation Adjustment Act), civil monetary penalties (CMPs) were increased to adjust for inflation. Adjusted penalties per violation under the following statutes became effective for CMPs assessed after August 1, 2016:

- **Trading with the Enemy Act** (TWEA) of 1917 – CMPs increased from US$65,000 to US$83,864
- **(IEEPA) -** CMPs increased from the greater of US$250,000 or twice the amount of the underlying transaction to the greater of US$284,582
- **Antiterrorism and Effective Death Penalty Act** (AEDPA) (1996) – CMPs increased from the greater of US$55,000 or twice the amount of which a financial institution was required to retain possession on control to the greater of US$75,122
- **Foreign Narcotics Kingpin Designation Act** (Kingpin Act) (1999) – CMPs increased from US$1.075 million to US$1.414 million
- **Clean Diamond Trade Act** (CDTA) (2003) - CMPs increased from US$10,000 to US$12,856

A non-negotiable part of any violation is the publication on the OFAC website of the violator's name (if it is an entity), details of the violations and amount of the fine.

In addition to monetary penalties, OFAC may impose the following actions for noncompliance:

- Cautionary or warning letter
- Revocation of license
- Criminal penalty (usually done through referral to the Department of Justice [DOJ]) (e.g., 10 to 30 years imprisonment for wilful violations)

1253. Are non-U.S. persons subject to penalties for noncompliance with OFAC sanctions?

Given the breadth of OFAC's definition of "U.S. Person" across sanctions regimes, certain foreigners must also comply with OFAC regulations. OFAC deems "U.S. Persons" to include: (1) U.S. citizens or permanent residents (i.e., green card holders), wherever located; (2) any entity organised under U.S. federal or state law, including – in certain circumstances – even foreign branches of such U.S. entities; and (3) any person, even a foreigner, who is physically in the United States. All of those categories of individuals and entities (which include some foreigners) must comply with the regulations, as well, or risk penalties.

Non-U.S. persons may be penalised as a counterparty in transactions with a designated person by having their funds frozen. Under the Iranian and Syrian Sanctions Program, non-U.S. persons who evade or attempt to evade OFAC sanctions (e.g., conduct transactions on behalf of a designated individual, strip transactions of names of designated individuals) may be designated as a Foreign Sanctions Evader (FSE) and risk being cut off from the U.S. and global financial system.

1254. What does it mean that OFAC is a "strict liability program"?

Strict liability means that the offender is liable even if it did not know that it violated a sanctions program.

1255. What are the penalties for failing to comply with OFAC sanctions?

Corporations and individuals may be subject to civil and/or criminal penalties for noncompliance with OFAC sanctions and individuals may also be subject to imprisonment, as follows:

- Civil penalties equal to the greater of US$284,582 or 2X the amount of the transaction up to US$1,414,020 per violation where there has been no voluntary disclosure; and
- Criminal fines of up to US$1 million and 20 years in jail.

These fines apply to most OFAC Sanctions Programs, with the exception of some cases (e.g., Cuba). Detailed OFAC enforcement guidelines, including how penalties are calculated, can be found here: https://www.treasury.gov/resource-center/sanctions/Documents/fr74_57593.pdf.

1256. Are there any exceptions for first-time offenders?

Yes. First-time offenders may be eligible for a 25 percent reduction of the base penalty.

1257. If the transaction was successfully blocked/rejected by the financial institution, can the individual/entity initiating the transaction still be subject to penalties?

Yes. Blocked Transactions and Rejected Transactions reports contain information that can be confirmed and examined to determine whether proper due diligence procedures were used. The Report of Blocked Transactions and the Report of Rejected Transactions show that the individual/entity originating the transaction violated OFAC regulations in some manner and thus can be subject to penalties. For example, if an individual initiates a wire transfer to a South Sudanese government-owned company, the payment would be blocked. The individual could be subject to penalties depending on the circumstances of the transaction under the International Emergency Economic Powers Act (IEEPA), the law that enforces the South Sudanese Sanctions Regulations.

1258. What is OFAC's process for issuing civil penalties?

OFAC will send a letter to the violator stating the details for each individual case. Most proceedings include the opportunity for an administrative hearing and prehearing discovery prior to imposition of a penalty or asset forfeiture. OFAC also has a process it may use for settlement of a matter before a prepayment penalty notice has been issued.

1259. What factors are considered by OFAC when evaluating the severity of OFAC violations?

With respect to how it evaluates the severity of OFAC violations, the 31 C.F.R. Part 501 – Economic Sanctions Enforcement Guidelines indicate that OFAC considers the following factors, though this is not necessarily an exhaustive listing:

- Evaluation of the OFAC program by the institution's regulator;
- History of the institution's OFAC compliance and whether it was a first offense;
- Circumstances around the identified OFAC violation and any patterns of weakness in the OFAC Compliance Program;
- Negligence or fundamental flaw in the institution's compliance effort or system;
- Whether the institution voluntarily disclosed the violation; and
- Actions taken by the institution to correct violations to ensure that similar violations do not reoccur.

1260. What is the difference between a civil penalty and a settlement?

Civil penalties require an actual agency determination of a violation. A settlement is a negotiated agreement between the agency and a company that does not require the actual determination of a violation.

1261. What are some examples of OFAC violations in nonfinancial services companies?

A travel service provider could be fined for unlicensed services rendered in Cuba. A medical products manufacturer could be penalised for the shipment of unlicensed medical equipment to Iran. A casino could be fined for payment of a slot jackpot to an individual on the Specially Designated Nationals and Blocked Persons List (SDN List).

1262. What are some common deficiencies that have been identified in recent enforcement actions and settlements?

The following areas are some of the common deficiencies in OFAC compliance programs that have been identified in recent OFAC settlements:

- Wilful violations of sanctions programs (e.g., the Iranian Transactions and Sanctions Regulations [ITSR], Cuban Assets Control Regulations)
- Processing of transactions in a nontransparent manner to evade sanctions restrictions
    - Utilisation of third parties to process transactions to circumvent sanctions controls
- Failure to screen high-risk customers and products/services (e.g., import-export letters of credit) against sanctions lists

For further details on recent OFAC settlements, please refer to Key U.S. Enforcement Actions and Settlements in the Appendix.

Common Gaps and Challenges

1263. What are some of the common challenges to maintaining an effective OFAC Sanctions Compliance Program?

The following include some of the challenges that companies have experienced in implementing an OFAC Sanctions Compliance Program:

- Inadequate OFAC policies (e.g., do not address use of cover payments or SWIFT messages, use of straw men, blocking of property and interests beyond transactions)
- Poor management of OFAC Sanctions Listings:
  - Updates to OFAC Sanctions Listings are not incorporated in a timely manner;
  - Lack of screening for non-SDN Lists (filter includes SDN List only and not the NS-PLC, SSI or FSE Lists or other international sanctions programs [e.g., United Nations] for global programs); or
  - Poor "white list" management.
- Lack of OFAC risk assessment (or incorporation of a risk-based approach)
- Inadequate OFAC training and/or understanding of the various OFAC Sanctions Programs
- Overreliance on third parties to perform the OFAC screening (e.g., correspondent banks, intermediary banks, service providers)
- Poor workflow and recordkeeping:
  - Inadequate investigation workflow
  - Inadequate and poor documentation of due diligence in clearing potential OFAC matches
  - Poor record retention
- Lack of complete screening coverage of customers and transactions:
  - Existing customers, employees or third-party service providers (e.g., vendors, consultants) are not screened against OFAC Sanctions Listings, and/or updates to the list are performed infrequently, if at all (e.g., safe deposit box customers who do not have deposit accounts, noncustomers or parties involved in letters of credit)
  - Transactions are not screened against OFAC Sanctions Listings, and/or updates to the lists are performed infrequently, if at all (e.g., checks, monetary instruments, ACHs, cover payments)
- Ineffective use of technology (e.g., interdiction software):
  - Use of multiple sanctions screening systems (e.g., different lines of business implementing their own sanctions screening systems)

- Overreliance on vendor settings (e.g., "out-of-the-box" settings or "plug–and-play" approach)
- Lack of system validation and testing
- Lack of screening beyond originator and beneficiary fields (e.g., cover payments often list originator/beneficiary in additional fields that may not be screened in interdiction software), additional address fields (e.g., physical, mailing, alternate)
- Utilisation of high confidence levels for matches (e.g., 100 percent), thereby preventing possible hits from generating alerts for further review
- Implementation of inconsistent matching algorithms/confidence levels for each product, transaction, customer and/or department
- Ineffective use of exclusion features, thereby suppressing potential hits

1264. What challenges have financial institutions faced when implementing a global sanctions program?

In addition to those listed above, financial institutions have faced the following challenges when implementing a global sanctions program:

- Lack of development of a coherent sanctions policy that incorporates inconsistent programs from multiple countries; and
- Lack of a culture of responsibility (e.g., buy-in) from employees for sanctions programs from other countries.

RISK ASSESSMENTS

Basics

1265. What is a risk assessment?

The Financial Action Task Force (FATF) defines a risk assessment as "a process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand … risks and serves as a first step in addressing them and making judgments" about identified risks.

There are many different types of risk assessments. Risk assessments may be designed to measure the following on a line of business or enterprise level:

- Inherent risks;
- Controls or control environment (e.g., strengths/deficiencies in a compliance program); and
- Residual risk.

Other risk assessments, such as ones performed to assess product/service risk or geographic risk, may only measure the inherent risk of these factors and may be used as an input in an organisation's other risk assessments.

1266. Are financial institutions required to conduct risk assessments?

Financial institutions are expected to develop and maintain risk-based AML/CFT Compliance Programs. This requires that they conduct risk assessments. Bank regulators, in particular, expect the financial institutions they supervise to conduct, among others:

- **Enterprisewide risk assessment –** An exercise intended to identify the aggregate money laundering (ML) and terrorist financing (TF) risks facing an organisation that may not be apparent in a risk assessment focused on a line of business, legal entity, or other assessment unit. In other words, it is the big picture view, or profile, of an organisation's ML/TF risks that aggregates the results of other risk assessment exercises in order to quantify and relate the total risks for the organisation to the established risk appetite and tolerance for the enterprise.
- **Horizontal risk assessment –** An exercise intended to identify systemic ML/TF risks of designated high-risk products/services and/or customers across an organisation regardless of which line of business or legal entity owns these activities or customers.
- **Line of business (LOB)/legal entity (LE) risk assessment –** An exercise intended to identify the level of vulnerability of each line of business (LOB) or legal entity (LE) to ML/TF. This is accomplished by evaluating, for a specific LOB or LE, among other factors, the ML/TF risks of products/services, the customer base (e.g., type, location) and geography (e.g., customers, transactions, operations) and the controls (e.g., policy and procedures, customer acceptance and maintenance standards, transaction monitoring, management oversight, training, personnel) mitigating those risks at the business line or legal entity level.

- **Product/transaction/service risk assessment –** An exercise intended to identify the inherent ML/TF risks of the products, transaction types and services offered by a financial institution.
- **Geographic risk assessment –** An exercise intended to identify the inherent ML/TF risks of the international and domestic jurisdictions in which a financial institution and its customers conduct business.
- **Customer risk assessment –** An exercise intended to identify the level of inherent ML/TF risks in the types of customers (e.g., individual, institutional, financial institution, not for profit) served by a financial institution.
- **OFAC/Sanctions risk assessment –** An exercise intended to identify an organisation's level of vulnerability to noncompliance with economic sanctions administered by OFAC or any sanctions program as required by the financial institution's policy. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types, the geographic origin and destination of transactions, and the strength of the controls mitigating those risks.

Further guidance on each of these risk assessments is provided below.

1267. How can financial institutions utilise risk assessments in their AML/CFT Compliance Programs?

Financial institutions can utilise risk assessments in many ways, including, but not limited to, the following:

- Development of an AML/CFT strategy (e.g., discontinue or prohibit the provision of products and services of heightened ML/TF risks)
- Allocation of resources (e.g., personnel, technology) to high-risk areas
- Design and application of a Know Your Customer (KYC) program
- Design and application of a suspicious activity monitoring program (e.g., application of specific suspicious activity monitoring parameters for high-risk customers)
- Development and provision of targeted training

1268. Are risk assessments required to be used explicitly in AML Programs (e.g., KYC, suspicious activity monitoring)?

Federal regulations do not require covered financial institutions to link their risk assessments explicitly to their AML Programs (e.g., risk-based customer profiles tied to specific monitoring rules in transaction monitoring systems). However, regulators do expect financial institutions to be able to demonstrate the alignment between risk assessments and other aspects of an institution's AML Program and the Customer Due Diligence Requirements for Financial Institutions final rule (Beneficial Ownership Rule), issued in July 2016, clarified that a financial institution is expected to utilise all available information (e.g., collected CDD, risk profiles) as part of its investigative processes to determine if customer activity is potentially suspicious in its suspicious activity monitoring program.

On a state level, in July 2016, the New York State Department of Financial Services (DFS) issued Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, requiring covered financial institutions in New York to explicitly link customer information and risk profiles to transaction monitoring programs, effective in early 2017.

Whether the requirement is explicit or implied, leading practice suggests a risk-based monitoring program based on customer data is more effective at generating "alerts" for potentially suspicious activity. For further guidance on suspicious activity monitoring, please refer to the Transaction Monitoring, Investigations and Red Flags section.

1269. What is inherent risk?

Inherent risk is the risk to an entity in the absence of any actions management might take (e.g., controls) to alter either the risk's likelihood or impact.

1270. What is a control?

A control is a process, designed and/or performed by an entity, to mitigate or reduce the likelihood or impact of a risk. Control processes may be manual, automated, preventive and/or detective.

In terms of a financial institution's AML/CFT Compliance Program, the following are examples of controls:

- The financial institution sets a policy prohibiting the offering of products/services to a particular type of customer (e.g., money services businesses).
- Supervisors or managers review and approve a documentation checklist, completed by an account officer, prior to account opening, as a control to ensure the necessary customer information is collected according to the financial institution's policies and procedures.
- The financial institution's systems require the input of necessary customer information before the account officer can proceed to the account opening screen as an automated control to ensure the necessary customer information is collected according to the financial institution's policies and procedures.
- The financial institution requires more frequent updating of customer information or may perform periodic site visits of its high-risk customers.
- The financial institution utilises an automated monitoring system to detect potentially suspicious activity.

1271. What is residual risk?

Residual risk is the risk remaining after all controls have been applied to reduce the likelihood or impact of the risk. An acceptable level of residual risk is determined by the risk appetite or tolerance of the financial institution.

1272. What is a risk assessment methodology?

A risk assessment methodology is an institution's documented process and approach for conducting the risk assessment. A methodology document typically includes the following:

- A detailed description of the procedures to follow in conducting the risk assessment;
- The roles of responsible and accountable parties;
- The scoring system(s) used along with definitions and weights;
- Supporting data types and sources;
- Frequency of updates;
- Required approvals; and
- Usage in shaping the compliance program.

1273. Who should be responsible for designing the risk assessment methodology?

A risk assessment methodology engages senior management, business or process owners, and compliance personnel. Compliance should develop the risk assessment methodology with input from the business or process owners; senior management should review and approve the methodology.

1274. Who should be responsible for conducting risk assessments?

The type of risk assessment will dictate the responsible parties. Compliance should conduct enterprisewide, horizontal, geographic and product/service risk assessments and should develop the methodology for LOB and LE risk assessments to ensure that a consistent approach is used across the enterprise.

An LOB/LE risk assessment should engage the business and process owners (i.e., the people who best understand the business and/or processes). Compliance should, however, review and approve business- or process-owner-assigned ratings.

At a minimum, the results of the enterprise and horizontal risk assessments should be presented to an institution's senior management and board of directors. LOB/LE risk assessments should be shared with senior management of these businesses.

1275. Are risk assessments strictly quantitative (e.g., based on statistics)?

No. Risk assessments should consider both quantitative and qualitative information.

1276. Are risk assessment models subject to validation?

According to regulatory guidance, the term "model" refers to a quantitative method, system or approach that applies statistical, economic, financial or mathematical theories, techniques and assumptions to process input data into quantitative estimates. A risk assessment, therefore, may be considered a model if it uses a mathematically or statistically-driven method to identify ML/TF risk.

1277. Are money laundering and terrorist financing addressed in a single risk assessment?

Terrorist financing is one form of money laundering, however when analysing underlying criminal activities (e.g., drug trafficking), the patterns of activity tend to be different for "laundering" related to terrorism. For example, terrorist financing often involves very small amounts of funds, which may be moved through charities or nontraditional banking systems, whereas laundering the proceeds from narcotics sales typically involves the movement of large volumes of funds (e.g., bulk cash smuggling). The same risk assessment may be leveraged to evaluate both ML and TF risks; however, different risk factors need to be included to detect vulnerability to all forms of illicit activity effectively.

1278. How can the results of an enterprise or business line risk assessment be presented?

The results of a risk assessment can be presented in a heat map. A heat map is a visual aid (a matrix or other graphic) that uses colour coding, usually green, yellow and red, to show the different risk ratings for risk assessment results or supporting component analyses.

1279. Do any customer types, products, services or transactions pose zero risk of money laundering or terrorist financing?

No. Every customer type, product, service or transaction poses some degree of ML/TF risk; therefore, it is recommended that "zero" not be used when assigning risk to customer types, products, services and transactions. However, some customers, products, services and transactions may pose only a very minimal risk, such as a customer who performs a one-time, low-dollar amount transaction or who only has direct deposits of payroll and performs only low-dollar transactions.

1280. Should a financial institution reduce the inherent risk score of a high-risk customer type, product, service or transaction to moderate or low if it has significant familiarity with that customer type, product, service or transaction?

No. The scale used to assign risk to customer types, products, services and transactions should be an absolute scale, not a relative scale particular to the financial institution. The inherent risks of customer types, products, services and transactions do not vary by financial institution or region. A financial institution's familiarity with a particular type of customer, product, service or transaction should factor into adjusting the residual risk by the implementation of appropriate controls, not into adjusting the inherent risk.

For example, if a financial institution has a significant number of money services businesses (MSBs), the inherent risk of its customer base will be higher. However, due to the financial institution's substantial experience with MSBs and its enhanced due diligence (EDD) and monitoring program, its residual risk may be lower. It would be unacceptable for the financial institution to reduce the inherent risk associated with MSBs from high to moderate or low, as the industry standard designates MSBs as high-risk. However, the financial institution may incorporate additional risk factors to differentiate the risk of its MSBs (e.g., consider product/service offerings of the MSB, geography of operations).

1281. What is "de-risking"?

De-risking often refers to a financial institution's policy to exit from a high-risk customer group or activity to reduce its inherent risk profile. To avoid risk, as opposed to managing risk, some financial institutions may opt out of offering services to certain categories of high-risk customers (e.g., foreign correspondents, money transmitters, marijuana-related businesses [MRBs]) or customers located in high-risk geographies. While this may reduce risk and simplify the KYC and suspicious activity monitoring programs of individual financial institutions, it may increase overall money laundering risk in the system as money is moved through less transparent or less regulated financial systems (e.g., hawalas, financial institutions in lax AML/CFT jurisdictions).

Many financial institutions have taken steps to de-risk because of perceived regulatory pressures. U.S. and international authorities, however, have released guidance cautioning against wholesale de-risking while attempting to provide further clarification on regulatory expectations on servicing inherently high-risk customers (e.g., Office of the Comptroller of the Currency [OCC] Risk Management Guidance on Foreign Correspondent Banking, Federal Deposit Insurance Corporation [FDIC] Financial Institution Letter: Statement on Providing Banking Services, Financial Action Task Force [FATF] Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking, International Monetary Fund [IMF] The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action).

1282. Should low-risk activity be exempt from AML/CFT controls?

No. Just as financial institutions should not wholesale de-risking out of high-risk activity, low-risk activity should not be categorically exempted from controls.

1283. What is the appropriate level of ML/TF risk a financial institution should undertake?

As with any other category of risk, the level of ML/TF risk that a financial institution is willing to undertake should be based on the unique circumstances of the institution and based on a variety of factors including, but not limited to, the following:

- Experience and capabilities of the institution's personnel;
- Geographic footprint;
- Availability of tools and methodologies for managing the risk; and
- Willingness or adversity to reputation risk.

The acceptable level of risk should be documented in a risk appetite statement (RAS) that is developed by management and approved by the institution's board of directors.

1284. What is the purpose of a "Risk Appetite Statement" (RAS)?

A Risk Appetite Statement (RAS) defines the amount of risk an institution is willing to accept in pursuit of its strategy and desired goals. For smaller institutions, it may be enough to develop a single RAS (e.g., we will not engage in any business or with any customer unless we can moderate our money laundering residual risk to no more than a moderate risk). For larger, more complex financial institutions, developing cascading RASs by business line may be more appropriate. To be effective, a

RAS must be broadly and clearly communicated throughout the institution and must be accompanied by operating guidelines which can be measured and monitored.

1285. Are there ever circumstances where deficiencies in the control environment may result in a residual risk rating higher than the inherent risk?

As a general rule, the expectation would be that a strong or moderately strong control environment would moderate a financial institution's inherent risk. However, in rare circumstances where the control environment is significantly deficient, it may be prudent to increase the evaluation of inherent risk as a result of the poor control environment; especially in instances where the quality and availability of data for evaluating inherent risk raises a question about the accuracy of the inherent risk assessment.

1286. How frequently should risk assessments be conducted?

At a minimum, risk assessments should be reviewed and updated annually. Updates to both the assessment and the underlying methodology may also be warranted in the following scenarios:

- When new products or services are introduced
- When new markets are targeted (e.g., type of customer, country of domicile of customer)
- With each merger/acquisition
- With significant changes to domestic/international AML/CFT requirements and standards

1287. What role can technology and automation play in the execution of risk assessments?

An automated process facilitates information gathering, making it easier to aggregate results across departments/groups and to develop a consolidated view of risk, and may make it easier to communicate risk assessment results to a broad audience. Automation also facilitates the risk assessment updating process and helps create a more repeatable and sustainable process.

For additional guidance, please refer to the Risk Assessment Automation section.

1288. How are risk assessments addressed by FATF?

FATF addresses risk assessments in multiple ways, including, but not limited to, the following:

- **FATF Recommendations**
  - Recommendation 1 – Assessing Risks & Applying a Risk-Based Approach provides guidance on how to assess risks and apply a risk-based approach (RBA) in developing an AML/CFT system.

    The principles in Recommendation 1 can be used by governments/lawmakers in developing a risk-based AML/CFT system, by regulatory authorities in developing risk-based examinations and by financial institutions in developing risk-based AML/CFT Compliance Programs.

- Other recommendations address applying measures (e.g., customer due diligence, regulatory oversight) based on risk (e.g., Recommendation 10 – Customer Due Diligence, Recommendation 19 – Higher Risk Countries, Recommendation 26 – Regulation and Supervision of Financial Institutions, Recommendation 28 – Regulation and Supervision of DNFBPs)

- **Guidance on Risk Assessments** – FATF provides guidance on various types of risk assessments including, but not limited to, the following:
  - Government/lawmakers, law enforcement, regulatory authorities (e.g., National Money Laundering and Terrorist Financing Risk Assessment [2013])
  - Financial institutions and NBFIs (e.g., RBA Guidance for Casinos [2008], RBA Guidance for Money Services Businesses [2009])
  - Professional service providers (e.g., RBA Guidance for Legal Professionals [2008], RBA Guidance for Accountants [2008])
  - High-risk products and payment vehicles (e.g., Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services [2013], Virtual Currencies: Key Definitions and Potential AML/CFT Risks [2014])

- **Execution of Risk Assessments**
  - FATF published its first "Global Money Laundering & Terrorist Financing Threat Assessment" (GTA) in July 2010. The GTA provides a global overview of the most prevalent systemic ML/TF threats, their potential negative impacts, and suggested steps for governments to take to mitigate the harm caused by these threats.

While FATF does not explicitly address all types of assessments, the same principles can be applied to any area of focus by identifying a clear purpose and scope for each assessment. For further guidance on international AML/CFT standards, please refer to the sections: International Perspectives and Initiatives and Financial Action Task Force.

1289. Do the FATF Recommendations outline how often risk assessments should be conducted?

No. FATF Recommendations suggest risk assessments be conducted "on an ongoing basis."

1290. What is a national risk assessment? Can FATF's "National Money Laundering and Terrorist Financing Risk Assessment" be used by financial institutions to develop risk-based AML/CFT Compliance Programs?

A national risk assessment is an exercise by a government agency intended to identify systemic ML/TF risks on a country or national level to assist in the development of an effective AML/CFT system (e.g., regulatory, law enforcement). Similar to how regulatory authorities utilise a financial institution's risk assessment to develop a risk-based examination, national risk assessments are used by FATF to conduct mutual evaluations of a country's AML/CFT system.

While the "National Money Laundering and Terrorist Financing Risk Assessment" issued by FATF in February 2013 was intended to assist in the development and execution of a national risk assessment, many of the principles can be applied to the development of AML/CFT risk assessments at the financial institution level. Financial institutions can leverage the following principles and approaches in the development of their own risk assessments:

- Standard terminology (e.g., risk, threat)
- Defining scope and purpose of risk assessments including the execution of limited-scope assessments for aggregation in a broader assessment
- Organising assessments into stages (e.g., identify, assess/analyse, evaluate/understand)
- Examples of key risk factors/threats (e.g., drug trafficking, terrorism, human trafficking, arms trafficking, corruption, fraud, tax evasion, illegal gambling) and controls/measures (e.g., FATF Recommendations)
- Examples of quantitative and qualitative data to evaluate risks and controls (e.g., Recommendation 33 – Statistics such as suspicious transaction reports [STRs], observations and internal surveys by compliance and business line personnel)
- Use of results to drive strategic planning in the execution of a risk-based AML/CFT Compliance Program
- Guidance on how frequently risk assessments should be conducted
- Designation of an authority to develop and conduct risk assessments (e.g., compliance personnel)
- Commitment from high-level personnel to the execution and follow-up of risk assessments (e.g., board of directors, business line management)
- Documentation of methodology and results and sharing of appropriate level of detail with key personnel (e.g., senior management, general employees as part of AML/CFT training)

Financial institutions can also incorporate the results of national risk assessments into their own assessments by evaluating their exposure to risks/threats identified in the national risk assessment.

1291. Has the United States conducted a national risk assessment?

Yes. The most recent National Money Laundering Risk Assessment (NMLRA) was published in 2015 by the U.S. Treasury with input from multiple federal agencies and offices (e.g., Federal Bureau of Investigation [FBI], the Internal Revenue Service (IRS), the Drug Enforcement Administration [DEA], the Office of Foreign Assets Control [OFAC], Financial Crimes Enforcement Network [FinCEN], Immigration and Customs Enforcement [ICE], United States Secret Service [USSS]) as an update to the U.S. Money Laundering Threat Assessment (MLTA), published in 2005. The NMLRA contains detailed analyses of money laundering vulnerabilities, similar to those identified in the MLTA (2005) across banking, insurance, casinos and MSBs including, but not limited to, the following:

- Use of currency and monetary instruments (e.g., bank notes, cashier's check, money order, traveller's check) in transactions structured under regulatory recordkeeping and reporting

thresholds (e.g., US$10,000 for currency transactions, US$3,000 for monetary instruments), commingled with licit funds, used in bulk cash smuggling activities and in trade-based money laundering (TBML) (e.g., Black Market Peso Exchange [BMPE]);

- Establishment of bank and brokerage accounts using nominees (i.e., agent acting by or on behalf of a third party) to disguise the identities of the individuals who control the accounts;
- Creation of legal entities (e.g., shell companies, shelf companies) without accurate information about the identity of the beneficial owner;
- Misuse of products and services (e.g., correspondent banking services, funnel accounts, omnibus accounts, remote deposit capture [RDC], prepaid access cards, virtual currency) resulting from deficient compliance with AML/CFT obligations; and
- Complicit merchants (e.g., wholesalers), third-party payment processors (TPPPs), money services businesses (MSBs) (e.g., foreign exchange dealers, money transmitters) and other financial institutions (e.g., banks, broker-dealers, casinos) with deficient compliance with AML/CFT obligations, and in some cases, wittingly facilitating illicit activity.

The National Terrorist Financing Risk Assessment (NTFRA) was also published in 2015 by the U.S. Treasury, with input from many of the same federal agencies and offices that collaborated on the NMLRA, as well as Customs and Border Protection (CBP), the Bureau of Counterterrorism, the Bureau of International Narcotics and Law Enforcement and the National Counterterrorism Center (NCTC). The NTFRA contains detailed analyses of terrorist financing vulnerabilities, including, but not limited to, the following:

- Global terrorism and terrorist financing threats
  - Terrorist threats to the United States (e.g., al-Qaeda, Al-Nusrah Front [ANF], Islamic State of Iraq and the Levant [ISIL], Hizballah, Hamas, Taliban, Haqqani Network, foreign terrorist fighters)
  - Terrorist financing sources (e.g., kidnapping for ransom [KFR], extortion, drug trafficking, private donations through charitable organisations, state sponsorship, cybercrime, identity theft) and vulnerabilities (e.g., charitable organisations, licensed and unlicensed MSBs, foreign correspondent banking, cash smuggling, virtual currency)
- Counterterrorism and CFT efforts
  - Law enforcement efforts (e.g., reorientation, interagency coordination and cooperation, information sharing)
  - Financial/regulatory efforts (e.g., Office of Foreign Assets Control [OFAC] sanctions)
  - International efforts (e.g., United Nations [UN], Financial Action Task Force [FATF])

FATF recommends that each country continues to conduct self-assessments to evaluate and ultimately mitigate money laundering and terrorist financing risks on a national level. For further guidance, please refer to the Risk Assessments section.

1292. What are the most common gaps with risk assessments?

The most common gaps with risk assessments include, but are not limited to, the following:

- The methodology does not identify and/or quantify, in whole or partially, all inherent risk factors.
- The methodology does not identify and/or assess, in whole or partially, all controls/control environments.
- The methodology does not calculate residual risk.
- The scope is inadequate or incomplete (e.g., certain business lines excluded, not adequately assessed or "double counted" due to shared customers).
- A consistent methodology is not used by each business line or entity within an enterprise.
- The methodology does not utilise clear or consistent scoring or weighting when calculating risk classifications.
- The risk bands used to determine risk classifications are arbitrarily determined and not supported by analytics.
- There is undocumented or unclear use of risk overrides (e.g., changes in risk classifications from high to low risk).
- There is a lack of quality data (quantitative or qualitative).
- Only the results, and not the methodology itself, are documented.
- The results of the executed methodology are not used to drive strategic changes in the AML/CFT Compliance Program.
- The results are not current (e.g., outdated or not reflective of latest business environment/geographic profile/product offerings/customers).
- The methodology is not current.
- There is a lack of involvement of key senior management and compliance personnel in the development of the methodology.
- There is a lack of involvement of key business unit stakeholders in the execution.
- There is a lack of or inadequate training on the purpose of the assessment and the meaning of the results with compliance personnel, business line management and senior management.
- There is over-reliance on a third party to develop and execute the assessment.
- There is a lack of ongoing validation of risk-based models.

1293. What guidance has been provided on risk assessments?

The FFIEC BSA/AML Examination Manual provides guidance for banks with respect to the identification of specific risk categories, the level of detail of the analysis of specific risk categories, the impact of the risk assessment on the organisation's AML Program, the recommended frequency with

which the assessment should be conducted, and the circumstances prompting an organisation to update its risk assessment. However, it does not dictate the format the risk assessment should take.

Additional resources include, but are not limited to, the following:

- **Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption** (2016) by the Wolfsberg Group
- **National Money Laundering and Terrorist Financing Risk Assessment** (2013) by the Financial Action Task Force (FATF)
- **Sound Management of Risks Related to Money Laundering and Financing of Terrorism (2014)** – (Merges and supersedes previous publications "Customer Due Diligence for Banks" [2001] and "Consolidated KYC Risk Management" [2004]) by the Basel Committee on Banking Supervision of the Bank for International Settlements (BIS)
- **The World Bank Risk Assessment Methodology by the World Bank** (WB)
- **The International Monetary Fund Staff's ML/FT NRA Methodology by the International Monetary Fund (IMF)** (Money Laundering/Financing of Terrorism National Risk Assessment)
- **Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing** (2007) by FATF
- **FATF Recommendation 1: Assessing Risks & Applying a Risk-Based Approach** (2012) by the FATF
- **Guidance for Dealers, Including Certain Retailers, of Precious Metals, Precious Stones, or Jewels, on Conducting a Risk Assessment of Their Foreign Suppliers** (2008) by the Financial Crimes Enforcement Network (FinCEN)
- **Guidance on a Risk-Based Approach for Managing Money Laundering Risks** (2006) by the Wolfsberg Group
- **Money Laundering and Terrorist Financing Risk Assessment Strategies** (2008) by FATF
- **Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services** (2013) by FATF
- **Risk-Based Approach for Casinos** (2008) by FATF
- **Risk-Based Approach Guidance for Legal Professionals** (2008) by FATF
- **Risk-Based Approach for the Life Insurance Sector** (2009) by FATF
- **RBA Guidance for Trust and Company Service Providers** (TCSPs) (2008) by FATF
- **RBA Guidance for Real Estate Agents** (2008) by FATF
- **RBA Guidance for Accountants** (2008) by FATF

- **RBA High-Level Principles and Procedures for Dealers in Precious Metals and Dealers in Precious Stones** (2008) by FATF
- **Guidance for Money Services Businesses – Risk-Based Approach** (2009) by FATF
- **Risk Matrix for Financial Institutions** (2005) by the Office of Foreign Assets Control (OFAC)
- **Risk Matrix for the Securities Sector** (2008) by OFAC
- **Risk Matrix for the Charitable Sector** (2007) by OFAC

Key guidance on "de-risking" includes, but is not limited to, the following:

- **Risk Management Guidance on Periodic Risk Reevaluation of Foreign Correspondent Banking** (2016) by the Office of the Comptroller of the Currency (OCC)
- **The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action** (2016) by the International Monetary Fund (IMF)
- **Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking** (2014) by the FATF

Enterprisewide Risk Assessment

1294. What is an enterprisewide risk assessment?

An enterprisewide risk assessment is an exercise intended to identify the aggregate money laundering (ML) and terrorist financing (TF) risks facing an organisation that may not be apparent in a risk assessment focused on a line of business, legal entity, or other assessment unit. In other words, it is the big picture view, or profile, of an organisation's ML/TF risks that aggregates the results of other risk assessment exercises in order to quantify and relate the total risks for the organisation to the established risk appetite and tolerance for the enterprise.

1295. Should all business lines and legal entities be treated equally when developing an enterprisewide risk assessment?

Some institutions use significance measures to aggregate different business lines and legal entities into the enterprisewide risk assessment. For example, business lines and legal entities which are larger in total assets or produce the most revenue for the institution will have a greater bearing on the enterprisewide risk assessment than smaller, less significant business lines or legal entities.

1296. Why are enterprisewide risk assessments important?

Enterprisewide risk assessments may disclose systemic ML/TF risk that is not otherwise apparent. For example, multiple business lines may note certain ML/TF risk, but conclude that the risk is not high for the business line. When aggregated across the organisation, however, the perception of such risk and the need to better manage it might take on greater significance.

Horizontal Risk Assessment

1297. What is a horizontal risk assessment?

A horizontal risk assessment is an exercise intended to identify systemic ML/TF risks of designated high-risk products/services and/or customers across an organisation regardless of which line of business or legal entity owns these activities or customers. One technique for developing horizontal risk assessments is to establish key risk indicators (KRIs) to support the quantitative assessment of risk. For example, KRIs used to assess the risk of wire activity might include the following:

- Customer Considerations: Total Wires for High-Risk Customers to Aggregate Total Wires, by dollar volume and by count.
- Geographic Considerations: Total Wires to/from High-Risk Jurisdictions, by dollar volume and by count.

Information is collected from all lines of business/legal entities based on these KRIs and consolidated to provide an overall picture of both the level and, over time, the trend of the risk.

1298. Why are horizontal risk assessments important?

The intent of a horizontal risk assessment is to identify an institution's total exposure to these high-risk products/services and customers, even though the exposure to a single business line or legal entity may not be significant.

If the right data can be harnessed, horizontal risk assessments can be executed more frequently than other risk assessments (e.g., line of business/legal entity risk assessment), thus better enabling organisations by identifying potential issues earlier.

Line of Business/Legal Entity Risk Assessment

1299. What is a line of business (LOB)/legal entity (LE) risk assessment?

An LOB/LE risk assessment is an exercise intended to identify the level of vulnerability of each line of business or legal entity to ML/TF.

This is accomplished by evaluating, for a specific business line or legal entity, among other factors, the inherent risk of products/services, the customer base (e.g., type, location) and geography (e.g., customers, transactions, operations) and the controls (e.g., policies and procedures, customer acceptance and maintenance standards, transaction monitoring, management oversight, training, personnel) mitigating those risks at the business line or legal entity level.

Results of LOB risk assessments can be aggregated to provide a legal entity assessment. LE risk assessments then can be aggregated to provide an enterprise-level assessment of the financial institution's ML/TF risks and controls.

1300. What are the typical components of an LOB/LE risk assessment methodology?

A typical LOB/LE risk assessment methodology addresses inherent risks and mitigating controls. Inherent risk includes the risks posed by the customer base, products/services/transactions, and geographic footprint (e.g., customers, transactions, operations) of the financial institution. Controls or the control environment can include the customer acceptance and maintenance program, the transaction monitoring program, training, and management oversight (e.g., compliance, audit, senior management, board of directors).

Residual risk is then determined by netting the level of risk (e.g., high, moderate, low) against the strength of the control and control environment (e.g., strong, moderate, low).

1301. How should the LOB/LE risk assessment be conducted?

The method used to conduct the LOB/LE risk assessment will depend on the complexity of the financial institution and the technology support available to the organisation. A combination of methods (e.g., questionnaires, internally or externally developed databases, web-based applications) often is used to collect the business line or legal entity information effectively. These methods should enable Compliance to review and validate the risk assessment results and engage in discussions with management to discuss the final risk rating and ensure management understands the ML/TF risk in the business line or legal entity.

1302. Should all business lines of a financial institution be included in the LOB risk assessment?

The business lines included in the LOB risk assessment will vary by organisation; however, all business lines providing products and services to customers or supporting customer transactions (e.g., deposit or wire operations) should be included in the LOB risk assessment to ensure no potential area of risk is overlooked. Business lines with risk management functions (e.g., customer acceptance, monitoring) should be included to ensure all controls/control environments are assessed.

1303. Should a financial institution use the same LOB/LE assessment methodology to assess each of its business lines?

In general, it is recommended that a financial institution use the same methodology to assess the risks and controls of its business lines or legal entities to ensure that risk is measured consistently across the institution and enterprise.

Business lines have flexibility in their response to the risks identified in the assessment. For example, one business line may have a higher risk appetite/tolerance than another business line and, therefore, may choose to implement more limited controls to mitigate these risks.

A consistent approach will allow for results to be aggregated at a legal entity or enterprise-level and enable comparisons of results over time.

1304. Should a financial institution be concerned if many of its business lines result in a high inherent risk rating?

An institution should be concerned if there are non-existent or ineffective controls to mitigate the high inherent risk.

Geographic Risk Assessment

1305. What is a geographic risk assessment?

A geographic risk assessment is an exercise intended to identify the inherent ML/TF risks of the international and domestic jurisdictions in which a financial institution and its customers conduct business.

1306. Why are geographic risk assessments important?

Geographic risk assessments support all other risk assessments as each has a geographic component (e.g., location of branches, affiliates and customers, destination/origin countries of international transactions). A sound geographic risk assessment methodology is crucial in developing a consistent AML/CFT policy, especially when conducting business in high-risk jurisdictions.

1307. What countries should financial institutions classify as increased risk for the purpose of performing a risk assessment?

Financial institutions should develop an objective approach to determine which countries should be considered at increased risk to money laundering or terrorist financing. Factors that can be considered include, but are not limited to, the following:

- Strength of AML/CFT infrastructure (e.g., legal and regulatory framework)
- Subject to government sanctions
- Degree of corruption
- Designation as a sponsor of terrorism
- Designation as a tax haven
- Strength of secrecy laws (i.e., favours/encourages secrecy)
- Designation as a drug trafficking region
- Designation as a human trafficking/smuggling region

1308. Where can a financial institution obtain information on high-risk countries?

Fortunately, analyses performed by numerous government agencies and organisations can be leveraged to help in the process of identifying high-risk countries.

Commonly used sources for this purpose include, but are not limited to, the following:

- Countries sanctioned by the Office of Foreign Assets Control (OFAC)

- Countries designated as jurisdictions of primary money laundering concern under Section 311 – Special Measures of the USA PATRIOT Act
- International Narcotics Control Strategy Report (INCSR) issued by the U.S. Department of State
- Country Reports on Terrorism issued by the U.S. Department of State
- Global Corruption Report and Corruption Perceptions Index issued by Transparency International (TI)
- Offshore financial centres (OFC), as identified by the International Monetary Fund (IMF)
- Uncooperative tax havens, as identified by the Organisation for Economic Co-operation and Development (OECD)
- Jurisdictions or countries identified as "high-risk and non-cooperative jurisdictions" by the Financial Action Task Force (FATF)
- Mutual evaluation reports (MERs) by FATF
- Trafficking in Persons Report (TIP Report) by the U.S. State Department

Financial institutions should consider adding countries identified as high-risk based on prior experiences and transaction history.

Additional guidance can be found through numerous other government and not-for-profit agencies. It is important to note, however, that the rationale for assigning country risk should be both well documented and defendable.

1309. Is it only a customer's country of domicile that should be considered or are there other geographic considerations that may have a bearing on risk?

In addition to the country of domicile, a customer's risk to money laundering and terrorist financing also may be impacted by where the customer conducts activities (e.g., business operations, origination/destination countries of wire transfers), so it also may be appropriate for the risk assessment to consider the following:

- Countries/jurisdictions where the customer principally operates
- Countries/jurisdictions of the customers/suppliers of the business
- Origination/destination countries/jurisdictions of transactions
- Countries/jurisdictions of other relationships (e.g., accounts held at financial institutions in tax havens, PEPs)

1310. Are high-risk jurisdictions limited to international locations?

No. High-risk geographic locations may include domestic locales, such as financial institutions doing business within, or having customers located within, a U.S. government-designated high-risk geographic location.

Domestic high-risk geographic locations include, but are not limited to, the following:

- High Intensity Drug Trafficking Areas (HIDTAs)
- High Intensity Financial Crimes Areas (HIFCAs)
- States with weak anti-human trafficking laws identified in the Polaris Project's Annual State Ratings Report

1311. How is the term "domestic" defined?

The term "domestic" is often defined as activity taking place entirely within national borders, but, the European Union, for example, defines domestic in some instances to include all of the countries operating within the borders of the European Economic Area (EEA), a supra-national jurisdiction.

1312. What is a High Intensity Drug Trafficking Area (HIDTA)?

HIDTAs were authorised in the Anti-Drug Abuse Act of 1988 to assist law enforcement with concentrating its efforts with drug control at the federal, state and local levels. HIDTAs are designated by area. Since the original designation of five HIDTAs in 1990, the program has expanded to 28 areas of the country which include approximately 18.3 percent of all counties in the United States and a little over 65.5 percent of the U.S. population. These include, but are not limited to, the following:

- Appalachia (e.g., counties in Tennessee, Kentucky, Virginia and West Virginia)
- New York/New Jersey
- Rocky Mountain (e.g., counties in Colorado, Utah, Wyoming and Montana)
- South Florida
- Southwest Border (e.g., southern regions of California, Arizona, New Mexico and Texas)

Funding for HIDTAs has faced some challenges under the Trump administration, as the White House Office of Management and Budget (OMB) has called the program duplicative with other federal programs (e.g., Drug-Free Communities [DFC]). However, funding was ultimately provided as many officials argued for the need for these federal programs during the country's opioid crisis.

1313. What is the purpose of designating a HIDTA?

The HIDTA designation serves to enhance and coordinate federal, state and local law enforcement drug control efforts. The program accomplishes this by institutionalising teamwork among the agencies, synchronising investments in strategy-based systems, and better focusing all agencies on the same outcomes. The program provides agencies with coordination, equipment, technology and additional resources to combat drug trafficking and its harmful consequences in critical regions of the United States.

1314. How are HIDTAs designated?

HIDTAs are designated by the Director of the Office of National Drug Control Policy (ONDCP), in consultation with the Attorney General, the Secretary of the Treasury, the Secretary of Homeland

Security, heads of the national drug control program agencies, and the governor of each applicable state. A coalition of interested law enforcement agencies from an area also may petition for designation as a HIDTA.

1315. What primarily is taken into consideration when designating a HIDTA?

The primary factors considered by the Director of the ONDCP when reviewing a petition to create a HIDTA are the extent to which:

- The area is a significant centre of illegal drug production, manufacturing, importation or distribution.
- State, local and tribal law enforcement agencies have committed resources to respond to the drug trafficking problem in the area, thereby indicating a determination to respond aggressively to the problem.
- Drug-related activities in the area are having a significant, harmful impact in the area and in other areas of the country.
- A significant increase in the allocation of federal resources is necessary to respond adequately to drug-related activities in the area.

1316. What is a High Intensity Financial Crimes Area (HIFCA)?

HIFCAs were defined in the Money Laundering and Financial Crimes Strategy Act of 1998 to assist law enforcement with concentrating its efforts in high-intensity money laundering zones at the federal, state and local levels. HIFCAs may be defined geographically; they also can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions. Examples include, but are not limited to, the following:

- California (e.g., southern district, northern district)
- Chicago
- Southwest Border (e.g., Arizona, southern region of Texas)
- New York/New Jersey
- Puerto Rico/U.S. Virgin Islands
- South Florida

1317. What is the purpose of designating a HIFCA?

The HIFCA designation serves to concentrate federal, state and local law enforcement efforts in order to combat money laundering in an area designated as a high-intensity money laundering zone. To accomplish this coordinated effort, a money laundering action team is created within each HIFCA. This team contains members from all relevant federal, state and local law enforcement, prosecutors, and financial regulators. It focuses on tracing funds to/from the HIFCA to/from other areas, and on collaborating on investigative techniques within the HIFCA and between the HIFCA and other areas. It

also has an asset forfeiture component, and the setup of the team provides for an easier flow of information among all members of the HIFCA.

1318. How are HIFCAs designated?

HIFCAs can be designated in two ways:

- Areas can be proposed by the Secretary of the Treasury or the Attorney General.
- Designations can come through an application process in which localities submit applications through FinCEN.

1319. How does a locality petition to become a HIFCA?

If a locality wishes to be designated as a HIFCA, it should request HIFCA designation in writing to the FinCEN Director. The letter should include:

- A description of the proposed area/entity/industry
- A focus and plan for the counter-money laundering projects to be supported
- Reasoning as to why such a designation is appropriate, which considers relevant statutory standards
- A designated point of contact

Applications are first reviewed by the HIFCA Designation Working Group, which is co-chaired by the Departments of the Treasury and Justice, and composed of senior officials from the Criminal Division of the DOJ, FBI, DEA, IRS-CI, U.S. Customs Service, FinCEN, U.S. Secret Service, U.S. Postal Inspection Service and other appropriate agencies. The Working Group then provides a recommendation to the Treasury Secretary and the Attorney General. Finally, the decision made by the Treasury Secretary and Attorney General is provided to the applicant in writing.

1320. What is a "narcotics and bulk currency corridor"?

Narcotics and bulk currency corridors are established distribution channels or logistical highways for the transportation of narcotics and the illicit proceeds from the sale of narcotics. Visual presentations and descriptions of these corridors have been detailed in the following:

- **National Drug Threat Assessment (2010)**, Appendix A – Presents multiple maps with distribution channels by select drug trafficking organisations (DTOs) (e.g., Asian, Colombian, Cuban, Dominican, Mexican), by involvement of street gangs, and by drug threat (e.g., cocaine, heroin, methamphetamines, marijuana, prescription drugs);
- **The Department of Justice's Regional Drug Transportation Corridors** – Describes drug transportation corridors within the United States by drug and by originating/destination cities.

1321. Are narcotics and bulk currency corridors the same as HIDTAs?

Narcotics and bulk currency corridors may or may not be located in HIDTAs.

1322. How much of the United States falls into a HIDTA or HIFCA region?

According to the Office of the National Drug Control Policy, in recent years, nearly 20 percent of U.S. counties and over 60 percent of the U.S. population are located in HIDTAs.

Even fewer U.S. counties are designated as HIFCAs. HIFCAs are often located in HIDTAs.

1323. How can financial institutions incorporate high-risk domestic regions (e.g., HIDTAs, HIFCAs) into their AML/CFT Compliance Programs?

Financial institutions can incorporate high-risk domestic regions into their AML/CFT Compliance Programs in the following ways:

- Importing HIFCA/HIDTA data (e.g., based on ZIP codes) into customer on-boarding systems and suspicious activity monitoring software to apply enhanced measures to customers located in or transacting to/from high-risk domestic regions;
- Reviewing HIFCA/HIDTA data when conducting investigations occurring in or near these regions to understand specific types of underlying criminal activities; and
- Applying enhanced measures on branches located in HIFCA/HIDTA regions.

1324. As a high-risk region, how is the "border" defined between the U.S. and Mexico? In other words, how far north should this high-risk region extend beyond the actual border?

According to the definition of HIFCAs, the "border" includes counties on the border, counties adjacent to counties on the border, and in some cases, the next tier of counties.

1325. What are the most common gaps with geographic risk assessments?

The most common gaps with geographic risk assessments include, but are not limited to, the following:

- Reducing the rating of a high-risk jurisdiction based on familiarity and volume of activity, inconsistent with leading practices; and
- Failure to update ratings timely to reflect current events.

Product/Service Risk Assessment

1326. What is a product/service risk assessment?

A product/service risk assessment is an exercise intended to identify the inherent ML/TF risks of the specific products and services offered by a financial institution.

1327. Why are product/service risk assessments important?

A sound product/service risk assessment methodology is crucial in developing a consistent AML/CFT policy, especially when providing high-risk products and services.

1328. What products/services/transactions pose a higher money laundering and terrorist financing risk?

Products/services that allow unlimited third-party transactions (e.g., demand deposit accounts), those that operate through channels with limited transparency (e.g., internet banking, telephone banking, pouch activity, prepaid access, ATM, trust), and those that may involve significant international transactions (e.g., correspondent banking) pose the highest risk.

Transactions that are processed quickly and electronically for customer convenience (e.g., wire transfers), are difficult to trace (e.g., cash), and are negotiable (e.g., monetary instruments, drafts, bearer securities, stored-value cards) also are susceptible to money laundering and terrorist financing.

Examples include, but are not limited to, the following:

- Currency
- Funds transfers
- Monetary instruments
- Trade finance activities
- Correspondent banking accounts and related services (e.g., payable-through accounts [PTAs]), pouch activities, U.S. dollar drafts)
- Trust and asset management services

For further guidance, please refer to the Know Your Customer's Activities: Product Considerations section.

1329. What is a third-party transaction?

A third-party transaction is defined as a transfer of funds to/from the account holder to/from an individual/entity that is different than the customer/account holder. It includes all types of transactions (e.g., wires, checks), regardless of direction (i.e., incoming, outgoing). "Third party" distinguishes the recipient/sender of the funds from the account holder. The individual/entity also can be a customer of the same financial institution, although the risk is greater when the individual/entity is not a customer of the financial institution, as the latter was not subject to the same customer acceptance procedures. Examples of third-party transactions are provided below:

- **Example 1**: Customer John sends a wire to beneficiary Jane from his deposit account. The deposit account allows third-party activity.
- **Example 2**: Customer John establishes a loan with Bank ABC and wishes to disburse the proceeds of the loan to his business partner, Jane. The financial institution's policy does not allow loan proceeds to be disbursed to a third party, as Jane is a third party.
- **Example 3**: Customer John established a certificate of deposit (CD) account with Bank ABC and wishes to liquidate the CD and disburse the funds to his wife, Jane. The financial institution's policy does not allow funds from the CD to be disbursed to a third party.

- **Example 4:** Correspondent bank (respondent bank) established a payable-through account (PTA) and either conducts transactions on behalf of its customers or allows customers to conduct transactions directly through the PTA. The customer's customers are third parties.

Customer Risk Assessment

1330. What is a customer risk assessment?

A customer risk assessment, sometimes referred to as customer risk rating (CRR), is an exercise intended to identify the level of inherent ML/TF risks in the types of customers (e.g., individual, institutional, financial institution, not-for-profit) served by a financial institution.

1331. Is a customer risk rating the same as a customer risk assessment?

A customer risk rating is used to determine the risk level of an individual customer or customer segments, as is often the case with retail customers. This rating is used, among other reasons, to determine due diligence and enhanced due diligence needs. A customer risk assessment is the overall assessment of the risk profile of the customer portfolio in a line of business or legal entity.

1332. Are financial institutions required to implement a customer risk assessment?

The risk assessment guidance provided in the FFIEC BSA/AML Examination Manual cautions financial institutions not to "define or treat all members of a specific category of customer as posing the same level of risk." Further guidance is provided to consider other customer-specific risk factors to assess customer risk. Leading practice dictates all financial institutions should have a customer risk assessment methodology in place.

1333. What factors should financial institutions consider in their customer risk assessment methodology?

Financial institutions should consider the following factors, as applicable, when assessing the money laundering and terrorist financing risk of customers:

- Occupation or nature of business
- Method/channel of account opening (e.g., face-to-face, mail, internet, solicited/unsolicited)
- Length of relationship with the client
- Financial institution's prior experience with and knowledge of the customer and his/her/its transactions (e.g., previous internal investigations, Currency Transaction Report [CTR] and/or Suspicious Activity Report [SAR] filings)
- Source(s) of income
- Type(s) of product(s)/service(s) provided
- Expected pattern of activity and actual transaction activity in the account in terms of transaction types, dollar volume and frequency

- Geographic considerations (e.g., residency or principal place[s] of business, incorporation, citizenship, origination/destination of funds, location of primary customers)
- Status as or relationship with other high-risk individuals/entities (e.g., politically exposed persons [PEPs])

A customer risk assessment is not one-dimensional. A customer may have a low-risk business/occupation but reside in a high-risk geographic jurisdiction. Money laundering and terrorist financing risks are assessed on the overall profile of a customer, not on any one factor.

1334. How is a customer risk assessment used?

Customer risk assessments can be used in multiple ways, including, but not limited to, the following:

- To determine the extent of due diligence for each customer (e.g., requiring provision of additional information, site visits, senior management approvals, reviews of profiles);
- To determine the scope and frequency of monitoring; and
- As inputs into other risk assessments (e.g., line of business/legal entity risk assessments, horizontal risk assessments).

1335. How should a customer risk assessment be conducted?

Customer risk assessments can be implemented using automated or manual processes. Automating customer risk assessments (e.g., as part of the account-opening platform, transaction monitoring system, back-end system) promotes consistency and objectivity in the process. Some institutions have implemented procedures whereby risk ratings are produced automatically based on the information provided in the account-opening process. In some institutions, the responsible account officer will assign the initial risk rating, and Compliance will review and approve the rating, either for all new customers, high-risk customers or on a sample basis.

If automated risk ratings are used, financial institutions should ensure they are updatable, particularly when the customer profile changes after the account-opening process.

For additional information on automating the customer risk assessment methodology, please refer to the AML/CFT Technology section.

1336. Should a financial institution develop one risk assessment methodology that applies to all of its customers?

It may be desirable to develop different risk assessment methodologies for different types of customers (e.g., individuals, non-individuals) or customer segments (e.g., corporate, financial institution, retail, private banking) in order to consider specific factors that may not apply to all customers. For example, a risk assessment methodology for correspondent customers should consider the underlying customers of the bank who/that may utilise the U.S. correspondent account. For PEPs, a risk assessment methodology may consider the country, level of office and degree of relationship of the PEP (in the case of family members and close affiliates).

1337. Is it always necessary or appropriate to risk-rate each customer separately?

In some instances, it may be acceptable to risk-rate customers on a segment basis. For example, homogeneous segments of retail customers might be risk-rated by groups based on the nature of products provided and levels of activity, rather than risk-rated individually.

1338. Should a customer risk assessment methodology be developed on an account level, customer level or household level?

A customer risk assessment methodology should be developed on a customer level, not an account level. Conducting a risk assessment on an account level prevents the financial institution from assessing the risk of all of the customer's relationships; rather, it focuses on a small snapshot of the customer's activity. Conducting a risk assessment on the customer level helps to ensure the financial institution understands the risks posed by all of the customer's accounts and relationships (e.g., household).

Ideally, risk should be assessed on a household or relationship level; however, the ability of an institution to do this will be a function of how it manages its data (i.e., its ability to link related accounts). For example, if high-risk business ABC Company and its owners have accounts at an institution, both the business and retail accounts should be rated as high-risk.

1339. How is the term "household" defined?

A "household" is generally defined as an entity consisting of two or more distinct customers who share a common factor such as an address, phone number or business owner.

1340. What should a financial institution do if it can only conduct an assessment on an account level as opposed to a customer level?

To compensate for this data limitation, a financial institution can conduct monitoring or request enhanced due diligence (EDD) on a customer or a household level. For example, if a customer has 10 accounts, of which only one resulted in a high-risk rating, all nine other accounts can be assigned a high-risk rating and be included in the monitoring or EDD request.

1341. Should financial institutions consider not opening an account or terminating an existing relationship if a customer is rated as high-risk, a practice known as de-risking?

A rating of high-risk does not imply that a customer relationship should not be extended or should be terminated. The decision to open or retain a relationship with high-risk customers should be defined by policy and by the risk tolerances established by the institution's senior management and board of directors and documented in a Risk Appetite Statement (RAS). Opening or maintaining the relationship simply means that due diligence for the customer should be more extensive and that the customer's transactions should be subject to heightened scrutiny.

U.S. and international authorities have released guidance cautioning against wholesale de-risking while attempting to provide further clarification on regulatory expectations on servicing inherently high-risk customers (e.g., Office of the Comptroller of the Currency [OCC] Risk Management Guidance

on Foreign Correspondent Banking, Federal Deposit Insurance Corporation [FDIC] Financial Institution Letter: Statement on Providing Banking Services, Financial Action Task Force [FATF] Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking, International Monetary Fund [IMF] The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action).

1342. How can a financial institution stratify the risk of its customers if all of its target customers are considered high-risk by industry standards (e.g., a financial institution and its customers are located primarily in high-risk jurisdictions)?

One high-risk factor alone does not necessarily mean a customer is high-risk. Financial institutions should use multiple factors when stratifying customers into high-, moderate- and low-risk segments. For example, a community bank located in a High Intensity Drug Trafficking Area (HIDTA) may have many customers with elevated risk based only on their location in the HIDTA zone. Upon further review, however, a majority of these customers may have had a relationship with the financial institution for more than five years, and most of them have been using low-risk products and services (e.g., safe deposit boxes, five-year CDs). These factors, combined with others, can be used to separate high-risk customers from moderate- and low-risk customers.

1343. When should a customer risk assessment be conducted?

Customer risk assessments typically are conducted at the inception of each new client relationship, based on information provided during the account-opening process. Some institutions initially flag a customer as new, but defer conducting the assessment for a short period (e.g., three months) to include actual transaction activity as a factor in the assessment.

While some believe it is more advantageous to conduct the customer risk assessment at the inception of the relationship, others argue that a customer risk assessment is more meaningful if it includes actual transaction activity as a factor as opposed to just theory (e.g., expected transaction activity). In either instance, customers should be assessed continually throughout the duration of the relationship.

1344. How often should customer risk ratings be re-evaluated by a financial institution?

Financial institutions should, on a regular basis, re-evaluate their customers. In addition, re-evaluations should take place shortly after new information about a customer becomes known to the financial institution. For example, when:

- A customer relationship manager becomes aware an individual is starting a new business in a high-risk activity or jurisdiction
- A customer begins using high-risk products or services
- A customer relationship manager notices significant changes in the number or amount of a customer's transactions
- A customer relationship manager reads an article about a customer recently indicted for illicit activities (e.g., drug offenses)
- The financial institution receives a grand jury subpoena naming the customer

1345. Can a financial institution customise or modify results of a customer risk assessment?

Yes. Usually the ability to modify an assigned risk score rests with Compliance. Changes to the score should be clearly documented. Some financial institutions limit reducing risk scores to customers who have maintained relationships with the financial institution for a minimum of one year.

1346. How often should a financial institution's customer risk assessment methodology be re-evaluated?

The customer risk assessment methodology should be re-evaluated when new products or services are introduced, with each merger/acquisition, and when new markets are targeted (e.g., type of customer, country of domicile of customer).

1347. What are the benefits of using technology to support the customer risk rating process?

There are several benefits that result from automating the customer risk rating (CRR) process. For example:

- An automated customer risk scoring process that derives inputs from information collected for KYC purposes eliminates much of the subjectivity that can result from a manual scoring process.
- Automated systems, by their nature, facilitate more dynamic risk ratings, allowing for real time adjustments based on changing circumstances.
- Automated customer risk scores can more easily be incorporated into transaction monitoring systems to create more risk-aware rules and scenarios.

For further guidance, please refer to the Risk Assessment Automation section.

1348. How can a financial institution test its customer risk assessment model and methodology?

The financial institution can test its customer risk assessment model and methodology by determining whether:

- Data sources are complete and properly fed
- Algorithms are properly functioning
- Risk ratings are logical, based on experience of compliance personnel
- Customer risk assessment results are used according to policies and procedures

1349. How can a financial institution validate the outcome of its customer risk assessment model?

A financial institution can validate its customer risk assessment model by running existing customer information through the model to ensure the results are consistent with the perceived risk of the customer.

1350. What are the most common gaps with customer risk assessments?

The most common gaps with customer risk assessments include, but are not limited to, the following:

- The methodology does not identify and/or quantify, in whole or partially, all inherent risk factors
- The same methodology is applied to different customer types (e.g., individual, business, financial institution)
- Not all customers are assessed
- The assessment is not executed in a timely manner, initially or ongoing
- The results of the methodology are not used to determine the extent of due diligence for each customer (e.g., requiring provision of additional information, site visits, senior management approvals, reviews of profiles) and the scope and frequency of monitoring
- Only the results, and not the methodology itself, are documented
- The classifications of high, moderate and/or low risk are inconsistent with leading practice
- The methodology is not current
- There is a lack of or inadequate controls on the ability to modify results of assessments

1351. What business types/occupations pose a higher money laundering and terrorist financing risk?

Business types and occupations considered to be high-risk for money laundering and terrorist financing include those that are cash-intensive; those that allow for the easy conversion of cash into other types of assets; those that provide the opportunity to abuse authoritative powers and assist in disguising the illegal transfer of funds; those that lack transparency; those that involve international transactions/customers; and those that offer high-risk or high-value products. High-risk business types/occupations include, but are not limited to, the following:

- Accountants/accounting firms
- Aircraft engine/part and military armoured vehicle manufacturing
- Amusement, gambling and recreation activities
- Attorneys/law firms
- Art/antiques dealers
- Car washes
- Common carriers of currency or monetary instruments (e.g., armoured car services [ACS])
- Charitable organisations/Nongovernmental organisations (NGOs)
- Cigarette distributors
- Consumer electronics rentals and dealers

- Convenience stores
- Flight training
- Gas stations
- Importers/exporters
- Leather manufacturing, finishing and goods stores
- Liquor stores
- Marijuana-related businesses [MRBs]
- Bank and Nonbank Financial Institutions (NBFIs) or their agents
- Notaries
- Offshore companies
- Parking garages
- Pawnbrokers
- Precious metals, precious stones or jewellery dealers and wholesalers
- Businesses that operate privately-owned Automated Teller Machines (ATMs)
- Racetracks
- Real estate brokers
- Restaurants/bars
- Retail establishments
- Politically exposed persons (PEPs) and political organisations
- Small arms and ammunition manufacturing
- Sole practitioners
- Tobacco wholesalers
- Transportation services and equipment rental
- Trusts and custodial entities
- Textile businesses
- Travel agencies and traveller accommodations
- Vehicle dealers
- Vending machine operators

Financial institutions may decide it is appropriate to add other business types/occupations based on a variety of sources, such as guidance provided by regulatory agencies or the FATF, or their own risk

analyses. For example, as an institution's internal investigation database expands, an institution may consider adding the business type/occupation of customers who/that have had a significant number of SAR/CTR filings.

Certain crimes, such as human trafficking may have their own high-risk types/occupations. For further guidance, please refer to the Human Trafficking and Migrant Smuggling section.

For further guidance on select customer types, please refer to the Know Your Customer Types section.

1352. Are high-risk activities limited to businesses?

No. High-risk activities include activities for both businesses and individuals (e.g., accountants, attorneys). For example, if a customer owns or is a principal of a high-risk business, that factor should be considered as part of the risk assessment. It is important to note that accounts established to support an accountant's or attorney's business pose different risks than personal accounts of these high-risk professional service providers.

1353. Should each nature of business/occupation be treated with the same risk within its scoring methodology?

A financial institution should clearly document how each nature of business/occupation is treated in its methodology. Some financial institutions, in line with the guidance issued by the FATF, risk-rate certain businesses/occupations by the types of services provided (e.g., lawyers who sell real estate on behalf of their customers are risk-rated differently than those who draft wills), thus allowing one nature of business/occupation to have a different risk rating depending upon the services provided.

1354. How can financial institutions identify high-risk customers in their existing customer bases?

Financial institutions can identify high-risk customers in their existing customer bases by doing the following:

- Reviewing North American Industry Classification System (NAICS) codes for high-risk business activities
- Conducting keyword searches (e.g., check casher, *casa de cambio*, jewellery, car) in customer databases and transaction details (e.g., wires)
- Reviewing high-volume/value transaction reports (e.g., cash, wires)
- Screening against FinCEN's MSB list
- Screening against proprietary databases (e.g., PEPs)
- Reviewing subjects of investigations and SARs
- Querying account officers
- Querying customers directly

Office of Foreign Assets Control/Sanctions Risk Assessment

1355. What is an Office of Foreign Assets Control (OFAC)/Sanctions risk assessment?

An OFAC/Sanctions risk assessment attempts to identify an organisation's level of vulnerability to noncompliance with economic sanctions administered by OFAC or any sanctions program as required by the financial institution's policy. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types, the geographic origin and destination of transactions, and the strength of the controls mitigating those risks.

For further guidance on OFAC and other sanctions requirements, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1356. Are financial institutions required to implement an OFAC/Sanctions risk assessment?

There is no requirement per se that institutions conduct OFAC/Sanctions risk assessments. However, banking regulators, in particular, expect financial institutions to conduct an OFAC/Sanctions risk assessment. Best practice suggests all financial institutions should conduct an assessment to understand their level of vulnerability to noncompliance with OFAC and applicable sanctions programs.

1357. How often should OFAC/Sanctions risk assessments be conducted?

At a minimum, OFAC/Sanctions risk assessments should be reviewed and updated annually. Updates to both the assessment and the underlying methodology may also be warranted in the following scenarios:

- When new products or services are introduced
- When new markets are targeted (e.g., type of customer, country of domicile of customer)
- With each merger/acquisition
- With significant changes to domestic/international sanctions requirements and standards

1358. How should an OFAC/Sanctions risk assessment be conducted?

The method used to conduct the OFAC/Sanctions risk assessment will depend on the complexity of the financial institution and the technology support available to the organisation. A combination of methods (e.g., questionnaires, internally or externally developed databases, web-based applications) is often used to collect the product/process information effectively and enable Compliance to review and validate the risk assessment results.

1359. Which customers pose a higher OFAC/Sanctions compliance risk?

Customers posing a higher OFAC/Sanctions compliance risk include, but are not limited to:

- Non-resident aliens (NRAs)
- Foreign customers (e.g., foreign exchange houses)

- Customers with foreign operations or a foreign customer base
- Nonprofit/charitable organisations
- Trading companies acting as informal money transmitters

1360. What types of products and services pose a higher OFAC/Sanctions compliance risk?

Per the FFIEC BSA/AML Examination Manual, products posing a higher OFAC/Sanctions compliance risk include, but are not limited to:

- International funds transfers
- Cross-border automated clearing house (ACH) transactions
- Commercial letters of credit
- Transactional electronic banking
- Foreign correspondent services
- Management of sovereign debt
- Payable-through accounts (PTAs)
- Products or services provided to entities or individuals without accounts at the financial institution (e.g., monetary instruments, wires)
- Online activities

1361. What guidance has been provided on OFAC/Sanctions risk assessments?

The FFIEC BSA/AML Examination Manual provides guidance with respect to the identification of specific risk categories, the level of detail of the analysis of specific risk categories, the impact of the risk assessment on the organisation's OFAC Sanctions Compliance Program, the recommended frequency for which the assessment should be conducted, and the circumstances prompting an organisation to update its risk assessments, but specifically avoids providing guidance on the form that risk assessments should take.

1362. What are the most common gaps with OFAC/Sanctions risk assessments?

The most common gaps with OFAC/Sanctions risk assessments include, but are not limited to, the following:

- The methodology does not identify and/or quantify, in whole or partially, all inherent risk factors
- The methodology does not identify and/or assess, in whole or partially, all controls/control environments
- The methodology does not calculate residual risk
- A consistent methodology is not used by each business line
- Inadequate or incomplete scope (e.g., certain business lines excluded, not adequately assessed)

- The methodology does not utilise clear or consistent scoring or weighting
- The classifications of high, moderate and/or low risk are inconsistent with leading practice
- Only the results, and not the methodology itself, are documented
- The results of the executed methodology are not used to drive strategic changes in the OFAC/Sanctions Compliance Program
- The results are not current (e.g., outdated or not reflective of latest business environment/geographic profile/product offerings/customers)
- The methodology is not current
- Lack of or inadequate training on the purpose of the assessment and the meaning of the results with Compliance, business line management and senior management
- There is a lack of involvement of key senior management and compliance personnel in the development of the methodology
- Over-reliance on a third party to develop and execute the assessment

KNOW YOUR CUSTOMER, CUSTOMER DUE DILIGENCE AND ENHANCED DUE DILIGENCE

KYC Basics

1363. What is Know Your Customer (KYC)?

Know Your Customer (KYC) generally refers to the steps taken by a financial institution to:

- Establish and verify the identity of a customer/account holder or, in select cases, non-account holders (e.g., beneficial owners);
- Understand the nature of a customer's activities (ultimately to be satisfied that the source of the customer's funds is legitimate and activity is consistent with stated purpose) at the inception of the relationship and ongoing based on risk; and
- Assess the money laundering (ML) and terrorist financing (TF) risks associated with that customer.

A KYC program, also referred to as an onboarding program or customer acceptance and maintenance program, generally includes the following components:

- **Customer identification program (CIP)** – CIP requires the collection, verification and recordkeeping of customer identification information and the screening of customers against lists of known terrorists. For additional guidance on CIP, please refer to the Section 326 – Verification of Identification section of the USA PATRIOT Act section.
- **Customer due diligence (CDD)** – CDD is baseline information obtained for all customers. Information obtained for CDD should enable a financial institution to obtain and verify the identity of a customer, gain a basic understanding of a customer's activities and assess the risks associated with that customer.
- **Enhanced due diligence (EDD)** – EDD, sometimes referred to as special due diligence, refers to additional information collected for higher-risk customers to provide a deeper understanding of customer activity to mitigate the associated heightened ML/TF risks.
- **Special due diligence** – Special due diligence refers to the due diligence requirements explicitly required by regulation for private banking and certain correspondent banking customers.
- **Simplified due diligence** – Simplified due diligence is a term used in some jurisdictions (e.g., Europe) to describe abbreviated due diligence requirements that may be applied to select categories of customers. Simplified Due Diligence is not a principle that has specific meaning in the U.S., but it may be included in the KYC policy and procedures of foreign bank organisations (FBOs) doing business in the United States. Under the 4th EU Directive, the reasons for applying

Simplified Due Diligence to a customer must be supported on a case by case basis rather than types of customers being automatically exempt from standard CDD.

1364. Who is a "customer" for purposes of CIP?

Section 326 – Verification of Identification of the USA PATRIOT Act, also known as the "Customer identification program (CIP), defines a "customer" as any person who opens a new account or enters into another formal relationship after October 1, 2003. "Person" in this context includes individuals, corporations, partnerships, trusts or estates, joint stock companies, joint ventures or other incorporated organisations or groups. As noted above, some CDD requirements apply to persons who may not be included in this definition of "customer" but to non-account holders such as beneficial owners as well.

For further guidance, please refer to the Customer Defined section of Section 326 of the USA PATRIOT Act.

1365. Which parties to an account should be subject to KYC?

Financial institutions should consider applying risk-based due diligence to other parties in addition to named account holders, including, but not limited to, the following:

- Beneficial owners, including those with less than the minimum percentage of control as indicated by AML/CFT laws and regulations (e.g., 10 percent by the Section 312 of the USA PATRIOT Act, 25 percent by the Beneficial Ownership Rule)
- Authorised signers
- Guarantors
- Third parties (e.g., agent, broker) conducting transactions by or on behalf of account holders

1366. Should financial institutions conduct due diligence on non-customers?

In instances when transactions are conducted on behalf of non-customers, financial institutions may consider conducting due diligence of the parties involved in the transaction/action executed by the financial institution. This may occur before the transaction is conducted to determine whether the transaction should be processed or afterward to determine if the activity should be reported as potentially suspicious activity.

1367. Is the term "due diligence" restricted to KYC?

The term "due diligence" may refer to all of the activities undertaken by a financial institution during the customer lifecycle including customer onboarding, updating of customer information and/or suspicious activity monitoring. For further guidance on suspicious activity monitoring programs, please refer to the sections: Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Reports.

1368. What new obligations does the "Customer Due Diligence Requirements for Financial Institutions" final rule impose on covered financial institutions?

Prior to the issuance of the final rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule), covered financial institutions were required to obtain beneficial ownership information in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule issued in July 2016 with full compliance required by May 2018, expands beneficial ownership requirements for all financial institutions currently subject to CIP requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to all legal entity customers Specifically, covered financial institutions are required to identify and verify beneficial owners of legal entity customers with 25 percent or greater ownership or significant control of legal entity customers.

For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

1369. Are financial institutions required to link their KYC programs and risk assessments to their suspicious activity monitoring program?

Federal regulations do not explicitly require covered financial institutions to link their KYC programs and risk assessments directly to their suspicious activity monitoring program (e.g., risk-based customer profiles tied to specific monitoring rules in transaction monitoring systems). However, the Beneficial Ownership Rule clarified that financial institutions are expected to utilise all available information (e.g., collected CDD, risk profiles) as part of their investigative processes to determine if customer activity is potentially suspicious, implying the need to link these processes.

On a state level, in July 2016, the New York State Department of Financial Services (DFS) issued Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications, requiring covered financial institutions in New York to explicitly link customer information and risk profiles to transaction monitoring programs, effective in early 2017.

Whether the requirement is explicit or implied, leading practice suggests that a risk-based monitoring program based on customer data is more effective at generating "alerts" for potentially suspicious activity. For further guidance on suspicious activity monitoring, please refer to the Transaction Monitoring, Investigations and Red Flags section. For further guidance on risk assessments, please refer to the Risk Assessments section.

1370. What should a financial institution consider when developing its KYC program?

A financial institution may consider the following when developing its KYC program:

- Complying with AML/CFT laws and regulations:

  - USA PATRIOT Act's Section 311 – Special Measures – Some measures require providing notices to foreign respondents of prohibited activity;
  - USA PATRIOT Act's Section 312 – Special Due Diligence (SDD) for Correspondent Accounts and Private Banking Accounts (including Politically Exposed Persons [PEPs]);
  - USA PATRIOT Act's Section 319 - Forfeiture of Funds in United States Interbank Accounts – Requires the collection of Foreign Bank Certifications on foreign respondents;
  - USA PATRIOT Act's Section 326 – Verification of Identification (also known as Customer Identification Program [CIP]); and
  - Customer Due Diligence Requirements for Financial Institutions – Referred to as Beneficial Ownership Rule, finalised in July 2016, outlines covered financial institutions' requirements related to beneficial owners.
- Incorporating international standards, including, but not limited to, the following:
  - FATF Recommendations 10 and 22 – Customer Due Diligence and DNFBPs: Customer Due Diligence
  - FATF Recommendations 11 and 17 – Recordkeeping and Reliance on Third Parties
  - FATF Recommendation 12 – Politically Exposed Persons
  - FATF Recommendation 13 – Correspondent Banking
  - FATF Recommendation 14 – Money or Value Transfer Systems
  - FATF Recommendation 24 and 25 – Transparency and Beneficial Ownership of Legal Persons and Legal Arrangements
  - Wolfsberg Anti-Money Laundering Principles for Correspondent Banking (2014)
  - Wolfsberg Anti-Money Laundering Principles for Private Banking (2012)
- Collecting relevant information to enable the assessment of ML and TF risks of all customers
- Understanding the extent to which public data sources or shared utilities can be used to obtain reliable information about customers
- Collecting relevant information to provide business line and compliance personnel adequate context to determine if monitored transactions are consistent with the customer's nature of business/occupation
- Understanding information available to verify customer identity, which may differ across customer and geographic markets
- Understanding technology available to collect, store, screen and risk rate customer information, including both internal and third-party solutions

For further guidance on international AML/CFT standards, please refer to the International Perspectives and Initiatives section. For further guidance on technology solutions, please refer to the AML/CFT Technology section.

1371. How can technology support the KYC process?

Technology can be used as part of the customer onboarding process to verify customer information (e.g., customer identification program [CIP]); to streamline the collection and exchange of data through the use of KYC utilities; to collect and store customer due diligence (CDD), calculate the customer risk rating (CRR) of the customer, and perform and store enhanced due diligence (EDD) information. Collectively the customer profile of each customer (e.g., CRR, CIP, CDD, EDD, associated documents) should be readily accessible to various institutional parties, including account officers and individuals responsible for monitoring and investigation; and to track and schedule the need for customer updates and visitations.

For further guidance, please refer to the AML/CFT Technology section.

1372. How can technology support the updating of KYC information?

Simple tickler file software can be used to keep track of due dates for updating KYC information or scheduling customer visits, as well as for tracking the expiration date of customer documents, such as identification documents or USA PATRIOT Act Certifications. Workflow features embedded in these systems allow financial institutions to assign follow-up responsibility and to track status.

1373. What is a KYC Utility?

A Know Your Customer (KYC) Utility is a central repository that stores the data and documents required to support a financial institution's KYC procedures. KYC Utilities may take different forms, including:

- **Industry Collaborated/Supported Utility**: a utility developed and maintained by a consortium of financial institutions
- **Service Provider Utility**: a utility or service provided by a third-party vendor
- **Jurisdictional Utility**: a utility designed to undertake core due diligence within a given jurisdiction

For further guidance, please refer to the AML/CFT Technology and KYC Process sections.

1374. What is “de-risking” and how can it impact a financial institution’s KYC program?

“De-risking” often refers to a financial institution’s policy to exit from a high-risk customer group or activity to reduce its inherent risk profile. To avoid risk, as opposed to managing risk, some financial institutions may opt out of offering services to categories of high-risk customers (e.g., foreign correspondents, money transmitters, marijuana-related businesses [MRBs]) or customers located in high-risk geographies. While this may reduce risk and simplify the KYC programs of individual financial institutions, it may increase overall money laundering risk in the system as money is moved

through less transparent or less regulated financial systems (e.g., hawalas, financial institutions in lax AML/CFT jurisdictions).

U.S. and international authorities have released guidance cautioning against wholesale de-risking while attempting to provide further clarification on regulatory expectations on servicing inherently high-risk customers (e.g., Office of the Comptroller of the Currency [OCC] Risk Management Guidance on Foreign Correspondent Banking, Federal Deposit Insurance Corporation [FDIC] Financial Institution Letter: Statement on Providing Banking Services, Financial Action Task Force [FATF] Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking, International Monetary Fund [IMF] The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action). For further guidance, please refer to the Risk Assessments section.

1375. What is "KYC remediation"?

"KYC remediation" is the enhancement of KYC information to an agreed-upon standard which is designed to focus on the highest risk elements of the KYC profile. A financial institution may voluntarily undertake remedial KYC projects to reduce its risk profile or may be required to by regulators who have found the financial institution's KYC program to be deficient.

The real purpose of a KYC remediation project is to ensure that the ML/TF risks posed by a customer are understood and mitigated, not simply to confirm that the KYC file is complete or updated to the latest KYC standard.

1376. What are key factors that may indicate the need for a KYC remediation project?

The following are key factors that may indicate the need for a KYC remediation project:

- Weak onboarding processes (e.g., inadequate controls over required fields, multiple onboarding systems that do not maintain current and correct customer information, lack of experienced staff); and
- Lack of or inadequate periodic-review processes of KYC data; and
- Lack of alignment between the KYC program and transaction monitoring.

1377. What are some challenges with KYC remediation projects?

The following include some of the challenges that financial institutions may experience when completing KYC remediation projects:

- Underestimating the level of effort to complete the KYC remediation project (e.g., identify population, review a file, contact a customer, update core systems) leading to project abandonment or restarting;
- Lack of agreement on key terms (e.g., client) across complex enterprises (e.g., lines of business, intermediaries, agents, distributors, geographies);
- Lack of existing client data to develop a risk-based approach to prioritise highest-risk customers for remediation;

- Lack of consistency in KYC processes among lines of businesses or geographies that may share customers;
- Unclear remediation project parameters established by the financial institution, if voluntary, or by regulators, if mandatory;
- Lack of focus on key data points (e.g., source of funds/wealth, high-risk business type/industry, negative news) when updating files leading to completing file reviews without reducing inherent risk;
- Unclear client-exit process for customers that have been determined to lie outside of the financial institution's risk appetite or when requests for further information have been unsuccessful; and
- Lack of transition to "business as usual" post project that incorporates regular periodic-reviews of KYC data.

CDD vs. EDD & Other Due Diligence Requirements

1378. What additional information might a financial institution request as part of a CDD/EDD and special due diligence process?

EDD might include additional steps to validate information provided by the customer, and/or conduct additional research and inquiry about the customer, which in the extreme might include engaging a third party to investigate the client. EDD also may include, but not be limited to, obtaining the following information:

- Occupation or nature of business
- Purpose of account
- Expected pattern of activity in the account in terms of transaction types, dollar volume and frequency
- Expected origination and destination of funds
- Articles of incorporation, partnership agreements and business certificates
- Understanding of the customer's customers (particularly in the case of foreign correspondent banks and international businesses)
- Identification of the nominal and beneficial owners of accounts (particularly in the case of private banking clients and foreign correspondent banks)
- Details of other personal and business relationships the customer maintains
- Details of other banking relationships the customer maintains
- Approximate salary or annual sales
- Additional sources of income
- Description/history of source of wealth

- Net worth
- Annual reports, financial statements (audited if available)
- AML/CFT policies, procedures and controls (in the case of foreign correspondent banks, money services businesses [MSBs] and other nonbank financial institutions)
- Third-party documentation, such as bank references and credit reports
- Local market reputation through review of media reports or other means
- Copies of any correspondence with client (e.g., letters, faxes, emails), including call reports/site visits
- Proximity of the residence/employment/place of business to the financial institution
- In the United States, special due diligence generally refers to due diligence prescribed by AML/CFT laws and regulations for select high-risk customers (e.g., foreign correspondents, private banking). SDD may include, but not be limited to, obtaining the following information as required by various sections of the USA PATRIOT Act: A Foreign Bank Certification, also known as a USA PATRIOT Act Certification, which requires foreign respondents to certify the following:
  - Physical presence/regulated affiliated status;
  - Prohibition of indirect use of correspondent accounts by foreign shell banks; and
  - Ownership status (for non-public institutions).
- Certification for Purposes of Section 104(e) of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA) and 31 C.F.R. 1060.300 (CISADA Certification), requires U.S. financial institutions to obtain information from their foreign correspondents relating to correspondent or transaction activity conducted on behalf of Iranian-linked financial institutions and Iran's Islamic Revolutionary Guard Corps (IGRC), upon written request by FinCEN.

1379. Is obtaining someone's occupation the same as identifying the source of income?

Typically, the source of most people's income is from their occupation. However, the source of income may be unclear if a customer responds to this question with any of the following:

- Self-employed
- Business owner
- Unemployed
- Housewife/househusband
- Student
- Retired

Additionally, some customers may have sources of income beyond their employment.

1380. Are financial institutions required to obtain the source of funds from their customers?

Financial institutions are specifically required to obtain the source of funds from their private banking customers pursuant to Section 312 of the USA PATRIOT Act. However, leading practice suggests financial institutions include the source of funds as part of their CDD or EDD program, which is typically accomplished by obtaining employment information (e.g., name of employer, occupation) from retail customers.

1381. Is there a difference between expected activity and average activity?

Yes. Expected activity describes anticipated activity from a particular customer or account category, including types, amounts, geographical locations where transactions are done and frequency of transactions. Average activity describes the mean activity historically conducted by a customer through an account. Expected activity provides a narrative for the types of activities that are deemed normal for a particular customer or account. When due diligence is accurate, expected activity and average activity are consistent.

Understanding both expected and average activities are extremely important in detecting potentially suspicious activity.

1382. How can a financial institution determine "normal" expected activity for each of its customers?

Expected activity can be obtained directly from each customer during the account opening process or developed independently by the financial institution based on historical transaction history for an individual customer or segments of a financial institution's customer population.

For example, some financial institutions ask for the following information directly from their customers during the account opening process:

- Deposits/credits per month (number and volume)
- Withdrawals/debits per month (number and volume)
- Cash transactions (number and volume)
- Wire transfer transactions (number and volume)
- Purpose of account
- Origination/destination country(ies) of incoming/outgoing wire transfers or other types of payments

To facilitate the account opening process, some financial institutions provide ranges of activity with triggers to ask for additional information if specified dollar thresholds are met or higher risk activities are identified. It is important to note that although customers may answer these questions to the best of their ability, their responses are often guesstimates and may need to be reviewed and revised throughout the duration of the relationship.

Expected activity can also be obtained by analysing underlying transaction activity based on defined segments, including, but not limited to, the following:

- Customer type (e.g., business, individual)
- Geography (e.g., home address, place of business)
- Nature of business/occupation
- Account type (e.g., savings, checking, certificate of deposit, loan)
- Account balance
- Transaction volume

For example, some financial institutions have opted to segment their customer population by customer type, geography (foreign/domestic) and class based on volume of transaction activity and balances held in their accounts to establish expected activity. In some cases, these expected activity profiles were used to compare actual transaction activity in suspicious transaction monitoring software. Typically, this due diligence is used to conduct customer risk assessments and provide context for investigations.

1383. What are some examples of "purpose of account"?

For individuals, common responses to the question of "purpose of account" include, but are not limited to, the following:

- Daily living expenses
- Savings (e.g., college, retirement, vacation)

For businesses, common responses include, but are not limited to, the following:

- Payroll
- Operating account
- Manage treasury activities

The challenge is obtaining a meaningful response that will aid financial institutions in understanding what types of transaction activities can be expected in their customers' accounts. Some financial institutions have gone as far as asking for the purpose of specific transactions, particularly in the case of international wire transfers. While it is common practice to ask for the purpose with lending products, it has not been consistently applied with other product types.

1384. Should financial institutions apply EDD to other types of customers beyond the special due diligence required by Section 312 of the USA PATRIOT Act?

Section 312 covers additional information required for foreign correspondent accounts, private banking accounts and politically exposed persons (PEPs), sometimes referred to as special due diligence. A financial institution's EDD requirements should cover all types of customers and accounts that it deems to pose higher risk (e.g., money services businesses [MSBs], trusts, private investment companies [PICs]), not just correspondents, private banking and PEPs.

Detailed guidance specific to select high-risk customers has been provided in this publication for the following:

- Non-resident Aliens and Foreign Persons
- Politically exposed persons (PEPs)
- Foreign embassies and consulates
- Private banking
- Professional service providers (e.g., attorneys, accountants)
- Trust and asset management service providers
- Business entities (e.g., shell companies, private investment companies [PICs])
- Correspondent banking
- Charitable organisations/nongovernmental organisations (NGOs)
- Third-party payment processors (TPPPs)
- Deposit brokers
- Owners of privately owned automated teller machines (ATMs)

For additional information and guidance issued on EDD and special due diligence for these specific types of customers, please refer to the Know Your Customer Types section.

1385. Should an institution simplify its KYC program by performing EDD on all of its customers?

Unless a financial institution operates a mono-line business where all of its customers are deemed to be high-risk (e.g., private banking), conducting EDD on all customers may create an unnecessary burden and undermine the purpose of a risk-based AML Program. Even in a mono-line private banking business, some customers, by nature of the types of accounts they have or the transactions they conduct, may be lower risk than others.

1386. Should an institution aim to minimise CDD collected on all of its customers?

Financial institutions that establish an overly cumbersome CDD program may run the risk of turning away customers who are reluctant to provide extensive personal information. Additionally, financial institutions need to balance the degree of collected information with the risks associated with privacy laws that outline what can be obtained and kept.

1387. Should a customer's status as an affiliate of the financial institution impact applied CDD/EDD and special due diligence procedures?

CDD/EDD and special due diligence procedures should be consistently applied to affiliated and non-affiliated institutions; however, the level of verification of collected information for affiliates may not be as extensive as for non-affiliates.

1388. What international efforts have been made to collect and share due diligence information on correspondent banks?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) has developed a KYC Registry that collects correspondent banking due diligence information and documentation submitted by financial institutions in accordance with international best practices (e.g., Wolfsberg AML Principles for Correspondent Banking). The KYC Registry aims to create a global standard from a single validated source to ease the complex and often inconsistent due diligence standards for correspondent banking. Examples of due diligence and documents maintained by the KYC Registry include, but are not limited to, the following:

- Banking licenses
- Corporate governance documents (e.g., by-laws, articles of incorporation)
- Foreign bank certifications as required by Section 319 of the USA PATRIOT Act
- AML/CFT Policies and Procedures related to correspondent banking services

Participation in the registry is voluntary.

Additionally, multiple vendors providing regulatory solutions, often referred to as "regtech," are providing agile cloud-based technology solutions for KYC repositories and customer verification across the globe. For further guidance on AML/CFT technology solutions, please refer to the AML/CFT Technology section.

1389. When should a financial institution initially collect CDD/EDD and special due diligence information?

Some financial institutions obtain CDD/EDD and special due diligence information (when necessary) during the account-opening process. While it is best to collect due diligence at inception to mitigate risks better, some financial may choose to defer collecting EDD information until they have some experience with the performance of the account.

1390. Should a financial institution update CDD and EDD after the initial account-opening process?

Although this practice was already in place in the industry, the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) issued in May 2016, clarified that CDD/EDD and special due diligence should be updated on an ongoing basis based on risk consistent with existing requirements for conducting on-going suspicious activity monitoring. If a financial institution detects significant changes to the customer's profile (e.g., volume of transaction activity, risk level, account type) as a result of normal monitoring, financial institutions are required to update customer records to reflect these changes. For example, if the customer's transaction profile indicates that the customer is expected to conduct an average of six transactions per month in an amount of US$20,000 each, and then the customer's transaction size and frequency increase to 20 transactions for an average of US$100,000 per month, the financial institution should seek to understand the reason for the change in transaction activity. Once the financial institution has satisfied itself that it has obtained a

reasonable explanation, this information should be used to update the customer's profile. For example, a customer's employment status may change from student to professional, thereby changing the expected level and type of activity in his or her account. If the financial institution is not able to satisfy itself that the change is reasonable, then it needs to determine if a SAR must be filed and if any other actions, which may include termination, are appropriate.

Updating the customer's CDD/EDD and special due diligence can enable a financial institution to direct better its monitoring and investigation efforts. An up-to-date customer profile can help avoid having transactions flagged unnecessarily, thus enabling the financial institution to devote time to those transactions that need to be investigated.

Beyond updates prompted by a financial institution's monitoring activities, financial institutions should review accounts periodically to identify any changes in profile. The frequency and nature of this review is not a categorical requirement but should be based on the customer's risk rating and results of suspicious activity monitoring.

1391. Where should the information obtained during the CDD/EDD and special due diligence processes be stored?

Storing CDD/EDD and special due diligence information as paper files or images may limit the ability to use critical information, such as occupation or expected activity. Housing CDD/EDD and special due diligence information in an electronic format, such as an automated risk assessment or KYC system, however, allows it to be queried and updated more easily. Increasingly, regulators are suggesting, at least for larger financial institutions, that customer information should be maintained electronically. For additional guidance on AML/CFT technology relating to customer databases, customer risk assessment and suspicious transaction monitoring systems, please refer to the AML/CFT Technology section.

KYC Challenges

1392. What types of customers may present KYC challenges?

KYC challenges may arise with the following customer types:

- **Customers who are self-employed "business owners," unemployed, housewives/househusbands, students or retired** – The aforementioned responses to the question of employment/source of income do not provide financial institutions with a clear understanding of their customers' source(s) of income. Further due diligence may be required (e.g., request additional information, conduct more frequent monitoring for potentially suspicious activity).
- **Doing Business As (DBAs)** – In some cases, customers use personal accounts for their DBAs, and either commingle personal and business activities or simply use personal accounts for business purposes. This makes it difficult for financial institutions to collect the appropriate due diligence at the inception of the relationship and to monitor for potentially suspicious transactions on an ongoing basis.

- **Professional service providers (e.g., attorneys, accountants)** – Financial institutions should distinguish between accounts opened by professional service providers for personal use versus accounts established for business when conducting due diligence and evaluating risk. These types of customers can pose challenges when attempting to identify the source of income and, where applicable, the beneficial owners of funds/assets in these accounts, especially depending on how client funds are managed. For additional guidance, please refer to the Professional Service Providers section.
- **Correspondent banking customers** – Due to the complex nature of correspondent banking businesses and the heightened ML/TF risks, especially with clearing activities for foreign correspondents and payable-through accounts (PTAs), many financial institutions establish separate departments specialising in collecting due diligence and monitoring correspondent banking relationships. For further guidance, please refer to the Correspondent Banking section.
- **Private banking customers** – Due to the strict privacy and confidential culture of private bankers, high net-worth powerful clientele, and the international nature and propensity of clients to use complex business entities (e.g., trusts), financial institutions often establish separate departments or assign relationship managers to conduct due diligence and service private banking clients.
- **Politically exposed persons (PEPs)** – Due to the difficulty in identifying PEPs (and close associates) and heightened ML/TF and corruption risks, PEPs may require EDD such as requiring senior management approval prior to establishing an account relationship. For further guidance, please refer to the sections: Senior Foreign Political Figures and Politically Exposed Persons.
- **Charitable organisations** – A charitable organisation may state its mission or status as a not-for-profit when asked to provide "nature of business." The challenge with charitable organisations is in understanding their sources of income, which ultimately speaks to understanding their donor base. For additional guidance, please refer to the Charitable Organisations and Nongovernmental Organisations section.
- **Trusts** – Similar to charitable organisations, many of the standard due diligence questions for businesses (or non-personal customer types) do not apply to trusts (e.g., nature of business). Many financial institutions have separate trust departments to manage these types of customers. For additional guidance, please refer to the Trust and Asset Management Services section.
- **Certain types of business entities (e.g., shell companies, private investment companies [PICs], limited liability companies [LLCs])** – Business entities typically organised for certain purposes (e.g., tax and estate planning) are vulnerable to abuse due to their lack of ownership transparency, and in some instances, formation in high-risk jurisdictions in lax regulatory environments. For additional guidance, please refer to the Business Entities: Shell Companies, Private Investment Companies section.
- **Nonbank financial institutions (NBFIs)** – NBFIs (e.g., money services businesses [MSBs], casinos and card clubs) pose additional challenges due to the heightened ML/TF risks of the

NBFI's customers. Many NBFIs are also subject to their own AML/CFT requirements. For further guidance, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

1393. What challenges have financial institutions faced when developing their KYC program?

Some challenges include, but are not limited to, the following:

- Identifying and complying with KYC standards globally and across mixed financial groups
- Tailoring and implementing requirements for high-risk customers
- Finding a balance between effective and overly burdensome CDD/EDD requirements
- Identifying the true beneficiary beyond the nominal customer (e.g., beneficial owners)
- Identifying and documenting holistic customer relationship lines of business or legal entities
- Critically evaluating customer information to determine if it is reasonable
- Developing ongoing, risk-based due diligence programs
- Applying updated standards to existing customer populations

Beneficial Owners

1394. What is a "beneficial owner"?

A "beneficial owner" generally an individual who has a level of control over, or entitlement to the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, without corresponding authority to control, manage or direct the account, such as an account in which a minority age child is the beneficiary, does not cause an individual to become a beneficial owner.

The term reflects a recognition that a named account holder may not necessarily the person who ultimately controls such funds or who is ultimately entitled to such funds. "Control" or "entitlement" in this context is to be distinguished from mere legal title or signature authority.

Two key AML/CFT regulations offer differing definitions and requirements for beneficial owners:

- USA PATRIOT Act Section 312 - Special Due Diligence for Correspondent Accounts and Private Banking Accounts
- FinCEN's "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule)

Section 312 defines "beneficial owners" as "individual[s] who [have] a level of control over [of 10 percent], or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual[s], directly or indirectly, to control, manage or direct the account."

The Beneficial Ownership Rule uses a two-pronged concept – ownership and effective control – by defining a "beneficial owner" as a natural person, not another legal entity, who meets the following criteria:

- **Ownership prong** – Each individual, up to four, who owns, directly or indirectly, 25 percent or more of the equity interest in a legal entity customer; and
- **Control prong** – At least one individual who exercises significant responsibility to control, manage or direct (e.g., a C-suite Executive, Managing Member, General Partner, President, Treasurer) the legal entity.

In cases where an individual is both a 25 percent owner and meets the control definition, that same individual can be defined as a beneficial owner under both prongs. From an industry perspective, the second prong improves upon the definition in the advanced notice of proposed rulemaking (ANPR) issued in 2012. The earlier definition would have required the identification of the individual who had "greater responsibility than any other individual."

1395. Are covered financial institutions required to verify the status as beneficial owners is accurate in addition to verifying the identifying information of beneficial owners?

No. Financial institutions may rely upon the information provided by the individual establishing the relationship. Unless the financial institution has reason to doubt the information, covered financial institutions are not required to verify the status of individuals as beneficial owners.

1396. What are the heightened money laundering risks of beneficial owners?

By using nominal account names rather than disclosing the true owners of the funds, money launderers and other criminal elements can conceal the source, purpose or actual ownership of funds, thus enabling them to circumvent controls to combat money laundering; engage in terrorist financing and fraud; evade sanctions and taxes; and commit other financial crimes.

1397. What other concerns should financial institutions consider when maintaining accounts for beneficial owners?

Another potential risk to financial institutions that maintain accounts for which beneficial owners have not been identified is that they may unknowingly be doing business with individuals or entities who/that are on government sanctions lists. Or, they may fail to obtain other records or file reports required by the Bank Secrecy Act (BSA), such as Currency Transaction Reports (CTRs).

1398. Do covered financial institutions have new obligations related to USA PATRIOT Act Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities?

According to FinCEN guidance, FIN-2016-G003, covered financial institutions do not have new obligations under Section 314(a) of the USA PATRIOT Act. For further guidance on information sharing, please refer to Section 314(a) – Cooperation among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities.

1399. What is expected of an effective CDD program according to the Beneficial Ownership Rule?

The Beneficial Ownership Rule states that an effective CDD program must include, at a minimum, the following four elements:

- Conducting initial due diligence on customers, including identifying the customer and verifying that customer's identity as appropriate on a risk basis, at the time of account opening;
- Identifying the beneficial owner(s) of legal entity customers, subject to exemptions, and verifying the beneficial owner(s)' identity;
- Understanding the purpose and intended nature of the customer/account for the purpose of assessing risk, referred to as the customer risk profile; and
- Conducting ongoing monitoring of the customer relationship pursuant to a risk-based approach and conducting additional CDD as appropriate, based on such monitoring and scrutiny, for the purposes of identifying and reporting suspicious activity.

1400. Are these new elements for a CDD program?

While the due diligence requirement for beneficial owners is new for some financial institutions, the Beneficial Ownership Rule notes that the other three elements of an effective CDD Program are already required by existing BSA laws and regulations and that this final rule only serves to make them explicit requirements for the sake of clarity and consistency. The first element of an effective CDD program is already addressed by existing CIP requirements. The third and fourth elements are implicitly required by existing suspicious activity reporting requirements. For further guidance, please refer to the Suspicious Activity Reports section.

1401. Are there any circumstances where financial institutions must obtain information on beneficial owners with 25 percent or less ownership/control?

Prior to the Beneficial Ownership Rule, covered financial institutions were required to obtain beneficial ownership information in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

Financial institutions are required to identify beneficial owners with 10 percent or more ownership/control.

For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

1402. To what types of financial institutions do the requirements of the Beneficial Ownership Rule apply?

Covered institutions include those currently subject to CIP requirements under USA PATRIOT Act Section 326 – Verification of Identification:

- Banks
- Broker-dealers in securities
- Mutual funds
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities

1403. Is FinCEN considering including other types of financial institutions under the Beneficial Ownership Rule?

Yes, FinCEN considered whether the scope of the Beneficial Ownership Rule should be expanded to include the following types of financial institutions:

- Money services businesses (MSBs)
- Providers of prepaid access
- Insurance companies
- Casinos and card clubs
- Dealers in precious metals, precious stones and jewels
- Nonbank residential mortgage lenders or originators (RMLOs)

1404. When are covered financial institutions required to comply with the Beneficial Ownership Rule?

The Beneficial Ownership Rule was finalised in July 2016. Covered financial institutions are required to collect required information of beneficial owners on accounts opened on or after May 11, 2018.

1405. Is there a minimum number of beneficial owners required to be identified under the ownership and/or control prong of the Beneficial Ownership Rule?

The number of beneficial owners will vary based on each customer's circumstances. At a minimum, one natural person must be identified and verified under the control prong to satisfy the Beneficial Ownership Rule.

1406. Can covered financial institutions identify beneficial owners with less than the 25 percent equity interest?

Yes. Under the Beneficial Ownership Rule, covered financial institutions can opt to obtain the identity of beneficial owners who do not meet the de minimis 25 percent equity interest threshold based on risk. At a minimum, in circumstances where no person has 25 percent equity interest, at least one natural person must be identified and verified under the control prong of the Beneficial Ownership

Rule. Under Section 312, more beneficial owners may be identified as the de minimis percentage outlined for correspondents and private banking accounts is 10 percent.

1407. How does the 25 percent equity threshold of the Beneficial Ownership Rule compare to international standards?

The 25 percent equity threshold is consistent with the Recommendations of the Financial Action Task Force (FATF) and hundreds of intergovernmental agreements consistent with the Financial Account Tax Compliance Act (FATCA). For further guidance, please refer to the sections: International Perspectives and Initiatives and Foreign Account Tax Compliance Act.

1408. How is "significant" control defined by the Beneficial Ownership Rule?

The Beneficial Ownership Rule does not define "significant" control but does provide examples (e.g., a C-suite Executive, Managing Member, General Partner, President, Treasurer). Covered financial institutions are expected to identify the beneficial owners who have "significant" control under the control prong of the Beneficial Ownership Rule.

1409. Should covered financial institutions file a Suspicious Activity Report (SAR) if a customer attempts to evade the Beneficial Ownership Rule?

If covered financial institutions are able to detect a customer's attempt to evade the Beneficial Ownership Rule (e.g., restructuring their equity interests, providing a nominee owner/straw man), an investigation into possibly suspicious activity may be warranted. The decision to file a SAR should be based on the institution's investigation of the activity involved.

1410. Do beneficial owners include anyone who can fund or is entitled to the funds in an account?

No, the ability to fund an account, or the mere entitlement to the funds in an account without corresponding control over the account, does not result in beneficial ownership. For example, a minor child who is the beneficiary of an account established by her parents is not a beneficial owner.

1411. How are "legal entity customers" defined in the Beneficial Ownership Rule?

The Beneficial Ownership Rule defines "legal entity customers" to include the following types of entities created by the filing of a public document with a Secretary of State or similar office in the United States:

- Corporations
- Limited liability companies (LLCs)
- Limited Partnerships
- Business trusts (e.g., statutory trusts created by a filing with the Secretary of State or similar office)
- Similar entities as the aforementioned formed under laws of other countries

1412. Are sole proprietorships included in the definition of "legal entity customer" of the Beneficial Ownership Rule?

No. Sole proprietorships and unincorporated associations are not included in the definition of "legal entity customer."

1413. Are trusts included in the definition of "legal entity customer" of the Beneficial Ownership Rule?

Unless the trust was created by a filing with the Secretary of State or similar office, trusts are not included in the definition of "legal entity customer" of the Beneficial Ownership Rule.

1414. Are there any exemptions to the "legal entity customer" definition of the Beneficial Ownership Rule?

Yes. The Beneficial Ownership Rule does not require identification of beneficial owners of exempted entities, consistent with the CIP Rule under USA PATRIOT Act Section 326 – Verification of Identification, and some of the exemptions related to Currency Transaction Reports (CTR). According to FinCEN guidance FIN-2016-G003 on the Beneficial Ownership Rule, exemptions from the definition of "legal entity customer" include the following:

- Regulated entities such as:
  - "Financial institutions regulated by a Federal functional regulator or a bank regulated by a State bank regulator;
  - A bank holding company, as defined in section 2 of the Bank Holding Company Act of 1956 (12 USC 1841) or savings and loan holding company, as defined in section 10(n) of the Home Owners' Loan Act (12 USC 1467a(n));
  - A pooled investment vehicle operated or advised by a financial institution excluded from the definition of legal entity customer under the final CDD rule;
  - An insurance company regulated by a State;
  - A financial market utility designated by the Financial Stability Oversight Council under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010;
- Certain exempt persons for purposes of the currency transaction reporting obligations:
  - A department or agency of the United States, of any State, or of any political subdivision of a State;
  - Any entity established under the law of the United States, or any State, or of any political subdivision of any State, or under an interstate compact;
  - Any entity (other than a bank) whose common stock or analogous equity interests are listed on the New York, American, or NASDAQ stock exchange;

  - Any entity organised under the laws of the United States or of any State at least 51 percent of whose common stock or analogous equity interests are held by a listed entity;

- Issuers of securities registered under section 12 of the Securities Exchange Act of 1934 (SEA) or that is required to file reports under 15(d) of that Act;
- An investment company, as defined in section 3 of the Investment Company Act of 1940, registered with the U.S. Securities and Exchange Commission (SEC);
- An SEC-registered investment adviser, as defined in section 202(a)(11) of the Investment Advisers Act of 1940;
- An exchange or clearing agency, as defined in section 3 of the SEA, registered under section 6 or 17A of that Act;
- Any other entity registered with the SEC under the SEA;
- A registered entity, commodity pool operator, commodity trading advisor, retail foreign exchange dealer, swap dealer, or major swap participant, defined in section 1a of the Commodity Exchange Act (CEA), registered with the Commodity Futures Trading Commission (CFTC);
- A public accounting firm registered under section 102 of the Sarbanes-Oxley Act;
- Excluded foreign entities:
  - A foreign financial institution established in a jurisdiction where the regulator of such institution maintains beneficial ownership information regarding such institution;
  - A non-U.S. governmental department, agency or political subdivision that engages only in governmental rather than commercial activities; and
  - Any legal entity only to the extent that it opens a private banking account subject to 31 CFR 1010.620."

1415. Is there any de minimis size exclusion for accounts for complying with the requirements of the Beneficial Ownership Rule?

No, there is no threshold. The requirements apply to legal entity customers of covered institutions of accounts of all types and sizes.

1416. Are customers exempted under the Beneficial Ownership Rule also exempt from other AML/CFT requirements, such as monitoring for potentially suspicious activity?

No. Exemptions under the Beneficial Ownership Rule do not apply to other AML/CFT requirements, such as monitoring for potentially suspicious activities, filing BSA reports (e.g., Suspicious Activity Reports [SARs], Currency Transaction Reports [CTRs]).

1417. Does the Beneficial Ownership Rule apply to existing legal entity customers?

The Beneficial Ownership Rule applies to new legal entity customers, established after the effective date of the final rule. The fourth element of the Beneficial Ownership Rule does clarify regulatory expectations on updating customer information on an ongoing basis on existing customers. While the expectation to update customer information is not a categorical requirement, the frequency and nature of this review should be based on the customer's risk rating and results of suspicious activity monitoring.

1418. How is an "account" defined by the Beneficial Ownership Rule?

Consistent with the USA PATRIOT Act's CIP Rule, Section 326, an "account" is defined as:

- A formal relationship in which financial transactions or services are provided. Examples of products and services where a formal relationship would normally exist include deposit accounts and extensions of credit; a safe deposit box or other safekeeping services; or cash management, custodian or trust services.

1419. Are there exemptions to the definition of "account" under the Beneficial Ownership Rule?

Yes. According to FinCEN guidance FIN-2016-G003 on the Beneficial Ownership Rule, covered financial institutions are not required to obtain beneficial ownership information for the following types of accounts:

- "Accounts established at the point-of-sale to provide credit products, solely for the purchase of retail goods and/or services at these retailers, up to a limit of US$50,000;
- Accounts established to finance the purchase of postage and for which payments are remitted directly by the covered financial institution to the provider of the postage products;
- Accounts established to finance insurance premiums and for which payments are remitted directly by the financial institution to the insurance provider or broker; and
- Accounts established to finance the purchase or lease of equipment and for which payments are remitted directly by the covered financial institution to the vendor or lessor of this equipment.

These above exemptions do not apply under the following circumstances:

- If the accounts are transactions accounts through which a legal entity customer can make payments to, or receive payments from, third parties.
- If there is the possibility of a cash refund for accounts opened to finance purchase of postage, insurance premium, or equipment leasing."

1420. How is "customer risk profile" defined in the Beneficial Ownership Rule?

"Customer risk profile" is defined as "the information gathered about a customer to develop the baseline against which customer activity is assessed for suspicious transaction reporting." While the Beneficial Ownership Rule does not explicitly require covered financial institutions to risk rate each

customer and update this profile on an ongoing basis, it does expect institutions to understand the ML and TF risks posed by their customers and be able to demonstrate their understanding. For further guidance on risk assessments, please refer to the Risk Assessments section.

1421. Are covered financial institutions expected to integrate "customer risk profiles" into their automated transaction monitoring systems under the Beneficial Ownership Rule?

Covered financial institutions are not required per se to integrate "customer risk profiles" into automated transaction monitoring systems, covered financial institutions are expected to develop and maintain customer profiles to support their transaction monitoring efforts. Automating the capture of customer information, including customer profiles, is the best way to make this information available to those performing transaction monitoring.

1422. How often should beneficial ownership information be updated?

The Beneficial Ownership Rule indicates that beneficial ownership information should be updated, along with other customer information, using a risk-based approach and triggers from normal suspicious activity monitoring.

1423. How long are financial institutions required to retain beneficial ownership information under the Beneficial Ownership Rule?

Consistent with the other BSA recordkeeping and retention requirements, financial institutions are required to maintain beneficial ownership information for five years from the date an account closed, under the Beneficial Ownership Rule.

1424. Under the Beneficial Ownership Rule, are financial institutions expected to identify the beneficial owners of underlying customers in the case of correspondent and other intermediary relationships?

No. Financial institutions are not required to identify the beneficial owners of their customers' customers. However, as a practical matter, this may be information that a financial institution attempts to develop as part of its review or investigation of transaction activity.

1425. How can financial institutions satisfy the beneficial ownership identification requirement of the Beneficial Ownership Rule?

Financial institutions can satisfy the beneficial ownership identification requirement of the Beneficial Ownership Rule by:

- Obtaining the required information on beneficial owners as part of its customer onboarding program/process; or
- Obtaining a model certification form at the time a new account is opened, which includes basic CIP elements. The model Beneficial Ownership Certification Form includes the following:

- General instructions explaining the purpose of the form, who is required to complete the form and what information is required to be provided by customers/beneficial owners;
- Certification of beneficial owners including name, title, CIP elements and an attestation that the information provided on the form is accurate to the best of the knowledge of the natural person completing the form.

1426. Are financial institutions required to use the model Beneficial Ownership Certification Form to satisfy the Beneficial Ownership Rule?

No. The model Beneficial Ownership Certification Form is not an official government document and is not required to be used by covered financial institutions to satisfy the Beneficial Ownership Rule.

1427. Are covered financial institutions provided Safe Harbor if they elect to use the model Beneficial Ownership Certification Form?

No. Unlike Foreign Bank Certifications, covered financial institutions are not provided Safe Harbor if they elect to use the model Beneficial Ownership Certification Form.

1428. Are covered financial institutions required to verify the identity and status of beneficial owners to satisfy the Beneficial Ownership Rule?

No. Covered financial institutions are only required to verify the identity of beneficial owners and not their status as beneficial owners, provided the natural person opening the account certifies, to the best of his/her knowledge, the accuracy of the information provided.

1429. Does every customer need to be asked for the nature and intended purpose of each account to satisfy the Beneficial Ownership Rule?

No. The Beneficial Ownership Rule acknowledges that it is industry practice to gain an understanding of how a customer is expected to use an account through analysis, and not by asking every customer for a statement of the nature and intended purpose of each account. Other AML/CFT obligations require financial institutions to obtain the purpose of loans.

1430. Can covered financial institutions rely on a third party to satisfy the beneficial ownership identification requirement of the Beneficial Ownership Rule?

Yes. The Beneficial Ownership Rule permits reliance on other financial institutions for beneficial ownership information subject to the same conditions that allow for CIP reliance.

1431. Can a financial institution rely on a W-8BEN to identify and verify beneficial owners?

Because of the inconsistent definition of "beneficial owner" within and across industries, covered financial institutions are not permitted to rely upon previously gathered sources of beneficial ownership information (e.g., W-8BEN).

1432. Why can't financial institutions rely on beneficial ownership information collected by state authorities involved in company formation?

The requirements to provide beneficial ownership information vary across states. After conducting a rigorous analysis, FinCEN determined that financial institutions were in the best position to collect beneficial ownership information consistently thereby enhancing law enforcement investigations.

1433. What types of questions should financial institutions ask to determine the legitimacy of different vehicles used or entities controlled by beneficial owners?

Financial institutions may consider the following types of questions:

- What is the purpose of the structure or vehicle?
- Who are the underlying beneficial owners?
- In what jurisdiction is it established and why?
- When was the structure or vehicle set up?
- Is the jurisdiction one that is of high risk to money laundering?
- What kind of activity will be conducted by the entity or vehicle?
- What type of activity will be conducted through the financial institution?
- Where applicable, what is the reason why the same beneficial owners are behind multiple legal entities or vehicles?
- Do the answers provided to the questions above make sense?

Additionally, as appropriate, beneficial owners should be subject to EDD. This would include, for example, PICs, shell companies, Special Purpose Vehicles (SPVs) and instances where the beneficial owners include politically exposed persons (PEPs). For additional guidance on PICs, shell companies and SPVs, please refer to the sections: Business Entities: Shell Companies, Private Investment Companies; and Politically Exposed Persons.

1434. Are bearer shares a type of beneficial ownership?

Yes, bearer shares, which are negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate, are a type of beneficial ownership. Because bearer shares are negotiable, they create additional risk for financial institutions because beneficial ownership changes if the bearer share certificate is transferred to another party.

1435. How do financial institutions manage the risk of bearer shares?

In an interpretive note to Recommendation 24, FATF suggests the following measures to mitigate the risks of bearer shares:

- Prohibiting bearer shares;
- Converting bearer shares into registered shares;

- Immobilising bearer shares by requiring that they be held with a regulated financial institution or professional intermediary; or
- Requiring shareholders with a controlling interest to notify the company and the company to record their identity.

1436. Are there specific AML/CFT requirements for bearer shares?

Yes, bearer shares, if valued at greater than US$10,000 and physically transported across a border (incoming or outgoing) are required to be reported on the Report of International Transportation of Currency or Monetary Instruments (CMIR). For further guidance, please refer to the sections: Monetary Instruments and Report of International Transportation of Currency or Monetary Instruments.

1437. How do the FATF Recommendations address beneficial ownership?

FATF defines "beneficial owner" as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."

FATF Recommendation 24 – Transparency and Beneficial Ownership of Legal Persons and **Recommendation 25 – Transparency and Beneficial Ownership of Legal Arrangements** recommend applying due diligence measures to beneficial owners (e.g., any person owning or controlling more than a designated percentage of a company) before establishing a business relationship or providing services (e.g., conducting transactions). FATF also suggests identifying the beneficial owners of existing customers utilising a risk-based approach.

To assist financial institutions in determining entities and instances which may require identification of beneficial owners, FATF offered the following examples:

- Legal entities that have shares in bearer form
- Legal entities that have nominee shareholders (e.g., a person who holds shares on behalf of the actual owner)
- Legal entities that may be deliberately designed to obscure ownership (e.g., trusts, shell companies, private investment companies [PICs])
- Customers located in high-risk jurisdictions (e.g., high corruption, high crime, lax regulatory environment)
- Owners of financial institutions
- Potential involvement of foreign politically exposed persons (PEPs)
- Beneficiaries of life insurance policies and other investment-related insurance policies (e.g., preferably at designation versus at the time of payout)
- Customers under investigation for money laundering and terrorist financing

1438. What are some of anticipated challenges to complying with the Beneficial Ownership Rule?

The following include some of the challenges that financial institutions may experience in complying with the Beneficial Ownership Rule:

- High costs and other issues with updating legacy AML/CFT technology to manage and monitor beneficial owners (e.g., customer onboarding to store newly required information on beneficial owners, suspicious activity monitoring systems to analyse accounts related through beneficial owners, currency monitoring to file Currency Transaction Reports [CTRs] on aggregate activity conducted by or on behalf of beneficial owners);
- Increased time to complete the lengthened customer onboarding process;
- Inability or difficulty in verifying beneficial ownership identification; and
- Difficulty in keeping beneficial ownership information current.

1439. What guidance has been issued related to the risks of beneficial ownership and expected industry practices?

Guidance has been issued on the risks of beneficial ownership and expected industry practices including, but not limited to, the following:

- Ending Secrecy to End Impunity: Tracing the Beneficial Owner (2014) by Transparency International
- FATF Recommendation 24 and 25: Transparency and Beneficial Ownership of Legal Persons and Legal Arrangements by FATF
- Guidance on Obtaining and Retaining Beneficial Ownership Information (2010) by the Financial Crimes Enforcement Network (FinCEN), the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC), Office of Thrift Supervision (OTS) and the Securities and Exchange Commission (SEC)
- Customer Due Diligence Requirements for Financial Institutions (2012, 2014, 2016) by FinCEN
- FinCEN Clarifies Expectations Regarding Beneficial Ownership (2012) by FinCEN
- Standard on the Regulation of Trust and Corporate Service Providers (2014) by the Group of International Finance Centre Supervisors (GIFCS)
- Transparency of Company Ownership and Control (2013) by various global partners (e.g., Group of Twenty Finance Ministers and Central Bank Governors (G-20), FATF, Global Forum on Transparency and Exchange of Information for Tax Purposes)
- Joint Guidance on Obtaining and Retaining Beneficial Ownership Information (2010) by FinCEN
- Advisory – Potential Money Laundering Risks Related to Shell Companies (2006) by FinCEN

- FAQs on Beneficial Ownership (2012) by the Wolfsberg Group
- FAQs on Intermediaries (2012) by the Wolfsberg Group
- The Misuse of Corporate Vehicles, Including Trust and Company Service Providers (2006) by the Financial Action Task Force (FATF)
- Behind the Corporate Veil – Using Corporate Entities for Illicit Purposes (2001) by the Organisation for Economic Co-operation and Development (OECD)
- Identification of Ultimate Beneficiary Ownership and Control of a Cross-Border Investor (2007) by the Organisation for Economic Co-operation and Development (OECD)
- Principles on Client Identification and Beneficial Ownership for the Securities Industry (2004) by the International Organisation of Securities Commissions (IOSCO)
- The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies (2006) by FinCEN

Know Your Customer Types

Non-resident Aliens and Foreign Persons

1440. What is the difference between the terms "resident alien" and "non-resident alien"?

An alien is any person who is not a U.S. citizen. For tax purposes, the Internal Revenue Service (IRS) classifies aliens as either resident aliens or non-resident aliens (NRAs) based on (1) a Green Card test or (2) a Substantial Presence test.

- **Resident Alien**: If the alien has a Green Card, also known as an alien registration receipt card, or if he or she was physically present in the United States for 31 days during the current year and 183 days during a three-year period that includes the current year and the two years immediately before that, the alien is then classified as a resident alien and his or her earned income is taxed like a U.S. citizen's earned income.
- **Non-resident Alien (NRA)**: A non-resident alien is an alien who does not meet the Green Card test or the Substantial Presence test. For NRAs, only income that is generated from U.S. sources, excluding certain investments such as stocks, is subject to taxation.

1441. What is the difference between the terms "NRAs" and "foreign persons"?

NRAs are foreign individuals who (or businesses that) are not permanent residents of the United States but may reside on a part-time basis in the United States. "Foreign persons" generally refers to individuals who (or businesses that) do not reside in the United States for any amount of time. In some instances, the term "NRA" is used interchangeably with "foreign persons" to describe all non-U.S. persons, regardless of actual residency.

1442. What is the difference between the terms "NRAs" and "illegal aliens"?

Illegal aliens are foreigners who have violated U.S. laws and customs in establishing permanent residence in the United States. NRAs are foreign individuals who (or businesses that) have not met the criteria described above to be classified as resident aliens.

1443. Why do NRAs and foreign persons establish account relationships at U.S. financial institutions?

Non-resident aliens and foreign persons establish accounts at U.S. financial institutions for various reasons, including, but not limited to, the following:

- Cross-border business or personal needs
- Asset preservation
- Access to investments
- Unstable financial system in their home country
- Expansion in business

1444. Are NRAs and foreign persons required to provide a taxpayer identification number to establish account relationships at U.S. financial institutions?

No. According to the USA PATRIOT Act's Section 326 – Verification of Identification, commonly referred to as the Customer Identification Program (CIP) requirement, individuals and businesses must provide the following information prior to establishing an account at a U.S. financial institution:

- Name
- Date of birth (DOB) for individuals
- Address
- Identification number

A taxpayer identification number (TIN) should always be obtained for U.S. persons. For non-U.S. persons, one or more of the following should be obtained for the identification number:

- TIN
- Passport number and country of issuance
- Alien identification card number
- Number and issuing country of any other unexpired government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard

For further guidance on the CIP requirement, please refer to the Section 326 – Verification of Identification section.

1445. What are W-8BEN forms and why might an NRA complete one when establishing an account with a financial institution?

A W-8BEN form, formally known as the "Certificate of Foreign Status of Beneficial Owner for United States Tax Withholding," is an IRS form that attests to the NRA's tax-exempt status. As a result, financial institutions, as the withholding agents, will not withhold taxes for income earned on accounts held by the NRA.

1446. What responsibilities do financial institutions have with respect to W-8BEN forms?

Financial institutions are responsible for maintaining completed W-8BEN forms in accordance with AML/CFT recordkeeping requirements, ensuring they are updated as necessary, providing completed forms to the IRS upon request, and monitoring customer activity for patterns that indicate U.S. resident status or other potentially suspicious activity.

1447. Are financial institutions responsible for determining whether a potential or existing customer is an NRA or an illegal alien?

No. Financial institutions are not responsible for determining whether a customer is an NRA or an illegal alien. If a financial institution detects patterns that indicate U.S. resident status for a customer who certified otherwise, it is only responsible for reporting potentially suspicious activity – in this case, false or inaccurate information provided on official IRS forms.

1448. Would resident aliens complete the same W-8BEN forms when establishing accounts with a financial institution?

No. Similar IRS forms exist for individuals who (and businesses that) are not NRAs who would like to certify their citizenship/residence status and/or tax-exempt status. Exceptions exist in applicability, but in general, the forms are:

- **Resident aliens/U.S. citizens** complete a **W-9** form, formally called a "Request for Taxpayer Identification Number and Certification."
- **Persons claiming that income is effectively connected with the conduct of a trade or business in the United States** complete **W-8ECI** forms, formally known as "Certificate of Foreign Persons Claim That Income Is Effectively Connected With the Conduct of a Trade or Business in the United States."
- **Foreign partnerships, foreign simple trusts, or foreign grantor trusts** complete **W-8ECI** forms or **W-8IMY** forms, formally referred to as "Certificate of Foreign Intermediary, Foreign Flow-Through Entity, or Certain U.S. Branches for United States Tax Withholding."
- **Foreign governments, international organisations, foreign central banks of issue, foreign tax-exempt organisations, foreign private foundations**, or **governments of a U.S. possession** that receives effectively connected income complete W-8ECI forms or W-8EXP forms, formally called "Certificate of Foreign Government or Other Foreign Organisation for United States Tax Withholding."

- **Persons acting as intermediaries** complete **W-8IMY** forms, formally known as "Certificate of Foreign Intermediary, Foreign Flow-Through Entity, or Certain U.S. Branches for United States Tax Withholding."

1449. What are the heightened money laundering and terrorist financing risks of NRAs and foreign persons?

The heightened risk of NRAs and foreign persons lies in the following:

- Challenges in verifying their identities, source of funds, source of wealth and relationships/affiliations;
- Increased frequency of international transactions;
- Possible residency in a high-risk jurisdiction with lax AML/CFT laws and regulations; and
- Increased chance of being identified as a politically exposed person (PEP).

Additionally, NRAs are at heightened risk of being victims of human trafficking and migrant smuggling. For further guidance, please refer to the Human Trafficking and Migrant Smuggling section.

1450. As customers, do all NRAs and foreign persons pose the same degree of risk?

No. The risks of each NRA and foreign person should be assessed based on a variety of factors (e.g., products/services, occupation/nature of business, associated geographies, transaction activity). Status as an NRA or foreign person is only one risk factor. Evaluating the risks of NRAs and foreign persons in this manner will result in different risk ratings (e.g., low, moderate, high).

For further guidance on risk assessments, please refer to the Customer Risk Assessment section.

Employment-Based Immigration Program: EB-5

1451. What is the EB-5 Program?

Established as a pilot permanent worker program in 1990, the Employment-Based Immigration: Fifth Preference (EB-5) Program, is an immigration-visa sponsorship program administered by the United States Citizenship and Immigration Services (USCIS) that facilitates permanent resident status (e.g., green cards) for eligible foreign investors who invest capital in a "new commercial enterprise" (i.e., established after November 29,1990) that promotes economic growth (e.g., direct or indirect creation of 10 permanent full-time positions in the United States). The number of visas granted through the EB-5 Program is currently capped at 10,000. According to the U.S. State Department, in recent years, the majority of EB-5 Program visas were granted to Chinese nationals. While there are ongoing discussions about the need to reform the program to guard against abuse, the EB-5 Program was granted a short term extension by the U.S. Congress through September 2017.

The other EB programs (first through fourth preference) are based on "extraordinary ability," holding an advanced degree in a particular profession, being a "skilled worker" or having status as a "special

immigrant" (e.g., religious workers, broadcasters, physicians, translators). The EB-5 Program is unique in that the visa is granted to the investor who may or may not be an employee of the regional centre.

The USCIS also administers multiple programs for temporary (non-immigrant) workers as well (e.g., E-1 Treaty Traders, H1B Specialty Occupations and Fashion Models, H-2A Agricultural Workers, Q-1 Cultural Exchange).

1452. What are the qualifications and/or eligibility requirements for the EB-5 Program?

Foreign investors or "immigrant entrepreneurs" are required to invest a minimum of the following:

- US$1 million into a qualifying new commercial enterprise; and/or
- US$500,000 into a qualifying new commercial enterprise in a targeted employment area (TEA).

The qualifications for a "new commercial enterprise" require the following:

- For-profit;
- Established after November 29, 1990; or
- If established on or before November 29, 1990 the existing business must be restructured in a way that results in the following:
  - A new commercial enterprise; or
  - The business's net worth or number of employees is expanded by 40 percent or more.

An application can be submitted for any type of business. A panel of government experts on economic-stimulus will determine whether the capital received from prospective EB-5 applicants would be effective in generating job growth in the United States.

The EB-5 qualifications outlined herein are specific to the EB-5 Program and do not necessarily reflect the myriad of other general immigration qualifications/requirements to which an applicant may be subject (e.g., medical examinations, submission of identification documentation such as birth certificates, passing background checks, providing an affidavit of financial support).

1453. What is a targeted employment area (TEA)?

Targeted employment areas (TEAs) are areas with high unemployment (e.g., 150 percent of the U.S. average national unemployment rate) that are typically designated by the federal or state department of labour. Some TEAs have drawn controversy as designations have allegedly been made for political reasons (e.g., through gerrymandering) to benefit wealthy investors, rather than to regions that are truly economically depressed.

1454. Are foreign businesses eligible to be designated as "regional centres" under the EB-5 Program?

No. Foreign businesses are not eligible to be designated as "regional centres" under the EB-5 Program.

1455. Are the permanent full-time positions created by regional centres required to be filled by U.S. citizens?

No. The permanent full-time positions must be filled by "qualified U.S. workers" which includes U.S. citizens and resident aliens eligible to work in the United States.

1456. Is the granting of visas limited to the EB-5 applicant?

No. Spouses and unmarried children of EB-5 applicants can also apply for visas under the EB-5 Program.

1457. What is the "Immigrant Investor Program" or "Regional Center Program"?

In 1992, the "Immigrant Investor Program" or "Regional Center Program" was created to set aside EB-5 visas for foreign nationals who invested in USCIS-approved "regional centres," allowing investors to pool their capital investments into one or more designated businesses in a specific location that directly or indirectly created the minimum number of permanent full-time jobs.

The designation as a "regional center," in essence, certifies to other prospective investors that it qualifies as a "new commercial enterprise" and would satisfy the EB-5 Program requirements. The USCIS publishes a list of approved and terminated regional centres on their website.

The Regional Center Program has drawn criticism due to the alleged exploitation of TEAs and the EB-5 Program criteria of "indirectly" creating jobs. Some argue for the Regional Center Program to become permanent. Others argue for elimination or at a minimum, more regulations to guard against fraud and increase transparency of the overall process (e.g., application, reporting).

1458. What are the heightened money laundering and terrorist financing risks of the EB-5 Program?

The EB-5 Program is vulnerable to abuse by both foreign individuals looking for a mechanism to conduct illicit financial activity through the U.S. financial system as well as by fraudulent business enterprises looking to take advantage of foreign investors. The heightened money laundering and terrorist financing risks associated with the EB-5 Program include, but are not limited to, the following:

- Unclear source of funds for the initial EB-5 program investment (e.g., individuals pool funds from multiple unknown sources to "sponsor" a single EB-5 applicant);
- High net worth applicants often from high-risk jurisdictions;
- Status as a politically exposed person (PEP) and/or close associate/family member of a PEP;
- Lack of identification of financial accounts of EB-5 applicants leading to inadequate monitoring of activity, whether applicant was accepted or not; and
- History of criminals exploiting the EB-5 Program application process to attract foreign investment into fraudulent business development projects.

1459. What is a recent example of abuse involving the EB-5 Program?

In 2013, as a joint effort with the USCIS to protect the integrity of the EB-5 Program, the Securities and Exchange Commission (SEC) issued Investor Alert: Investment Scams Exploit Immigrant Investor Program. The SEC report described how businesses were exploiting the EB-5 Program application process to convince foreign nationals to invest in fraudulent businesses and securities offerings. Specific examples included:

- **SEC v. Marco A. Ramirez, et al.** – Defendants began solicitations before being approved by the USCIS as a regional center and falsely promised a 5 percent return and an EB-5 visa for investors; and
- **SEC v. A Chicago Convention Center, et al.** – Defendants used false and misleading information to attract foreign investors (e.g., secured required building permits, backed by major hotel chains) and promised the return of administrative fees if EB-5 visa applications were denied after having spent more than 90 percent of collected fees.

The SEC report also included recommended due diligence steps to take before investing in an EB-5 business project including, but not limited to, requesting documentation of investment information and application documents submitted to the USCIS and seeking independent verification through third-party sources.

1460. What can financial institutions do to mitigate their ML/TF risk as it relates to the EB-5 Program?

The steps a financial institution may take to mitigate ML/TF risk associated with the EB-5 Program will vary based on the nature of the customer relationship. For example, a financial institution which is looking to provide services to an EB-5 regional center, may seek to ensure KYC information includes:

- Copies of marketing, solicitation, disclosure documentation and subscription terms provided to prospective investors;
- Copies of documentation submitted to, or obtained from, USCIS for regional center approval;
- Identification of the total volume being requested and/or any planned tranche structures;
- Policies, procedures and other program documentation supporting due diligence performed by the customer on EB-5 investors;
- Copies of audited financial statements, as well as policies governing compliance with the Foreign Corrupt Practices Act (FCPA) (as applicable), or other anti-bribery and corruption (ABC) compliance programs;
- Identification/information about expected payout structures, vendors, contractors and third parties associated with joint-ventures; and
- To the extent a financial institution is establishing escrow accounts or providing any type of bridge lending, KYC information may be required for the underlying investors as well.

For financial institutions providing services to prospective EB-5 applicants, the collection of documentation as to the source of funds, as the EB-5 Program requires that invested capital be derived by lawful means and applicants are expected to attest to the source of funds.

It will be important for financial institutions to understand what is reasonable and appropriate expected activity associated with EB-5 Program investments, in order to leverage existing transaction monitoring functionality to determine whether alerted activity is potentially suspicious.

1461. Is it acceptable to rely on the USCIS vetting process of EB-5 applicants for CIP Verification or other aspects of KYC?

No. The screening, vetting, processing and other due diligence performed by the USCIS as part of an EB-5 application process does not waive CIP verification requirements nor the need for financial institutions to conduct KYC. Approval as an EB-5 regional center by the USCIS does not constitute an endorsement of the commercial enterprise.

1462. What reforms have been recently proposed for the EB-5 Program?

In January 2017, the Department of Homeland Security (DHS) published the EB–5 Immigrant Investor Program Modernisation notice of proposed rulemaking with statutory changes and significant reforms for the EB-5 Program including, but not limited to, the following:

- **Priority Date Retention** – Retention of the date on which an approved EB-5 petition was filed on subsequent petitions filed due to circumstances beyond the control of the petitioner.
- **Increases to Investment Amounts** – Increasing minimum investment amounts (e.g., US$1 million to US$1.8 million for projects in high employment areas, US$500,000 to US$1.35 million in TEAs) with adjustments occurring every five years
- **TEA Designations** – Reform of the TEA designation process (e.g., clarification on TEA designation criteria, designations made by DHS only)
- **Removal of Conditions** – Clarification that derivative family members must file separate EB-5 petitions to remove conditions (e.g., 2 year expiration) on their permanent residence when not included in the principal investor's EB-5 petition.

Private Banking

1463. How is the term "private banking" defined?

For the purpose of Section 312 of the USA PATRIOT Act, a private banking account is defined as an account (or combination of accounts) maintained at a financial institution that meets the following criteria:

- Requires a minimum aggregate deposit of funds or other assets of not less than US$1 million
- Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account

- Is assigned to, or is administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account

1464. What are the heightened money laundering and terrorist financing risks of private banking customers?

Private banking can be vulnerable to money laundering schemes for the following reasons:

- Strict privacy and confidentiality culture of private bankers
- Powerful clientele (e.g., PEPs)
- Use of trusts, private investment companies (PICs) and other types of nominee companies
- Increased frequency of international transactions

1465. Do all private banking customers pose the same degree of risk?

No. The risks of each private banking customer should be assessed based on a variety of factors (e.g., products/services, occupation/nature of business, associated geographies, transaction activity). Status as a private banking customer is only one risk factor. Evaluating the risks of private banking customers in this manner will result in different risk ratings (e.g., low, moderate, high).

1466. Are there specific AML/CFT requirements for private banking customers?

Yes. Due to the high-risk nature of private banking, Section 312 of the USA PATRIOT Act, formally referred to as "Section 312 - Special Due Diligence for Correspondent Accounts and Private Banking Accounts," outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have private banking customers.

1467. Does the Customer Due Diligence Requirements for Financial Institutions final rule (Beneficial Ownership Rule) impact AML/CFT requirements for private banking customers?

No. Due to the high-risk nature of private banking, covered financial institutions were already required to collect and verify beneficial ownership information on their private banking customers. The Beneficial Ownership Rule did not add any additional requirements. For further guidance, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Beneficial Owners sections.

1468. How do Section 312 requirements for private banking correspond to FATF Recommendations?

In **Recommendation 10 – Customer Due Diligence**, FATF recommends financial institutions implement enhanced measures for higher risk customers, geographies, products, services, transactions and delivery channels, including private banking.

Section 312 outlines enhanced due diligence for private banking, including, but not limited to, the identification of beneficial owners and politically exposed persons (PEPs).

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section. For further guidance on customer due diligence, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

1469. What guidance has been issued on private banking?

The following are examples of key guidance that has been issued on private banking:

- **Private Banking Due Diligence Program (Non-U.S. Persons)** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Wolfsberg Anti-Money Laundering Principles for Private Banking** (2012) by the Wolfsberg Group of Banks (Wolfsberg Group)
- **Private Banking and Money Laundering: A Case Study of Opportunities and Vulnerabilities** (2001) by the U.S. Senate (Hearing)

Additional topics related to private banking include beneficial ownership and politically exposed persons (PEPs). For further guidance, please refer to the sections: Beneficial Owners, Politically Exposed Persons and Senior Foreign Political Figures.

Politically Exposed Persons

1470. How is the term "politically exposed person" defined?

A senior foreign political figure, also known as a politically exposed person (PEP), is defined under Section 312 of the USA PATRIOT Act as:

- A current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not);
- A senior official of a major foreign political party;
- A senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual;
- An immediate family member of such an individual; or
- Any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual.

"Immediate family member" means an individual's spouse, parents, siblings, children and spouse's parents or siblings. "Senior official" or "senior executive" means an individual with substantial authority over policy, operations or the use of government-owned resources.

1471. What are the heightened money laundering and terrorist financing risks of politically exposed persons?

Access to government funds may increase the potential for corruption and bribery. **Section 315 – Inclusion of Foreign Corruption Offenses as Money Laundering Crimes** of the USA PATRIOT Act includes multiple offenses as money laundering crimes, including, but not limited to the following:

- Bribery of a public official or the misappropriation, theft or embezzlement of public funds by or for the benefit of the public official
- Any felony violations of the Foreign Corrupt Practices Act of 1977 (FCPA)
- An offense with respect to multilateral treaties in which the United States would be obligated to extradite the offender or submit the case for prosecution if the offender were found in the United States

For additional guidance on corruption, please refer to the Anti-Bribery and Corruption Compliance Program and Foreign Corrupt Practices Act sections.

1472. Do all PEPs pose the same degree of risk?

No. Not all PEPs pose the same degree of risk. A financial institution may consider, for example, the country of domicile, level of office, negative history/media on the PEP, and the degree of affiliation to the PEP (in the case of family members and close associates) when assessing the degree of risk.

1473. Are there specific AML/CFT requirements for PEPs?

Yes. Due to the high-risk nature of PEPs, Section 312 of the USA PATRIOT Act, formally known as "Special Due Diligence for Correspondent Accounts and Private Banking Accounts," outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have PEPs as customers. For further guidance, please refer to Senior Foreign Political Figure section.

1474. How do Section 312 requirements for PEPs correspond to FATF Recommendations?

FATF's definition of PEP, developed to be consistent with the United Nation's Convention Against Corruption (UNCAC), includes the following:

- **Foreign PEPs** are defined as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).
- **Domestic PEPs** are individuals who are, or have been, entrusted domestically with prominent public functions (e.g., heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).

- **International organisation PEPs** are individuals who are, or have been, entrusted with prominent functions by an international organisation (e.g., senior management, directors, board members).

Family members (e.g., direct relatives, through marriage) and close associates (e.g., social, professional) of PEPs are also included in FATF's definition.

FATF Recommendation 12 – Politically Exposed Persons recommends financial institutions implement risk-based measures to mitigate the money laundering risks of PEPs including, but not limited to, the following:

- Identification of foreign PEPs (and family members or close associates) in the customer population (or as beneficial owners);
- Establishing the source of wealth/funds of PEPs;
- Conducting ongoing monitoring of PEP relationships; and
- Requiring senior management approval to provide services to PEPs (e.g., opening an account, paying out on a life insurance policy).

If other high-risk factors are present (e.g., high-risk nature of business, high-risk country of operation), enhanced measures should be applied to domestic PEPs as well.

The USA PATRIOT Act's definition of PEP is consistent with FATF's definition of foreign PEP. While Section 312 of the USA PATRIOT Act outlines enhanced due diligence measures for "senior foreign political figures," many U.S. financial institutions have voluntarily applied due diligence measures to domestic PEPs as well. For further guidance on international standards, please refer to the Financial Action Task Force section.

1475. Is the definition of a PEP limited to "foreign" senior officials?

Consistent with FATF Recommendations, many financial institutions extend the definition of PEP to include domestic senior political figures as well, though this is not required by Section 312.

Other jurisdictions have explicitly expanded their definition to include domestic senior political figures as PEPs (e.g., European Union). Some multinational financial institutions may modify their definition of PEPs to include senior foreign political figures of all countries, irrespective of where each bank/branch is based. Additionally, they may utilise a risk-based approach and only include PEPs from countries with lax AML/CFT laws and regulations or a high index of corruption.

1476. Is the definition of a PEP limited to private banking customers?

No. Status as a PEP is not dependent on the types of products and services utilised by the PEP.

1477. Do embassy and foreign consulate accounts fall within the definition of a PEP?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is

unlikely to reach PEP status. For further guidance on embassy accounts, please refer to the Foreign Embassy and Consulates section.

1478. Is the definition of a PEP limited to natural persons? Are there instances when corporations are considered as PEPs?

A PEP is a natural person. However, if a legal entity (e.g., corporation) is formed by or for the benefit of a PEP, it would be a PEP-associated entity and be subject to similar enhanced due diligence as a PEP.

1479. Should an entity controlled by a PEP be subject to similar measures as the PEP itself?

Yes. The same enhanced due diligence should be applied to entities owned or controlled by PEPs.

Criminals, such as corrupt foreign officials, may use legal entities such as private investment companies (PICs) to obscure their identity and disguise their illicit activities. While Section 312 requires the collection and verification of beneficial ownership information for private banking customers, not all PEPs fall under the definition of private banking customers.

To address this vulnerability, FinCEN issued the notice of proposed rulemaking (NPRM), "Customer Due Diligence Requirements for Financial Institutions" in 2014, which would require financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers.

For further guidance, please refer to the following sections: Beneficial Owners, Business Entities: Shell Companies, Private Investment Companies and Anti-Bribery and Corruption Compliance Programs.

1480. Is someone who was a PEP always a PEP?

The most conservative approach would be "once a PEP, always a PEP." A moderate approach, endorsed by the Wolfsberg Group and outlined in the European Union's Fourth Anti-Money Laundering Directive, would be for a financial institution to remove the individual from the institution's PEP list one year after the individual is no longer in a political function. However, if derogatory information or suspicious activity is detected, a financial institution should continue to categorise the customer as a high risk.

1481. What steps should a financial institution take when determining if a customer is a PEP?

The rules provide that reasonable steps are in place to ascertain whether any account holder may be a senior foreign political figure. These steps should include, but not be limited to, holding conversations with the client, conducting reference checks, and reviewing information available in databases provided by list providers or public sources on the internet.

1482. Where can a financial institution find a list of PEPs?

Financial institutions can use several third-party vendors that provide a variety of Know Your Customer (KYC) and customer identification solutions, such as a list of PEPs. Public resources include,

but are not limited to, lists published by OFAC, the FBI, the Central Intelligence Agency (CIA), Interpol, the Drug Enforcement Administration (DEA) and the United Nations.

1483. Should financial institutions consider not opening an account or terminating an existing relationship if a customer is a PEP?

Status as a PEP does not mean that an account should not be opened or that an existing relationship should be automatically terminated. It simply means that due diligence for the PEP should be more extensive than for a standard customer and that the PEP's transactions should be subject to heightened scrutiny.

1484. Should political parties be considered PEPs?

Though political parties are not covered by the PEP definition, financial institutions should consider applying heightened scrutiny to business relationships holding assets of *foreign* political parties.

1485. How would a financial institution monitor for transactions involving proceeds of foreign corruption?

Financial institutions can monitor for proceeds of foreign corruption by identifying customers and transaction counter-parties who may have greater access to foreign government funds (i.e., PEPs). For further guidance, please refer to the Anti-Bribery and Corruption Compliance Programs and Foreign Corrupt Practices Act sections.

Foreign Embassy and Consulates

1486. How are the terms "foreign embassy" and "consulate" defined?

An embassy, led by an ambassador (i.e., official diplomat), is a foreign government's official representation in a host country, serving as a communication channel between the two countries. While embassies are often located in a host country's capital, they can be located elsewhere (e.g., many foreign embassies in the United States are located in the United Nations headquarters in New York City).

Consulate offices act as branches of an embassy with an objective to perform various administrative and governmental functions (e.g., issuing visas, handling immigration matters) that serve the citizens of that consulate's home country.

The U.S. Department of State maintains a list on its website of foreign embassies, foreign consular offices (FCOs) and recognised consular offices, as well as embassies, consulates and diplomatic missions from the United States in foreign countries.

1487. Do embassy and foreign consulate accounts fall within the definition of a PEP?

Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status.

1488. Why do embassies and foreign consulates establish account relationships at U.S. financial institutions?

Embassies and foreign consulates establish accounts at U.S. financial institutions for various reasons, including, but not limited to, the following:

- Manage operational expenses (e.g., payroll, rent, utilities)
- Facilitate inter- and intra-governmental transactions (e.g., commercial and military purchases)
- Provide ancillary services or accounts to embassy staff, families, and current or prior foreign government officials

1489. What are the heightened money laundering and terrorist financing risks of foreign embassies and consulates?

The heightened risk of embassies and foreign consulates lies in the following:

- Customers from high-risk jurisdictions
- Increased volume of high-risk products/services and transactions (e.g., cash, pouch activity) which may involve third parties
- Increased frequency of international transactions
- Increased chance of being affiliated with a politically exposed person (PEP)

1490. As customers, do all foreign embassies and consulates pose the same degree of risk?

No. The risks of each embassy and foreign consulate customer should be assessed based on a variety of factors (e.g., the strength of AML/CFT laws in the home country, services provided, employees who meet the definition of a PEP). Evaluating the risks of embassy and foreign consulate customers in this manner will result in different risk ratings (e.g., low, moderate, high).

1491. Are there specific AML/CFT requirements for foreign embassies and consulates?

- Certain individuals within an embassy or consulate may fall within the definition of a PEP (e.g., the ambassador or a high-ranking military officer). The average employee in an embassy or consulate is unlikely to reach PEP status.
- Due to the high-risk nature of PEPs, Section 312 of the USA PATRIOT Act, formally known as "Special Due Diligence for Correspondent Accounts and Private Banking Accounts," outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions who have PEPs as customers. For further guidance, please refer to Senior Foreign Political Figures section.

1492. What are "foreign missions" and should they be treated in the same manner as foreign embassies and consulates?

The Foreign Missions Act (1982) defines a foreign mission as "any mission to or agency or entity in the United States which is involved in the diplomatic, consular, or other activities of, or which is substantially owned or effectively controlled by:

- A foreign government; or
- An organisation (other than an international organisation … defined [as a public international organisation pursuant to the International Organisations Immunities Act … pursuant to a treaty … and an official mission]) representing a territory or political entity which has been granted diplomatic or other official privileges and immunities under the laws of the United States or which engages in some aspect of the conduct of the international affairs of such territory or political entity, including any real property of such a mission and including the personnel of such a mission."

Some may use "mission" as a more general term including foreign embassies and consulates.

In March 2011, Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions was released as an interagency advisory, building on Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies and Foreign Political Figures (2004). As with other types of customers and accounts, federal agencies expect financial institutions to conduct risk-based supervision of foreign mission customers similar to that of foreign embassies and consulates.

1493. What guidance has been issued with respect to PEPs and embassy banking?

The following key guidance has been issued on PEPs, embassy banking and related topics:

- **Politically Exposed Persons – Overview** (2010) and **Embassy and Foreign Consulate Accounts – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)** (2013) by the Financial Action Task Force (FATF)
- **Best Practices Paper: The Use of FATF Recommendations to Combat Corruption** (2013) by FATF
- **Corruption: A Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight against Corruption** (2012) by FATF
- **Interagency Advisory: Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions** (2011) by the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), FinCEN, National Credit Union Administration (NCUA), Office of the Comptroller of the Currency (OCC) and the Office of Thrift Supervision (OTS)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** (2008) by FinCEN

- **Wolfsberg FAQs on Politically Exposed Persons** (2008) by the Wolfsberg Group of Banks (Wolfsberg Group)
- **Guidance on Enhanced Scrutiny for Transactions That May Involve the Proceeds of Foreign Official Corruption** (2001) by the U.S. Treasury, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency, Office of Thrift Supervision, and the Department of State
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** (2010) by the World Bank (WB)
- **Stolen Asset Recovery: Guide on Non-Conviction Based** (NCB) Asset Forfeiture (2009) by the WB
- **Interagency Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions** (2011) by FinCEN
- **Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies and Foreign Political Figures** (2004) by FinCEN
- **Money Laundering and Foreign Corruption: Enforcement and Effectiveness of the PATRIOT Act: Case Study Involving Riggs Bank Report** (2004) by the United States Senate Permanent Subcommittee on Investigations

For further guidance on foreign embassies, corruption and beneficial ownership, please refer to the sections: Foreign Embassy and Consulates, Anti-Bribery and Corruption Compliance Programs and Beneficial Owners.

Charitable Organisations and Nongovernmental Organisations

1494. How are the terms "charitable organisations" and "nongovernmental organisations" defined?

A charitable organisation is generally defined as an organisation that is established and operated for purposes that are beneficial to the public interest. Private charitable organisations generally receive funding from an individual, family, corporation or other singular source, whereas public charities solicit funds from the general public. Specific definitions of charitable organisations and related requirements (e.g., registration, tax filing) are determined by the laws and regulations within the jurisdiction(s) in which the charitable organisation is established and/or operates. Charitable organisations can be based locally, regionally, nationally or internationally. In the United States, these charitable organisations are often referred to as 501(c)(3) organisations, in reference to the Internal Revenue Service (IRS) code for tax-exempt organisations, which imposes many restrictions (e.g., prohibition from political and legislative activities) to be granted tax-exempt status.

Nongovernmental organisations (NGOs) are organisations that are independent from government. Some are for-profit organisations, but the majority of NGOs are not-for-profits with a wide range of causes (e.g., human rights abuses, environmental degradation).

The Financial Action Task Force (FATF) defines the broader term "non-profit organisation" (NPO) as "a legal person or arrangement that primarily engages in raising or disbursing funds for purposes such as charitable, religious, cultural, educational, social or fraternal purposes, or for the carrying out of other types of 'good works.'"

1495. What are the heightened money laundering and terrorist financing risks of charitable organisations?

The heightened risk of charitable organisations lies in the following:

- Cash-intensive
- Lack of transparency in complex transactions
- Increased frequency of international transactions
- Global presence facilitates quick transfer of funds internationally
- Varied source of funds (e.g., funds received from donors around the world)
- Subject to little or no oversight

Historically, NGOs and charities have been susceptible to abuse by terrorists.

1496. How can charitable organisations be abused by money launderers and tax evaders?

Charitable organisations can be abused by the charity itself, by donors or other third parties in many ways, including but not limited to, the following:

- Embezzlement/misuse of donations received by the charitable organisation;
- Inaccurate valuation of donated assets by the charitable organisation;
- Wilful abuse of tax relief or tax benefits through the submission of fraudulent tax returns by the charitable organisation;
- Posing as a false charitable organisation to receive donations;
- Submission of falsified donation receipts with tax returns by donors;
- Fraud committed by an intermediary (e.g., tax return preparer); or
- Identity theft (e.g., criminal submits falsified tax returns and collects tax refund in lieu of the charitable organisation).

For more examples of methods of abuse, red flags to detect potentially suspicious activity of charitable organisations and case studies by country, please refer to the Organisation for Economic Co-Operation and Development's (OECD) Report on Abuse of Charities for Money-Laundering and Tax Evasion (2009). For further guidance on offshore tax evasion, please refer to the section Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act.

1497. How can charitable organisations or charitable giving be abused by terrorist organisations?

Terrorist organisations have abused charitable organisations and charitable giving to raise funds, evade sanctions and to generate support for their activities (e.g., ideological and logistical support, recruitment). Examples include, but are not limited to, the following:

- Use of legitimate charitable organisations to raise, conceal and transfer funds or evade sanctions
- Creation of front organisations to raise, conceal and transfer funds or evade sanctions
- Diversion of funds (e.g., humanitarian aid) to terrorist organisations, both with or without the knowledge of charitable organisations, through formal or informal affiliations with terrorist organisations
- Use of logistical networks and programs to generate support and recruit supporters

According to the U.S. State Department's "Country Reports on Terrorism," one of the most common methods of terrorist financing is kidnapping for ransom. Other major sources include private donations, directly or indirectly through charitable organisations, revenue from legitimate businesses and illicit revenue from criminal activities (e.g., smuggling, narcotics trafficking).

1498. What are private foundations, and do they pose the same degree of ML/TF risk as charitable organisations?

According to the IRS, private foundations are distinct from public charities in that they typically have a single major source of funding (e.g., gifts from a family or corporation), mostly make grants to other charitable organisations or individuals and do not directly operate a charitable program. Insider abuse aside, due to the clearer source of funds and limited operations, private foundations are not as inherently high-risk for ML/TF as public charities.

1499. What is a "zakat"?

The practice of almsgiving within the Islamic faith is called a "zakat." Donations can be given to "zakat committees," which direct funds to Islamic charitable organisations or community-based initiatives aimed at aiding the poor.

International and U.S. regulatory authorities have stressed the importance of not disrupting legitimate charitable giving such as zakats or G'machs while guarding against abuse from terrorist organisations.

1500. What is a "G'mach"?

The practice of almsgiving in the Jewish community is called "G'mach" which stands for "gemilut chasadim" or "acts of loving kindness."

1501. Do all charitable organisations pose the same degree of risk?

No. The risks of each charitable organisation should be assessed based on a variety of factors, including, but not limited to, the following:

- The strength of AML/CFT laws in the home country and country(ies) of operation
- Affiliation with a trusted entity
- Reputation of the principals/owners
- Nature and geography of volunteer, donor and recipient base
- Size and geography of operations
- Purpose of the charitable organisation
- Funding and disbursement criteria.

Evaluating the risks of charitable organisations in this manner will result in different risk ratings (e.g., low, moderate, high).

For further guidance on customer due diligence measures and risk ratings, please refer to the sections Know Your Customer, Customer Due Diligence and Enhanced Due Diligence and Customer Risk Assessments.

1502. Do all not-for-profits (NPOs) pose the same degree of risk as charitable organisations?

No. An NPO can be an association of people with a shared interest that does not distribute profits to its members (e.g., professional associations). As defined above, a charitable organisation operates with a mission to benefit the public interest with a funding structure that may involve receiving donations from numerous third parties. Charitable organisations are generally considered higher risk for abuse than NPOs, but financial institutions should consider individual factors when assessing the AML/CFT risks of NPOs.

1503. Should measures be directed at other parties beyond donors and beneficiaries?

Yes. Mitigating measures should be directed at donors, beneficiaries, volunteers and key employees within charitable organisations, such as officers, directors, trustees, both current and former.

1504. What due diligence can be conducted by financial institutions on charitable organisations to mitigate ML/TF risks?

Financial institutions may consider conducting the following due diligence on charitable organisations:

- Reviewing policies and procedures and internal reports addressing self-guided efforts of the charitable organisation to combat against ML/TF
- Reviewing national ML/TF response of the jurisdiction(s) in which the charitable organisation is located and operates
- Confirming licensing and/or registration and reviewing required public disclosures (e.g., annual information return) with proper authorities (e.g., state, Internal Revenue Service [IRS])
- Reviewing if charitable programs align with stated mission (e.g., locations, consistent with expected and historical transaction activity)

- Reviewing senior management, key partnerships, major donors (or general transparency of funding sources and integrity of accounting and financial reporting practices) and primary beneficiaries
- Conducting research of public sources (e.g., media reports, social media profiles) for negative news (e.g., history of abuse by terrorists)

1505. Are there specific AML/CFT requirements for charitable organisations?

Although not required to maintain an AML Program, charitable organisations are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)).

However, key domestic and international groups such as the Financial Action Task Force (FATF) have highlighted the need for charitable organisations to establish AML/CFT controls due to their risk of being abused by money launderers and financiers of terrorism. In order to establish accounts at financial institutions, charitable organisations already may be required to implement basic AML/CFT controls to mitigate the risks associated with their work (e.g., knowing their donors and beneficiaries).

Additionally, assuming they are U.S. companies, all charitable organisations are required to comply with Office of Foreign Assets Control (OFAC) laws and regulations. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1506. Are charitable organisations required to file Suspicious Activity Reports (SARs)?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages charitable organisations to file a SAR voluntarily for reporting suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

For further guidance on these BSA reporting requirements, please refer to the sections Form 8300 and Suspicious Activity Reports.

1507. If terrorism-related activity is detected related to charitable organisations (e.g., beneficiary is a suspected terrorist), how should OFAC be notified?

OFAC developed a “Counter-Terrorist Referral Form for Charities” to report suspected terrorism-related activities. The form requests a contact person, a description of the suspicious activity and any additional information (e.g., documents) that support the referral.

The OFAC form is available at http://www.treasury.gov.

If a charitable organisation confirms a positive match with a designee on OFAC Sanctions Lists (e.g., Specially Designated Nationals and Blocked Persons List [SDN List]), a Report of Blocked Transactions or a Report of Rejected Transactions should be filed with OFAC.

For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Program section.

1508. Should referrals be submitted for activities beyond "terrorist financing"?

Yes. The Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) criminalised terrorist financing as well as other activities dealing with terrorism, including providing material support or resources to designated terrorists or terrorist organisations, providing or collecting terrorist funds, concealing or disguising material support or funds to terrorists and receiving military-type training from terrorist organisations.

1509. Are OFAC designations limited to foreign charitable organisations?

No. There are several charitable organisations designated as foreign terrorist organisations (FTOs) under OFAC's Counter Terrorism Program operated out of the United States, including, but not limited to, the following:

- Holy Land Foundation (HLF) (formerly known as the Occupied Land Fund) was a California-based charity designated as an FTO in 2001 and 2002 for providing support to Hamas.
- Benevolence International Foundation (BIF-USA), an Illinois-based charity, was designated as an FTO in 2002 for providing support to Osama Bin Laden and Al Qaida, with additional designations in 2002 and 2003 for its branches in Canada, Bosnia and the Netherlands.
- Multiple offices of the Al Haramain Islamic Foundation (AHF) were designated as FTOs for providing support to Al Qaida in 2004, including branches located in Ethiopia, Indonesia, Kenya, Pakistan, the Netherlands and the United States (Oregon). In 2008, all branches of AHF were designated as FTOs.
- Islamic African Relief Agency (IARA) was a Sudanese-based charity, with an office in Missouri, designated as an FTO in 2004 for providing support to Osama Bin Laden and Al Qaida's precursor, Maktab Al-Khidamat (MK).
- Goodwill Charitable Organisation (GCO) was a Michigan-based charity designated as an FTO in 2007 for providing support to Hezbollah. GCO has no known relation to the better known Goodwill Industries International, Inc.
- Tamils Rehabilitation Organisation and Tamil Foundation, a Sri-Lankan-based charity with offices in Maryland, were designated as FTOs in 2007 and 2009, respectively, for providing support to Liberation Tigers of Tamil Eelam (LTTE), also an FTO.

For further guidance on OFAC's counter-terrorism related efforts, please refer to the Counter-Terrorism Program section.

1510. What agency is responsible for providing oversight of charitable organisations?

The IRS Tax Exempt and Government Entities Division (IRS-TEGE) provides federal oversight to all nonprofit organisations in the United States through the review of applications for tax-exempt status and subsequent audits. The IRS-TEGE also conducts examinations of applications and returns filed to determine if the nonprofit organisations are facilitating terrorist financing.

1511. How do U.S. AML/CFT laws for charitable organisations correspond to FATF Recommendations?

FATF Recommendation 8 – Non-Profit Organisations suggests the implementation of a legal and regulatory framework that protects nonprofit organisations from abuse by terrorist organisations, including, but not limited to, terrorist financing and other types of support (e.g., recruitment). Measures are suggested for both supervisors and nonprofit organisations such as examinations, licensing, registration, periodic reporting of financial activities and the implementation of due diligence programs for donors, beneficiaries and affiliated nonprofit organisations. In 2015, Recommendation 8 was revised to address the evolution of threats and mitigating responses in the NPO sector. Additional revisions to the accompanying Interpretative Note are anticipated, including, but not limited to, the following:

- Guidance on the application of the risk-based approach to the NPO sector as outlined in previous FATF publications (e.g., Best Practices Paper on Combating the Abuse of Non-Profit Organisations [2015])
- Refining key terminology (e.g., adoption of functional definition of NPO) to distinguish from inherently higher-risk organisations within the NPO sector
- Guidance on understanding ML/TF risks of domestic NPOs, in addition to foreign NPOs

Recommendation 5 – Terrorist Financing Offense and Recommendation 6 – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing addresses terrorist financing for all sectors, including the criminalisation of terrorist financing and the implementation of sanctions to deter terrorist financing.

In the U.S., federal oversight of charitable organisations is provided by the IRS-TEGE. All U.S. persons, including charitable organisations, are required to comply with OFAC sanctions, including the Counter-Terrorism Program.

1512. What guidance has been issued on charitable organisations?

The following are examples of key guidance that has been issued on charitable organisations:

- **Nongovernmental Organisations and Charities – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 8: Non-Profit Organisations** (2015) by the Financial Action Task Force (FATF)
- **FATF Interpretive Note to Special Recommendation Eight: Non-Profit Organisations** (2012) by FATF
- **Best Practices: Combating the Abuse of Non-Profit Organisations (Recommendation 8)** (2015) by FATF
- **Risk of Terrorist Abuse in Non-Profit Organisations** (2014) by FATF

- **Report on Abuse of Charities for Money-Laundering and Tax Evasion** (2008) by the Organisation for Money-Laundering and Tax Evasion (OECD)
- **FATF International Best Practices for Combating the Abuse of Non-Profit Organisations** (2002) by FATF
- **Protecting Charitable Organisations** (www.treasury.gov/resource-center) – A web portal administered by OFAC
- **Compliance Guide for 501(c)(3) Public Charities** by the Internal Revenue Service (IRS)
- **Tax Information for Charities & Other Non-Profits** (https://www.irs.gov/charities-non-profits) – A web portal administered by the IRS
- **Life Cycle of a Public Charity** (https://www.irs.gov/charities-non-profits) – A web portal administered by the IRS
- **Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities** (2010) by the U.S. Department of the Treasury (updates previous versions and comments published in 2002 and 2005)
- **Office of Foreign Assets Control Regulations for Non-Governmental Organisations** (2012) by the Office of Foreign Assets Control (OFAC)
- **Risk Matrix for the Charitable Sector** (2006) by OFAC
- **Frequently Asked Questions on NGO Registration Numbers** (2002) by OFAC

Marijuana-Related Businesses

1513. Are marijuana-related businesses [MRBs] legal in the United States?

Marijuana is a Schedule I controlled substance under the Controlled Substances Act (CSA), a federal law passed under Title II of the Comprehensive Drug Abuse Prevent and Control Act of 1970, that made it illegal to manufacture, import, possess, use and distribute certain substances.

However, numerous states have legalised certain marijuana-related activities. According to the Office of National Drug Control Policy (ONDCP), state-level marijuana-related laws have ranged from legalising marijuana for medicinal uses to decriminalising marijuana (e.g., reducing penalties of existing laws to civil penalties) to legalising marijuana for recreational use.

1514. What countries have passed or proposed decriminalising marijuana-related activities?

The following are examples of countries that have, at least partially, decriminalised marijuana for medicinal or recreational use:

- Australia
- Canada
- Czech Republic
- India

- Iran
- France
- North Korea
- Mexico

1515. How many states have passed or proposed decriminalising marijuana-related activities?

According to the ONDCP, at the time of this publication, over 20 states have passed legislation legalising marijuana-related activities for medical purposes and nearly 10 states have legalised marijuana for recreational use.

1516. What guidance has been provided to address the conflicting federal and state marijuana-related laws?

Multiple petitions and laws have been proposed on the federal and state levels to resolve the conflict by decriminalising marijuana on a federal level, rescheduling marijuana for medical use, providing protection to financial institutions when providing financial services to MRBs, allowing for the creation of banking cooperatives by MRBs or by granting states the power to regulate the industry themselves, similar to alcohol. Examples include, but are not limited to, the following:

- **Ending Federal Marijuana Prohibition Act of 2013**
- **States' Medical Marijuana Patient Protection Act** (2013)
- **Respect State Marijuana Laws Act of 2013**
- **Marijuana Businesses Access to Banking Act of 2013**
- **Legitimate Use of Medicinal Marijuana Act** (2014)
- **Colorado House Bill 14-1398** – Concerning the Provision of Financial Services to Licensed Marijuana Businesses
- **Regulate Marijuana Like Alcohol Act (H.R.1013)** (2015)
- **Consolidated Appropriations Act** (2017)

The U.S. Department of Justice (DOJ) also issued two memoranda highlighting enforcement priorities as they relate to marijuana-related activities under federal law, specifically the CSA:

- **Memorandum for All United States Attorneys: Guidance Regarding Marijuana Enforcement (Cole Memo)** (August 2013)
- **Memorandum for All United States Attorneys: Guidance Regarding Marijuana Related Financial Crimes** (February 2014)

The Cole Memo included eight priorities covering public safety, public health and other law enforcement priorities:

- Preventing the distribution of marijuana to minors;

- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
- Preventing state-authorised marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on publics lands; and
- Preventing marijuana possession or use on federal property.

The 2014 DOJ memorandum provided guidance on the impact on financial crimes for which marijuana-related activities are predicate crimes. Persons found to violate any of the enforcement priorities outlined by the Cole Memo could be prosecuted under the following money laundering statutes:

- Prohibition on engaging in financial and monetary transactions with proceeds from a specified unlawful activity (SUA) pursuant to 18 U.S.C 1956 and 1957;
- The unlicensed money transmitter statute pursuant to 18 U.S.C. 1960; and
- Reporting of financial transactions involving marijuana-related violations of the CSA pursuant to the BSA.

As with the money laundering offense, prosecution under the aforementioned offenses does not require conviction on an underlying marijuana-related crime under federal or state law.

1517. Are financial institutions granted Safe Harbor from federal prosecution if they comply with the guidance provided by the DOJ memos?

No. Although, if financial institutions abide by the guidance provided in the DOJ memoranda, this may reduce their risk of federal prosecution and they may be able to rely on the DOJ's use of prosecutorial discretion as it relates to marijuana-related activities.

1518. With the recent change in administrations in the White House, are there any indicators that may reveal the direction of future legislation related to marijuana (e.g., pro-marijuana vs anti-marijuana)?

The Cole and DOJ memos released during the Obama administration indicated that the federal government would not interfere in states where nonmedical use of marijuana was legal. The Trump administration has issued multiple statements indicating a possible reversal of this policy. The

enforcement of current federal laws related to both medical and recreational marijuana remains uncertain. Early indications lean toward stricter enforcement.

1519. Are MRBs subject to the Counter Narcotics Trafficking Sanctions Program administered by the Office of Foreign Assets Control (OFAC)?

Although marijuana is not a narcotic, it is a controlled substance subject to the Foreign Narcotics Kingpin Sanctions Regulations. Significant marijuana traffickers may be designated as Specially Designated Narcotics Traffickers - Kingpins (SDNTKs) under the Counter Narcotics Trafficking Sanctions Program. Financial institutions should continue to conduct enhanced due diligence and monitoring of transactions and third parties (e.g., suppliers) associated with their MRBs to guard against abuse from these criminal elements.

For further guidance on sanctions related to drug trafficking, please refer to the Counter Narcotics Trafficking Sanctions Program section.

1520. What methods have MRBs used to gain access to the financial system when denied account services by banks?

Since a limited number of banks have been willing to accept MRBs as customers, MRBs have sought out indirect alternatives to gain access to the financial system, including, but not limited to, the following:

- Underground banking systems or informal value transfer systems (IVTSs);
- Alternative financial systems such as virtual currencies;
- Use of personal accounts for MRB activities;
- Use of pseudonyms and fictitious business names to disguise MRB activities; and
- User of third parties (e.g., armoured car services [ACS]) to gain indirect access to financial services (e.g., currency replenishment).

1521. How can financial institutions identify marijuana-related activity that may fall within any of the eight law enforcement priorities of the Cole Memo?

In February 2014, FinCEN issued guidance providing examples of red flags to assist financial institutions in detecting marijuana-related activities that may fall within the law enforcement priorities of the Cole Memo or may violate state law. Examples include, but are not limited to, the following:

- To detect the use of state-licensed MRBs as fronts to launder proceeds from criminal activities (e.g., activities not permissible under state licensing, sale of other controlled substances, other criminal activities):
    - High volume of revenue inconsistent with expected activity for the business (e.g., based on location, time period, related businesses);
    - High volume of cash deposits and withdrawals not commensurate with the amount of marijuana-related revenue reported for federal and state tax purposes;

  - Business is unable to demonstrate revenue is derived exclusively from state-licensed marijuana-related activities;
  - Excessive commingling of funds between business and personal accounts of owners or employees;
  - Transactions that appear to be conducted on behalf of seemingly unrelated third parties or for unclear business purposes; and
  - Unexplained surge in use of third-party services (e.g., equipment suppliers, shipping services).

- To detect unlicensed marijuana-related activities of existing customers:
  - Business unable to provide state license;
  - Business unable or refuses to demonstrate legitimate source of funds of account activity or other investment(s);
  - Business deposits currency that smells like marijuana;
  - Excessive payments made to owners or employees;
  - Frequent inter-state transactions with third parties (e.g., customers, vendors, suppliers) in high-risk jurisdictions (e.g., located in or near states that have legalised marijuana-related activities, high intensity drug trafficking areas [HIDTAs]);
  - Business is located on federal property or in close proximity to a school in violation of federal and state laws;
  - Marijuana sold by the business was grown on federal property in violation of federal law; and
  - Searches of publicly available sources reveal business owners, employees or other related parties are involved in the illegal purchase of drugs, violence or other criminal activity or have been subject to sanctions for violations of state or local marijuana-related laws.

For further guidance, please refer to FinCEN Advisory FIN-2014-G001: BSA Expectations Regarding Marijuana-Related Businesses.

A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments, insurance) has been provided in this publication. For further guidance on red flags, please refer to the sections: Suspicious Activity Red Flags and Drug Trafficking and Marijuana-Related Businesses Red Flags.

1522. Is the presence of a state license indicative of the legitimacy and/or legality of an MRB?

No. Since state laws impose restrictions on MRBs (e.g., sales volume beyond permitted limits, sales to minors or other states where use or possession is illegal), the fact that a business was granted a license is not indicative of ongoing compliance.

1523. Should financial institutions consider not opening an account or terminating an existing relationship if a customer is identified as an MRB?

Identification as an MRB does not imply that a customer relationship should not be extended or should be terminated. The decision to open or retain a relationship with an MRB should be defined in policy and by the risk tolerances established by the financial institution's senior management and board of directors, including consideration of the existing conflicts between state and federal law. If a financial institution does decide to open or maintain the relationship, due diligence for the customer should be more extensive and that the customer's transactions should be subject to heightened scrutiny.

1524. What policy changes should financial institutions consider to enhance their AML Programs as they relate to MRBs?

Financial institutions should consider the following:

- Documenting and disseminating the institution's policy on accepting MRB customers;
- Designing and implementing a process to collect due diligence information that will enable the identification of MRB customers;
- Designing and implementing a process for identifying red flags to help detect instances of illicit dispensaries attempting to gain access to the institution under the guise of a legal entity;
- Validating and enhancing customer risk scoring methodologies to ensure MRB customers are appropriately rated;
- Establishing processes for obtaining information on the number of dispensary licenses to be granted in the state, approval requirements for applicants and thresholds for activity at the state level (versus the individual level for a specific MRB); and
- Implementing an enhanced monitoring program to identify activity exceeding the MRB's permitted volumes and to distinguish illicit activity above the legalised limit.

1525. What due diligence can financial institutions conduct on marijuana-related business customers?

Following are examples of the types of due diligence that financial institutions can conduct on marijuana-related business customers:

- Collect and validate applicable state licenses (e.g., dispensary license);
- Review state(s) of operations as compared to the state that issued the license and conduct site-visits at the inception of the relationship and ongoing as needed;
- Collect and analyse permitted volumes and activities as indicated by state laws versus expected volumes and activities as provided by customers; and
- Conduct ongoing due diligence and monitoring of accounts for potentially suspicious activities.

1526. Should financial institutions apply similar due diligence to customers who provide peripheral MRB activities (e.g., equipment suppliers, shipping and delivery services)?

Guidance remains unclear whether enforcement authorities perceive accepting marijuana money from these peripheral sources differently from MRBs directly. Financial institutions should design a risk-based program that identifies the risks of providing services to MRBs, both directly and indirectly. Financial institutions should consider whether to maintain customer relationships with the following:

- Real estate leasing companies whose tenants may include MRBs;
- Companies that sell or lease equipment that may be used in the production or sale of marijuana;
- Third-party payment processors (TPPPs) that facilitate MRB transactions;
- Payroll service providers organised in states that have legalised marijuana;
- Money services businesses (MSBs) organised or operating in legalised jurisdictions or near MRBs;
- High net-worth or private clients with entrepreneurial investment histories or located in legalised jurisdictions;
- ATM manufacturers or providers with operations in these jurisdictions; and
- Armored car services (ACS) with operations in these jurisdictions.

1527. Are financial institutions required to file SARs on all marijuana-related activity?

Yes. To satisfy BSA requirements to report financial transactions involving proceeds from illicit activities under federal law (e.g., sale of a controlled substance such as marijuana), financial institutions must regularly file SARs on all marijuana-related activities. To distinguish legal marijuana-related activities from illicit marijuana-related activities, FinCEN has advised financial institutions to use the following phrases in their SAR narratives:

- **Marijuana Limited** – Involves marijuana-related activities that the financial institution reasonably believes do not implicate one of the Cole Memo's enforcement priorities or does not violate state law;
- **Marijuana Priority** – Involves marijuana-related activities that may implicate one of the Cole Memo's enforcement priorities or may violate state law; or
- **Marijuana Termination** – Involves marijuana-related activities that resulted in the termination of the account relationship.

1528. What SAR statistics have been provided by FinCEN on MRBs?

In March 2017, FinCEN published Marijuana Banking Update, providing SAR statistics on the aforementioned MRB phrases. Of the 28,651 MRB SARs received by FinCEN, they were distributed as follows:

- Marijuana Limited: 20,288 (71 percent)
- Marijuana Priority: 2,007 (7 percent)

- Marijuana Termination: 7,326 (26 percent)

1529. Can MRBs be eligible for CTR exemption?

No. Per FinCEN's guidance, MRBs cannot be treated as a non-listed business and therefore are not eligible for consideration for CTR exemption.

1530. Are MRBs required to establish AML Programs pursuant to Section 352 of the USA PATRIOT Act?

MRBs that do not otherwise provide services that would cause them to be included in the definition of "financial institution" per AML/CFT laws and regulations are not required to establish AML Programs, however, they are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments [CMIR], Report of Foreign Bank and Financial Accounts [FBAR]). Additionally, assuming they are U.S. persons, MRBs are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

1531. What is Internal Revenue Service Code 280E?

Internal Revenue Service (IRS) Code 280E "Expenditures in Connection with the Illegal Sale of Drugs" forbids MRBs (or any business with revenues from the illegal sale of a controlled substance) from deducting business expenses from gross income for tax filing purposes. Due to the high-tax burden IRS Code 280E creates, many fear this incentivises MRBs to evade taxes by submitting fraudulent tax returns or not filing at all. For further guidance on controlled substances, please refer to the Drug Trafficking section.

1532. What challenges have arisen within the marijuana-related industry?

Until marijuana becomes legal under federal law, many financial institutions have opted to de-risk by not offering services (e.g., bank accounts, cash management, payroll, bill payment, armoured car services) to MRBs as they did for other high-risk businesses (e.g., money services businesses [MSBs], foreign correspondents). Despite some financial institutions opting to cater to MRBs (e.g., uninsured marijuana banking co-ops), the industry has become even more cash-intensive due to their lack of access to other payment methods (e.g., debit cards, credit cards). Innovative vendors have attempted to fill this gap by offering alternative payment methods (e.g., payment apps) to assist MRBs and customers in moving away from cash transactions. Challenges persist as applications to offer traditional financial services continue to be denied by the federal government. As the need for financial services continues to grow, MRBs may look to less transparent means of processing payments as they continue to be locked out of traditional financial services.

1533. What guidance has been issued related to the marijuana-related industry?

The following, though not intended to be all-inclusive, lists key resources and guidance that have been issued on the marijuana-related industry:

- **National Alliance for Model State Drug Laws (NAMSDL)** is a nonprofit funded by U.S. congressional appropriations that provides research and analysis of state statutes, policies and

regulations as well as model drug laws to assist local, state and federal stakeholders in implementing comprehensive and effective drug and alcohol laws, policies, regulations and programs. Some publications released by NAMSDL include, but are not limited to, the following:

  - **Marijuana: Comparison of State Laws Allowing Use for Medicinal Purposes** (2015, 2017)
  - **Marijuana: Comparison of State Laws Legalizing Personal, Non-Medical Use** (2016)
  - **Marijuana: Laws Allowing the Limited Use of Low-THC for Medicinal Purposes** (2015)
  - **The Legalization of Marijuana in Colorado: Volume 2** (2014)

- **Marijuana Resource Center** administered by the Office of National Drug Control Policy (ONDCP) of the United States Government provides the following resources:
  - **Answers to Frequently Asked Questions About Marijuana**
  - **State Laws Related to Marijuana**
  - **The Public Health Consequences of Marijuana Legalization**
- **BSA Expectations Regarding Marijuana-Related Businesses** (2014) by Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions: Marijuana and Banking** (2014) by the American Bankers Association (ABA)
- **Memorandum for All United States Attorneys: Guidance Regarding Marijuana Enforcement** (2013) (also known as the "Cole Memo") by the Department of Justice (DOJ) Deputy Attorney General James M. Cole
- **Memorandum for United States Attorneys: Guidance Regarding the Ogden Memo in Jurisdictions Seeking to Authorise Marijuana for Medical Use** (2011) by the DOJ Deputy Attorney General James M. Cole
- **Memorandum for Selected United States Attorneys: Investigations and Prosecutions in States Authorizing the Medical Use of Marijuana** (2009) (also known as the "Ogden Memo") by the DOJ Deputy Attorney General David. W. Ogden
- **Medical Marijuana: Review and Analysis of Federal and State Policies** (2010) by the U.S. Congressional Research Service's Mark Eddy, Specialist in Social Policy

Additional key guidance and resources on drugs and various aspects of the drug trade include, but are not limited to, the following:

- **World Drug Report** – An annual report by the United Nations Office on Drugs and Crime (UNODC) that provides an overview of major developments in drug markets related to production, trafficking, consumption and impact on health. Covered drugs included opiates, cocaine, cannabis and amphetamines (including ecstasy).

- **International Narcotics Control Strategy Report (INCSR)** – An annual report issued by the U.S. Department of State that describes over 200 countries' efforts to combat the international drug trade, money laundering and financial crimes. Highlighted groups involved in domestic and multilateral efforts to combat drug trafficking and money laundering include, but are not limited to, the following:
    - Office of Overseas Prosecutorial Development, Assistance and Training
    - Asset Forfeiture and Money Laundering Section
    - FinCEN
    - Internal Revenue Service, Criminal Investigative Division (IRS-CI)
    - United Nations Global Programme Against Money Laundering, Proceeds of Crime and the Financing of Terrorism
    - The Organisation of American States Inter-American Drug Abuse Control Commission Group of Experts to Control Money Laundering
- **OFAC Counter Narcotics Sanctions Program and Transnational Criminal Organisation Sanctions Program –** Sanctions programs administered by OFAC that block the property and interests of persons designated as significant narcotics traffickers and transnational criminal organisations.

Nonbank Financial Institutions

1534. What is meant by the term "nonbank financial institution" (NBFI)?

For purposes of our discussion, NBFIs include all entities, excluding depository institutions, considered financial institutions under the USA PATRIOT Act. These include, but are not limited to, the following:

- Money services businesses (MSBs) (e.g., licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally; currency exchanges; issuer or seller of traveller's checks, money orders or similar instruments; sellers or providers of prepaid access)
- Broker-dealers in securities
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities
- Commodity trading advisers (CTAs)
- Commodity pool operators (CPOs)
- Mutual funds
- Insurance companies
- Casinos and card clubs

- Operators of credit card systems
- Dealers in precious metals, precious stones or jewels
- Persons involved in real estate settlements and closings
- Investment advisers
- Unregistered investment companies
- Loan or finance companies (e.g., nonbank Residential Mortgage Lenders and Originators [RMLOs])
- Housing Government-Sponsored Enterprises (GSE)
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Travel agencies
- Pawnbrokers
- Telegraph companies

In August 2016, FinCEN issued a notice of proposed rulemaking (NPRM), "Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks Lacking a Federal Functional Regulator," that will expand the types of financial institutions subject to AML/CFT laws and regulations. The NPRM would remove the exemption from AML/CFT requirements (e.g., Section 326 [CIP], Section 352 [AML Program]) for banks that lack a federal functional regulator. This includes, but is not limited to, the following:

- Private banks (e.g., owned by an individual or partnership)
- Non-federally insured credit unions
- Non-federally insured state banks and savings associations
- State-chartered non-depository trust companies
- International banking entities

For additional guidance on nonbank financial institution customers, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

1535. What are the heightened money laundering and terrorist financing risks of nonbank financial institution customers?

The following characteristics may heighten the money laundering and terrorist financing risks of NBFIs:

- Cash-intensiveness
- High volume of transactions

- High-risk nature of customer base (e.g., high net worth; geographically dispersed; financially sophisticated; increased use of corporate structures, such as offshore private investment companies; lack of ongoing relationships with customers, such as MSBs and casinos)
- High-risk product offerings (e.g., ability to transfer funds domestically and internationally, particularly to jurisdictions with weak AML/CFT requirements; prepaid access/stored-value cards; transportability of merchandise; high-value merchandise; merchandise that is difficult to trace, such as precious stones)
- Ability to store and transfer value (e.g., conversion to precious gems, immediate or deferred income through insurance and other investment products, real estate)
- Grants access to funds held in foreign financial institutions or gives foreigners access to funds held in domestic financial institutions
- Subject to varying, often fewer, levels of regulatory requirements and oversight as compared to traditional financial institutions (e.g., banks, credit unions)
- Potentially weaker controls than traditional financial institutions
- Difficulty in monitoring for suspicious activity due to complex nature of transactions (e.g., involvement of multiple third parties, therefore decreasing transparency of transaction details)
- Operation without proper registration or licensing (e.g., MSBs)
- History of abuse by money launderers and terrorists

1536. Are there specific AML/CFT requirements for NBFIs?

Some NBFIs are currently subject to their own AML/CFT requirements. For example, money services businesses (MSBs) and broker-dealers are required to establish a risk-based AML Program, and file Suspicious Activity Reports (SARs) and Currency Transaction Reports (CTRs). Some financial institutions that establish account relationships with NBFIs review the AML/CFT Compliance Program of NBFIs as part of the due diligence process of their customer acceptance and maintenance programs.

Additionally, any NBFI that is affiliated with a bank holding company (BHC) will, by necessity, need to perform a risk assessment in order for the BHC to meet regulatory expectations for performing an enterprisewide risk assessment.

For further guidance on the AML/CFT requirements of NBFIs, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.

1537. Are NBFIs required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

Correspondent Banking

1538. How is the term "correspondent banking" defined?

The term "correspondent banking" is defined broadly for banking organisations to include any account or formal relationship established by a financial institution to receive deposits from, make payments to or other disbursements on behalf of a foreign financial institution (FFI) (e.g., broker-dealers, mutual funds, money services businesses [MSBs]), or to handle other financial transactions related to the FFI. Under regulation 31 C.F.R. 1010.610 – Due Diligence Programs for Correspondent Accounts for Foreign Financial Institutions, "correspondent account" is defined as:

- "An account established for a foreign financial institution to receive deposits from, or to make payments or other disbursements on behalf of, the foreign financial institution, or to handle other financial transactions related to such foreign financial institution; or
- An account established for a foreign bank to receive deposits from, or to make payments or other disbursements on behalf of, the foreign bank, or to handle other financial transactions related to such foreign bank."

In the case of broker-dealers in securities, futures commission merchants (FCMs), introducing brokers (IBs) in commodities and mutual funds, a correspondent account would include, but not be limited to, any account or formal relationship that permits the FFI to engage in regular services, including, but not limited to, those established to engage in trading or other transactions in securities and commodity futures or options, funds transfers, or other types of financial transactions.

For further guidance on the AML/CFT requirements for correspondents, please refer to Section 312 – Special Due Diligence for Correspondents and Private Banking Accounts.

1539. What is a correspondent clearing account? Does it fall under the USA PATRIOT Act's definition of a correspondent account?

Though the terms often seem to be used as synonyms, correspondent clearing accounts and correspondent accounts are not the same. A correspondent clearing account is one type of correspondent account and, as such, falls under the USA PATRIOT Act's definition of correspondent account. Correspondent clearing accounts are accounts maintained on behalf of another financial institution through which that financial institution processes or clears transactions on behalf of third parties. One example of a correspondent clearing account is a U.S. dollar clearing account maintained in the U.S. on behalf of an affiliated or third-party FFI.

1540. What is the heightened money laundering and terrorist financing risk of correspondent accounts?

Correspondent banking relationships may expose the U.S. financial system to heightened money laundering and terrorist financing risk if they are established for foreign financial institutions located in jurisdictions with non-existent or weak AML/CFT laws and regulations. Additionally, correspondent banking may involve high-volume, international transactions involving multiple parties in which no

one institution may have a direct relationship with all parties involved nor have a complete view of the entire transaction.

1541. Do all correspondent banking customers pose the same degree of risk?

No. The risks of each correspondent banking customer should be assessed based on a variety of factors, including, but not limited to, the following:

- The nature of, and markets served by, the foreign respondent's business
- The type, purpose and anticipated activity of the foreign respondent's account
- The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
- The owners and senior management of the respondent are identified as or close associates of a politically exposed person (PEP))
- The AML/CFT and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent
- The AML/CFT and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available)
- Information known or reasonably available about the foreign respondent's AML/CFT record

Evaluating the risks of correspondent banking customers in this manner will result in different risk ratings (e.g., low, moderate, high).

1542. Are correspondent banking risks isolated to activities performed on behalf of foreign respondents?

No, while the main legislative and regulatory focus has been on foreign correspondent activity, accounts maintained on behalf of domestic respondents may pose similar risks and U.S. regulators are increasingly expecting that correspondent banks subject their domestic bank portfolios to the same scrutiny as their foreign portfolios.

1543. Are there specific AML/CFT requirements for correspondent banking customers?

Yes. Due to the high-risk nature of correspondent banking, the following AML/CFT requirements have been implemented:

- Under **Section 311**, the Fifth Measure restricts or prohibits the provision of correspondent banking and PTA services to financial institutions designated as a money laundering concern. For further guidance, please refer to the Section 311 – Special Measures section.
- **Section 312** outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have correspondent banking customers. For further guidance, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.

- **Section 313** prohibits U.S. financial institutions from establishing correspondent banking relationships with foreign shell banks. For further guidance, please refer to Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks.
- **Section 319** outlines circumstances in which funds can be seized from a U.S. interbank account; requirements to retrieve bank records of foreign respondents within "120 hours"; and "foreign bank certification" requirements of foreign respondents (e.g., certifies physical presence, regulated status, prohibition of indirect use of correspondent accounts by foreign shell banks). For further guidance, please refer to Section 319 – Forfeiture of Funds in U.S. Interbank Accounts.
- Although regulations have not been issued, **Section 325** outlines restrictions on the use of concentration accounts to prevent abuse similar to that conducted through correspondent banking accounts. For further guidance, please refer to Section 325 – Concentration Accounts at Financial Institutions.
- Some **OFAC** sanctions restrict or prohibit the provision of correspondent banking and PTA services to designated entities (e.g. Iranian-linked financial institutions, financial institutions providing services to Specially Designated Nationals [SDN])). For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1544. Do the new obligations of the "Customer Due Diligence Requirements for Financial Institutions" rule impact due diligence requirements for correspondent relationships?

No. The Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule) requires covered financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership or significant control of legal entity customers.

Due diligence requirements for correspondents under the USA PATRIOT Act's Section 312 already require the collection and verification of beneficial owners for private banking customers and correspondent accounts for certain foreign financial institutions (FFIs) but with 10 percent or greater ownership or control.

For further guidance on the proposed rule, please refer to the Beneficial Owners section.

1545. What is a foreign bank certification?

A foreign respondent that maintains a correspondent account with any U.S. bank or U.S. broker-dealer in securities must certify the following in writing:

- Physical presence/regulated affiliated status
- Prohibition of indirect use of correspondent accounts by foreign shell banks
- Ownership status (for non-public institutions)

This "foreign bank certification," also known as the PATRIOT Act certification, also must include the name and address of a person who resides in the United States and is authorised to accept service of legal process for records regarding the correspondent account.

Domestic correspondents are required to obtain a foreign bank certification from each foreign respondent.

For further guidance, please refer to the Section 319(b) – Bank Records section.

1546. Are correspondents required to obtain other certifications beyond the foreign bank certification from their foreign respondents?

Pursuant to OFAC's Iranian Sanctions Program, upon receiving a written request from FinCEN, U.S. financial institutions are required to obtain a "Certification for Purposes of Section 104(e) of the Comprehensive Iran Sanctions, Accountability and Divestment Act of 2010 (CISADA) and 31 C.F.R. 1060.300" (CISADA Certification) from specified foreign respondents. The CISADA Certification requires foreign respondents to provide information on whether they have maintained a correspondent account or processed transaction(s) other than through a correspondent account, directly or indirectly, for an Iranian-linked financial institution, Iran's Islamic Revolutionary Guard Corps (IGRC) or any of its agents or affiliates designated as a Specially Designated National (SDN). For each correspondent relationship/applicable transaction, U.S. financial institutions are required to provide the following details:

- Name of Iranian-linked financial institution/IGRC-linked person;
- Name on correspondent account;
- Correspondent account number(s);
- Approximate value in USD of transactions processed (through or outside of the correspondent account) within the preceding 90 calendar days; and
- Other applicable identifying information for the correspondent account or the transferred funds.

For further guidance on the CISADA Certification, please refer to the Foreign Bank Certification section. For further guidance on sanctions, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1547. Are financial institutions expected to conduct due diligence on their customers' customers?

While there is no U.S. law that requires it, in certain situations (e.g., where a financial institution provides clearing services for a correspondent), financial institutions may be expected to demonstrate an understanding of their customers' customers. This may be accomplished by conducting due diligence directly or indirectly by requesting information from the correspondent banking customer (e.g., respondent). This policy is known as Know Your Customer's Customer (KYCC) or Know Your Correspondent's Customer (KYCC).

Due to the uncertainty around KYCC, many financial institutions have opted to de-risk by terminating high-risk correspondent accounts instead of managing the high compliance burden of such relationships. To counter de-risking activities, several agencies (e.g., U.S. federal banking regulators) have issued guidance that KYCC is not required under current AML/CFT laws and regulations.

1548. What are cover payments and how are they a challenge to monitoring correspondent clearing activity?

"Cover payments" are used in correspondent banking as a cost effective method of sending international transactions on behalf of customers. A cover payment involves several actions by financial institutions:

- Obtaining a payment order from the customer;
- Sending of a credit transfer message for an aggregate amount through a messaging network (e.g., Society for Worldwide Interbank Financial Telecommunication [SWIFT]) that travels a direct route from the originating bank to the ultimate beneficiary's bank;
- Execution of a funds transfer that travels through a chain of correspondent banks to settle or "cover" the first credit transfer message; and
- Disbursement of funds to the ultimate beneficiary in accordance with the credit transfer message.

Previous messaging standards did not include information on the ultimate originators and beneficiaries of cover payments. The lack of information posed a challenge for recordkeeping, suspicious activity monitoring and sanctions screening.

For further guidance, please refer to the Cover Payments and SWIFT section.

1549. What are "nested" relationships? What are the risks of nesting?

A "nested" relationship, sometimes referred to as downstream correspondents, occurs when a correspondent bank client provides services to other banks. Nested relationships may expose financial institutions to the risks of downstream correspondents about which the financial institution may have little knowledge. If undetected, the financial institution may provide services to correspondents for which services have been terminated.

1550. What steps can a financial institution take to mitigate the risks of correspondent banking?

Financial institutions can establish a correspondent bank monitoring program that includes the following components:

- Know Your Customer (KYC) Program including due diligence and enhanced due diligence (EDD) compliant with AML/CFT requirements that enables an understanding of risks and provides context for ongoing suspicious activity monitoring. In addition to the EDD requirements, the KYC Program should also address foreign bank certifications and politically exposed persons (PEPs).
- Customer segmentation for risk identification and profiling purposes.

- Multifaceted monitoring programs that may include, depending on the nature of the correspondent account relations:
    - Routine transaction monitoring
    - Monitoring of product usage/deviation by respondent
    - Monitoring of underlying (or pseudo) customers of correspondent clearing accounts
    - Holistic customer reviews
    - A correspondent bank visitation program to update KYC information and resolve any questions that may arise through monitoring
    - Proactive tracking and response to emerging risks and negative news

1551. What are examples of correspondent bank activities that are considered higher risk?

Higher risk activities include, but are not limited to, the following:

- Third-party clearing (including clearing of U.S. dollar drafts)
- Pouch activities
- Bulk cash activities
- Payable-through accounts (PTAs)
- Concentration accounts
- Funds transfer activities
- Automated clearing house (ACH) activities
- Trade finance activities
- Nested relationships

1552. What international efforts have been made to collect and share due diligence information on correspondent banks?

The Society for Worldwide Interbank Financial Telecommunication (SWIFT) has developed a KYC Registry that collects correspondent banking due diligence information and documentation submitted by financial institutions in accordance with international best practices (e.g., Wolfsberg AML Principles for Correspondent Banking). The KYC Registry aims to create a global standard from a single validated source to ease the complex and often inconsistent due diligence standards for correspondent banking. Examples of due diligence and documents maintained by the KYC Registry include, but are not limited to, the following:

- Banking licenses
- Corporate governance documents (e.g., bylaws, articles of incorporation)
- Foreign bank certifications as required by Section 319 of the USA PATRIOT Act

- AML/CFT Policies and Procedures related to correspondent banking services

Participation in the registry is voluntary.

Additionally, multiple vendors providing regulatory solutions, often referred to as "regtech," are providing agile cloud-based technology solutions for KYC repositories and customer verification across the globe. For further guidance on AML/CFT technology solutions, please refer to the AML/CFT Technology section.

1553. How do U.S. AML/CFT requirements compare to the FATF Recommendations for correspondent banking customers?

U.S. AML/CFT laws have incorporated the following:

- **Recommendation 13 – Correspondent Banking** – FATF recommends financial institutions implement measures to mitigate the risks of cross-border correspondent banking and PTAs, including, but not limited to, the following:
  - Risk-based due diligence program to understand the nature of the respondent's business; the respondent's AML Program, especially as it relates to PTAs; and the respondent's public history of money laundering or terrorist financing investigations or regulatory actions;
  - Requiring senior management approval for new correspondent banking relationships; and
  - Prohibiting establishing correspondent banking relationships with shell banks.
- **Recommendation 19 – Higher Risk Countries** – FATF recommends financial institutions implement enhanced measures for correspondent banking relationships in high-risk countries (e.g., more frequent monitoring, termination).

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

1554. What guidance and information have been issued on correspondent banking?

Among the key guidance and information issued on correspondent banking are the following:

- **Correspondent Banking – Overview (Domestic and Foreign)** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 13: Correspondent Banking** (2012) by the Financial Action Task Force (FATF)
- **Risk Management Guidance on Periodic Risk Reevaluation of Foreign Correspondent Banking** (2016) by the Office of the Comptroller of the Currency (OCC)
- **Wolfsberg AML Principles for Correspondent Banking** (2014) by the Wolfsberg Group of Banks (Wolfsberg Group).

- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2014) by the Wolfsberg Group
- **Guiding Principles for Anti-Money Laundering Policies and Procedures in Correspondent Banking (Exposure Draft)** (2014) by The Clearing House
- **Guidelines for Counter Money Laundering Policies and Procedures in Correspondent Banking** (2002) by The Clearing House
- **Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism** (2017) (includes revisions to Annex II – Correspondent Banking and Annex IV – General Guide to Account Opening) by the Basel Committee on Banking Supervision
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payment Mess**ages (2009) by the Wolfsberg Group
- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** (2009) by the International Finance Corporation (IFC), the private sector arm of the World Bank Group
- **Application of Correspondent Account Rules to the Presentation of Negotiable Instruments Received by a Covered Financial Institution for Payment** (2008) by Financial Crimes Enforcement Network (FinCEN)
- **Application of the Correspondent Account Rule to Executing Dealers Operating in Over-the-Counter Foreign Exchange and Derivatives Markets Pursuant to Prime Brokerage Arrangements** (2007) by FinCEN
- **Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries** (2006) by FinCEN
- **Application of the Regulations regarding Special Due Diligence Programs for Certain Foreign Accounts to NSCC Fund/SERV Accounts** (2006) by FinCEN
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-border Wire Transfers** (2008) by the Basel Committee on Banking Supervision of the Bank of International Settlements (BIS)
- **U.S. Senate Hearing on the Role of U.S. Correspondent Banking in International Money Laundering** (2001)
- **Senate Permanent Subcommittee Hearing on "U.S. Vulnerabilities to Money Laundering and Terrorist Financing: HSBC Case History"** (2012)

For additional guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks, Section 319 – Forfeiture of Funds in U.S. Interbank Accounts, Foreign Bank Certifications, and Section 311 – Special Measures.

Third-Party Payment Processors

1555. What is a third-party payment processor?

Third-party payment processors (TPPPs) provide payment-processing services to third-party business entities (e.g., banks, merchants). TPPPs include, but are not limited, to the following:

- Funds transfer
- Check clearing
- Debit/credit cards processing
- Automated teller machine (ATM) networks
- Remote deposit capture (RDC) services
- Automated clearing house (ACH) networks

Financial institutions often utilise TPPPs as vendors to assist with payment processing needs on behalf of themselves of their customers.

Additionally, TPPPs may be customers of financial institutions that may use their accounts to conduct payment processing for the TPPP's clients who are often merchants with their own customers.

1556. What are the heightened money laundering and terrorist financing risks of TPPPs?

With the exception of operators of credit card systems, TPPPs are considered higher risk because they are not required to maintain an AML Program and their accounts at the financial institution are used to conduct payment processing services for merchants with whom financial institutions may not have a direct relationship. This increases risk because of the complexity of verifying the merchant identities and business practices, and the difficulty in identifying the nature and the source of the transactions.

1557. What is an independent sales organisation?

The FDIC defines an independent sales organisation (ISO) as an "outside company contracted to procure new merchant relationships."

1558. What is the relationship between a merchant and a payment processor?

A merchant is a business that has contracted with a payment processing service (e.g., credit card payment processor) and accepts the credit cards as a method of payment for its goods or services.

1559. What types of merchants of TPPP networks are considered higher-risk?

Merchants that pose a higher risk to fraud, money laundering and terrorist financing include, but are not limited to, the following:

- Online gambling operations
- Payday lenders
- Mail order and telephone order companies

- Telemarketing companies
- Adult entertainment businesses
- Entities located in high-risk jurisdictions (e.g., offshore)

Some higher-risk merchants routinely use TPPPs to process their transactions because of the difficulty they have in establishing a direct account relationship.

1560. What are some examples of due diligence that should be conducted on customers that are third-party payment processors?

Following are examples of the types of due diligence that can be performed on customers who are third-party payment processors:

- Review the TPPP's corporate documentation, including independent reporting services, contracts or references.
- Review public databases, such as the Better Business Bureau (BBB) and Federal Trade Commission (FTC), to identify potential problems or concerns with the merchant, ISO and/or principal owners.
- Review the TPPP's and merchant's promotional materials and website to determine the target clientele.
- Determine if the processor resells its services to a third party who may be referred to as an "agent or provider of ISO (sub-ISO) opportunities."
- Review the TPPP's policies, procedures and processes to determine the adequacy of due diligence standards for new merchants.
- Identify the major lines of business and volume for the TPPP's customers.
- Verify directly, or through the TPPP, that the merchant is operating a legitimate business by comparing the merchant's identifying information against public record, fraud and bank check databases.
- Visit the TPPP's business operations center.

1561. What type of information can a financial institution request about a TPPP's merchants in order to better understand the relationship?

Financial institutions can request the following merchant information:

- Merchant's name
- Principal business activity
- Geographic location
- Sales techniques, such as telemarketing and online sales.

- Charge-back history, including rates of return for ACH debit transactions and remotely created checks (RCCs)
- Method of credit card payment (i.e., swiping the credit card versus keying in the card number)
- Consumer complaint history

1562. What is a remotely created check?

A remotely created check (RCC), also known as a demand draft, telecheck, preauthorised draft, paper draft or digital check, is a payment instrument that is typically created by the payee when an account holder authorises a payee to draw a check on his or her account but does not sign the check. In lieu of a signature, the RCC may bear the customer's printed name or a statement that the customer authorised the RCC. Because RCCs do not have signatures, they are more difficult to authenticate and therefore more susceptible to fraud.

For further guidance, please refer to the Remote Deposit Capture section.

1563. Are TPPPs required to establish AML Programs pursuant to Section 352 of the USA PATRIOT Act?

Businesses that function solely as TPPPs (i.e., are not included in the definition of "financial institution" per AML/CFT laws and regulations) are not required to establish AML Programs; however, they are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments [CMIR], Report of Foreign Bank and Financial Accounts [FBAR]). Additionally, assuming they are U.S. persons, TPPPs are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

Also, in order to establish accounts at financial institutions, TPPPs may be required to implement basic AML/CFT controls to mitigate the risks associated with their services.

Additionally, participants in some payment systems (i.e., ACH systems, card systems, check collection systems, money transmitting businesses, wire transfer systems) are required to comply with the Unlawful Internet Gambling Enforcement Act (UIGEA) and Regulation GG. For further guidance, please refer to the Illegal Internet Gambling and Fantasy Sports Wagering section.

1564. Are TPPPs included in the definition of money services businesses?

Generally, no. A money services business (MSB) is defined as any organisation offering one or more of the following services:

- Issuer and seller of money orders and traveller's checks
- Check casher
- Dealer in foreign exchange
- Provider or seller of prepaid access
- Money transmitter

According to FinCEN, a merchant payment processor, also known as a TPPP, processes payments from consumers as an agent of the merchant to which the consumers owe money, rather than on behalf of the consumers themselves; therefore, it does not meet the regulatory definition of a money transmitter. The role of the merchant payment processor in these transactions is to provide merchants with a portal to a financial institution that has access to the payment system (e.g., ACH); it is not to transmit funds on behalf of third parties. If the TPPP provides other services beyond processing payments (e.g., check cashing), it may qualify as an MSB (or an agent of an MSB) and be subject to AML/CFT requirements for MSBs. Some banks have required or urged TPPPs to register as a condition to providing them with services; other TPPPs have voluntarily done so to provide additional assurance that they are mitigating ML/TF risks by establishing an AML Program.

For further guidance on MSBs, please refer to the Money Services Businesses section.

1565. How should TPPPs be monitored for potentially suspicious activity?

Financial institutions should examine the accounts of third-party payment processors for potentially suspicious activity by monitoring for common red flags including, but not limited to, the following:

- There are high rates of returns/charge-back history (e.g., ACH debit transactions and RCCs returned for insufficient funds and/or as unauthorised). A high charge-back history is often indicative of merchants processing fraudulent transactions such as unauthorised ACH debits (e.g., customer discontinues a service, therefore stops payment; however, merchant continues to process ACH debits), fraudulent checks (e.g., unauthorised RCCs, altered payees, amounts, dates).
- There is significant variance in expected/historical activity versus actual activity in terms of the volume and types of transactions conducted through the account.

Since many financial institutions will not have access to the underlying details of transactions conducted by merchants, they must rely on the monitoring conducted by their TPPPs to detect potentially suspicious activity. As stated above, financial institutions should conduct appropriate due diligence on TPPPs at the inception of the relationship, including a review of applicable merchant due diligence and monitoring programs.

For additional guidance on red flags, please refer to the Suspicious Activity Red Flags section.

1566. Are TPPPs obligated to report potentially suspicious activity of their merchants?

Businesses that function solely as TPPPs (i.e., are not included in the definition of "financial institution" per AML/CFT laws and regulations) are currently not required to file SARs; however, as stated above, participants in some payment systems are required to report suspected illegal gambling activities of their merchants pursuant to the Unlawful Internet Gambling Enforcement Act (UIGEA) and Regulation GG. TPPPs may choose to report potentially suspicious activity voluntarily. For further guidance on the UIGEA, please refer to the Illegal Internet Gambling section.

1567. What guidance has been issued on third-party service providers (TPSP)?

The following are examples of guidance that has been issued on third-party service providers:

- Third-Party Payment Processors – Overview within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- FATF Recommendation 17: Reliance on Third Parties (2012) by the Financial Action Task Force (FATF)
- Retail Payment Systems and Wholesale Payment Systems Booklet (2004) within the FFIEC Information Technology Examination Handbook by the FFIEC
- Third-Party Senders and the ACH Network: An Implementation Guide (2012) by The Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)
- Bank Use of Foreign-Based Third-Party Service Providers (2002) by the Office of the Comptroller of the Currency (OCC)
- Risk Management Principles for Third-Party Relationships (2001) by the OCC
- Payment Processor Relationships (2012) by the Federal Deposit Insurance Corporation (FDIC)
- Guidance on Managing Third-Party Risk (2008) by the FDIC

Owners/Operators of Privately Owned Automated Teller Machines (ATMs)

1568. What is an "automated teller machine (ATM)"?

An automated teller machine (ATM) is an electronic banking device that can be used by customers without the aid of a representative (e.g., teller) for the following types of services:

- Accessing account information (e.g., balance inquiry, account statements)
- Withdrawing and/or depositing funds (e.g., cash, monetary instruments)
- Transferring funds between linked accounts
- Bill payment

In some instances, customers may be able to manage value on prepaid access cards through ATMs.

1569. What are the heightened money laundering and terrorist financing risks associated with ATMs?

Due to the nature of non-face-to-face interactions of ATMs, they are of heightened risk for money laundering and terrorist financing. Examples of suspicious activity conducted through ATMs include, but are not limited to, the following:

- Structuring/smurfing transactions, domestically and internationally to evade BSA reporting requirements (e.g., Currency Transaction Reports [CTRs], Report of International Transportation of Currency or Monetary Instruments [CMIRs])
- Abuse as an informal money transmitter (e.g., deposit funds in one jurisdiction for withdrawal by a third party in another jurisdiction)

- Fraud (e.g., check fraud, identity theft, personal identification number [PIN] theft, account takeover)

1570. What is a "privately owned ATM"?

A privately owned automated teller machine is an ATM not owned by a financial institution.

Privately owned ATMs are often found in convenience stores, bars, restaurants, grocery stores and check-cashing establishments.

1571. What are the heightened money laundering and terrorist financing risks associated with privately owned ATMs?

Privately owned ATMs are considered high risk because U.S. law enforcement has observed an increase in their use in money laundering, identity theft and fraud schemes. For example, owners or operators of privately owned ATMs may use illicit cash (of their own or from their customers) to replenish their ATMs, as opposed to legitimate sources (e.g., cash from sales, cash from a financial institution).

Additionally, most states do not monitor or require registration of owners or operators of privately owned ATMs, thereby making it difficult to track current ownership.

1572. How can financial institutions identify which customers have privately owned ATMs?

If due diligence does not include an inquiry as to whether the customer maintains a privately owned ATM, financial institutions may be able to identify these customers by performing site visits and/or monitoring the accounts of select high-risk customers (e.g., stores, bars, restaurants, grocery stores, check-cashing establishments) for spikes in cash activity.

1573. Are owners and operators of privately owned ATMs required to establish AML Programs pursuant to Section 352 of the USA PATRIOT Act?

Unless they provide services that would otherwise qualify them as financial institutions, owners and operators of privately owned ATMs are not required to establish AML Programs; however they are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments [CMIR], Report of Foreign Bank and Financial Accounts [FBAR]). Additionally, assuming they are U.S. persons, owners and operators of privately owned ATMs are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations. For further guidance, please refer to the sections: Bank Secrecy Act and Office of Foreign Assets Control and International Sanctions Programs.

1574. Do owners and operators of privately owned ATMs fall under the definition of "money services business (MSB)"?

No. According to FinCEN Ruling FIN-2007-G006, owners and operators of privately owned ATMs that limit their services to remote access (e.g., balance inquiries and withdrawals) for their customers from their own accounts at a depository institution are not included within the definition of an MSB (e.g., currency dealer or exchanger, money transmitter). For example, the exclusion applies in the following limited scenario:

- Customers access their accounts with cards issued by the depository institution, not the owner/operator of the ATM;
- ATM services are limited to withdrawals (and balance inquiries) that are authorised by the account-holding institution (e.g., customers cannot transfer funds to third parties);
- The account of the owner/operator held at the third-party payment processor is electronically credited for the amount of the withdrawals in exchange for a fee for providing the ATM service; and
- Owner/operator replenishes the ATM with currency drawn from its own accounts.

In the aforementioned scenario, the owner/operator would not fall under the BSA's definition of a currency dealer or exchanger or a money transmitter because it is not exchanging currency nor permitting transfers to third parties.

For further guidance on the definitions and AML/CFT requirements of MSBs, please refer to the Money Services Businesses section.

1575. What steps can a financial institution take to mitigate the risks of customers with privately owned ATMs?

To mitigate the risks of privately owned ATM relationships, financial institutions should perform initial and ongoing due diligence on privately owned ATM relationships. They also should consider including contractual commitments advising of the financial institution's expectations with respect to preventing the use of the machines for illicit activities, requiring notification of a change in ownership and monitoring shipments for unusual activity.

1576. What type of due diligence can be collected on customers who own or operate privately owned ATMs?

Following are examples of the type of due diligence that may be performed on customers that own or operate privately owned ATMs:

- Review corporate documentation, licenses, permits, contracts or references;
- Review public databases to identify potential problems or concerns with principal owners or an independent sales organisation (ISO);
- Review existing relationships with other financial services providers (e.g., sources of replenishment currency, method of delivery of currency shipment);
- Review expected volumes;
- Review and/or visit locations of privately owned ATMs.

1577. How can customers that own or operate privately owned ATMs be monitored for suspicious activity?

Financial institutions should monitor customers that own or operate privately owned ATMs for suspicious activity by comparing expected versus actual ATM activity levels, and also compare the level of activity to other customers who own or operate privately owned or bank-owned ATMs in comparable geographic and demographic locations.

For additional guidance on red flags for potentially suspicious activity, please refer to the sections: Suspicious Activity Red Flags and ATM Transactions and Owners/Operators of Privately Owned ATM Red Flags.

1578. What are some challenges to monitoring the activities of owners and operators of privately owned ATMs?

Some challenges include, but are not limited to, the following:

- Difficulty in identifying customers with privately owned ATMs
- Lack of access to all transactions if financial institutions are not the sponsoring bank

Common Carriers of Currency and Armored Car Services

1579. What is a "common carrier of currency"?

The BSA defines a "common carrier" as "any person engaged in the business of transporting individuals or goods for a fee who holds himself out as ready to engage in such transportation for hire and who undertakes to do so indiscriminately for all persons who are prepared to pay the fee for the particular service offered."

"Common carriers of currency" are a subgroup of common carriers, who "engage as a business in the transportation of currency, monetary instruments or commercial papers." FinCEN also defined the term "currency transporter" as "any person that physically transports currency, other monetary instruments, other commercial paper, or other value that substitutes for currency, as a person primarily engaged in such business, such as armoured car services and some types of cash couriers."

1580. What is an "armoured car service"?

Armored car services (ACS), a subset of common carriers of currency also referred to as "cash in transit" (CIT) operators, are "secured transporters of valuable goods, including currency for various third parties including, but not limited to, financial institutions, the Federal Reserve, the U.S. Mint and private companies. Goods may be transported via cars, airplanes and couriers."

ACSs may also act as servicing agents for financial institutions (e.g., count and sort currency and coins).

1581. What are the heightened money laundering and terrorist financing risks of common carriers of currency?

Common carriers of currency, specifically ACSs, are considered high risk because they may assist in disguising the illegal transfer of funds. ACSs transport high risk goods (e.g., currency, monetary instruments) and service high-risk customers (e.g., cash-intensive businesses, foreign financial institutions [FFIs] such as *casas de cambio*, currency exchangers), some of which are located in high-risk jurisdictions (e.g., southwest border of the United States).

U.S. law enforcement has observed an increase in their use in money laundering schemes in recent settlements, enforcement actions and law enforcement raids. According to FinCEN, approximately 10 percent of the 15 million Currency Transaction Reports (CTR) filed in 2013 involved ACS transactions.

Additionally, some ACSs have allowed their clients (e.g., money services businesses [MSBs]) to use them as proxies to gain access to the financial system, unknown to banks.

1582. Do all ACSs pose the same degree of risk?

No. Not all ACSs pose the same degree of risk. ACSs contracted by the financial institution pose less risk than ACSs hired by a private third party.

A financial institution may consider the following factors when assessing the risks of an ACS:

- Types of services offered;
- The nature of ownership (e.g., private, public);
- The location of operations (both regionally and internationally); and
- The nature and location of the ACS clients.

For further guidance on assessing risk, please refer to the Customer Risk Assessment section.

1583. Are financial institutions required to file Currency Transaction Reports (CTRs) on shipments of currency transporters (e.g., armoured car services [ACS]) in excess of US$10,000 (e.g., as conductors of the reportable transaction on the CTR)?

In 2013 and 2014, FinCEN published guidance on the treatment of reportable transactions conducted by an ACS for CTR filing purposes that superseded previous guidance. According to FinCEN guidance published in 2009, financial institutions were required to collect information (e.g., name, date of birth, identification information) on all customers and person(s) conducting reportable transactions by or on behalf of the financial institution's customer, including the ACS employee who conducted the reportable transaction (i.e., the employee that made the delivery or pickup that resulted in a deposit to or withdrawal from the reporting financial institution's account), as they are required for all reportable transactions conducted by a third party.

FinCEN provided the following guidance, superseding previous guidance on CTR obligations related to ACS-involved transactions:

- Outlines CTR obligations of financial institutions (e.g., parties that should be included on the CTR, transactions that should be aggregated) based on the business model and the roles of each party in the reportable transaction:
    - Currency originator (e.g., customer of a financial institution, financial institution or other third party)
    - Currency transporter (e.g., contracted by currency originator to transport currency shipment)
    - Shipper (e.g., actual transporter of the physical currency shipment who may not be the currency transporter, subcontractor)
    - Consignee (e.g., receiver of the currency shipment who may not be the ultimate "currency recipient")
    - Currency recipient (e.g., final beneficiary of the currency shipment)
- Distinguishes between collecting required information on the corporate entity (e.g., the ACS as a legal entity) and employee of the corporate entity (e.g., ACS employee)
- Circumstances under which currency transporters are exempted from money transmitter status

For further guidance on exceptions, exemptions and examples of filing CTRs on ACS transactions, please refer to FinCEN's rulings and publications:

- Administrative Ruling on the Application of FinCEN Regulations to Currency Transporters, Including Armored Car Services, and Exceptive Relief (2014)
- Treatment of Armored Car Service Transactions Conducted on Behalf of Financial Institution Customers or Third Parties for Currency Transaction Reports Purposes (2013)
- Appendix I: Examples of the Completion of the FinCEN Currency Transaction Report (CTR) for Transactions Involving Armored Car Services (2013)
- Treatment of Deposits by Armored Cars for Currency Transaction Report (CTR) Purposes (2009) (Superseded by 2014 FinCEN guidance)

For further guidance on CTRs, please refer to the Currency Transaction Reports section.

1584. What exceptions were granted for certain types of currency shipments involving currency transporters (e.g., ACS) as it relates to CTRs?

According to FinCEN's 2014 guidance, financial institutions are granted exceptions for currency shipments in which the shipper is acting on behalf of the currency originator under the following circumstances:

- "[T]he shipment is wholly domestic (that is, the whole shipment originates and ends within the United States); and
- [T]he currency transporter never takes more than a custodial interest in the currency or other value that substitutes for currency at any point of the transportation; and

- [T]he shipper is acting on behalf of the currency originator; and either
    - [T]he currency transporter picks up the shipment from a financial institution and the same currency transporter physically transports it to the currency originator at the specified destination; or
    - [T]he currency transporter picks up the shipment from the currency originator and the same currency transporter physically transports it to a financial institution, for final credit to the currency originator's account with that financial institution."

1585. Under what conditions are currency transporters exempted from the definition of money transmitter?

According to FinCEN's 2014 guidance, currency transporters are exempted from the definition of money transmitter if the shipper is a federally regulated financial institution, under which the physical transportation of currency is treated to be a part of the financial institution's activities and under the following conditions:

- "[C]urrency transporter is a person that is primarily engaged as a business in the physical transportation of currency or other value that substitutes for currency, such as an armoured car;
- [C]urrency transporter has no more than a custodial interest in the items transported at any time during the transportation; and
- The transportation is from one person to the same person at another location or to an account belonging to the same person at a financial institution."

If not required to maintain an AML Program, common carriers of currency are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, common carriers of currency are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

For further guidance on the AML/CFT requirements of money transmitters, please refer to the Money Services Businesses section. For further guidance on sanctions requirements, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1586. Are common carriers of currency required to file CMIRs on cross-border shipments of currency or monetary instruments they transport in excess of US$10,000?

Yes. With limited exception, common carriers of currency are required to file CMIRs on cross-border shipments of currency or monetary instruments in excess of US$10,000. Common carriers of currency can also be required to file multiple CMIRs on separate deliveries within one shipment, even if the individual delivery is less than US$10,000, unless they otherwise qualify for an exception. Moreover, although the CMIR regulations include a number of exemptions that apply to other parties, a common carrier of currency may not claim for itself any exemption for filing a CMIR that might be applicable to other parties.

For example, a bank may be exempted from filing a CMIR with respect to currency that it ships or mails via a common carrier, but the common carrier cannot apply this exemption to itself. For example, if a common carrier of currency picks up at an airport a cargo of currency air-shipped to the U.S. bank from another country, the common carrier has an obligation to file a CMIR, even though the bank does not.

1587. Can common carriers of currency rely on other parties to file a CMIR on the cross-border shipment of currency or monetary instruments they transport in excess of US$10,000?

Yes, however, if a CMIR is not filed appropriately (e.g., timely, accurately), the parties that are required to file by law will be held liable which can include the common carrier.

1588. Are there any exceptions for common carriers of currency as it relates to CMIRs?

Common carriers of currency are not required to file CMIRs when all of the following conditions are met:

- The entity is engaged as a business in the transportation of currency, monetary instruments and other commercial papers;
- The transportation consists of currency or other monetary instruments imported into the United States or exported out of the United States in an aggregate amount of more than US$10,000 in currency or other covered monetary instruments;
- The transportation takes place overland;
- The transportation takes place between a bank or a broker-dealer in securities, on the U.S. side, and a non-U.S. person, on the foreign side; and
- The shipment is picked up or delivered at the established office of the bank or a broker-dealer in securities on the U.S. side.

For further guidance, please refer to FinCEN's "CMIR Guidance for Common Carriers of Currency, Including Armored Car Services."

Deposit Brokers

1589. What does the term "deposit broker" mean?

A deposit broker is an individual or a firm that, for a fee, places customers' deposits with insured depository institutions.

1590. What is a brokered deposit?

A brokered deposit is a deposit solicited by a third party. Deposit brokers may disaggregate larger deposits to an amount covered by deposit insurance so that all interest as well as the principal is covered.

1591. What are the heightened money laundering and terrorist financing risks of deposit brokers?

The potential heightened risk of brokered deposits lies in the following:

- Use of international brokers
- Targeting of higher risk customers – e.g., non-resident aliens, offshore customers, politically exposed persons (PEPs)
- Reliance on third parties to conduct adequate due diligence and monitor for potentially suspicious activity
- Use of front companies/shells to obscure the beneficial owner and/or source of funds
- Higher-risk methods of account opening
- Commingling of funds/anonymity of underlying depositor
- Lesser degree of regulatory oversight relative to financial institutions

1592. Who is the customer of the financial institution, the deposit broker or the client of the deposit broker?

For the purpose of the Customer Identification Program (CIP) rule pursuant to Section 326 of the USA PATRIOT Act, the "customer" is the deposit broker who opens the account with the financial institution. The identity of each individual "sub-account holder" does not require verification.

1593. What steps can a financial institution take to mitigate the risks associated with deposit brokers?

To mitigate the risks that lie with deposit brokers, financial institutions may consider executing the following at the inception of the relationship and on an ongoing basis:

- Limiting business dealings to include only deposit brokers who have an established relationship with the financial institution or other trusted entity
- Conducting background checks on deposit brokers, including a review of all services offered, methods of soliciting new clients, licensing, regulatory obligations and reputation
- Restricting services for certain high-risk customer types – e.g., non-resident aliens (NRAs), PEPs or customers located in high-risk jurisdictions
- Evaluating whether the deposit broker's AML/OFAC compliance program is adequate and consistent with the policies of the financial institution

1594. Are there specific AML/CFT requirements for deposit brokers?

Many U.S. deposit brokers, such as broker-dealers, are subject to their own AML/CFT requirements.

All U.S.-based deposit brokers, whether firms or individuals, are also obligated to comply with OFAC. The requirements affecting international deposit brokers vary by jurisdiction.

1595. What specific guidance has been issued on the money laundering risk of deposit brokers?

The **Brokered Deposits – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC) offers specific guidance on the money laundering and terrorist financing risks of brokered deposits.

Professional Service Providers

1596. How is the term "professional service provider" defined?

A professional service provider, also referred to as a "gatekeeper," acts as an intermediary between its client and a third-party financial institution and may conduct or arrange for financial dealings and services on its client's behalf (e.g., management of client finances, settlement of real estate transactions, asset transfers, investment services, trust arrangements). Examples of professional service providers include, but are not limited to, the following:

- Lawyers
- Notaries
- Accountants
- Trust and asset management service providers
- Corporate service providers (e.g., company formation)
- Real estate agents

1597. What are the heightened money laundering and terrorist financing risks of professional service providers?

The heightened risk of professional service providers lies in their ability to mask the identity of underlying clients when conducting financial services on their behalf. Financial institutions often do not have any information on underlying clients as their account relationship is with the professional service provider. As such, financial institutions must rely on professional service providers to conduct appropriate due diligence to mitigate the risks of doing illicit business.

Additionally, the privacy and confidentiality adhered to by some of these service providers can be exploited by criminals, with or without the knowledge of the provider.

1598. As customers, do all professional service providers pose the same degree of risk?

No. The risks of each professional service provider should be assessed based on a variety of factors (e.g., products/services offered by the provider, associated geographies, transaction activity, history of regulatory report filings). Status as a professional service provider is only one risk factor. Evaluating the risks of professional service providers to include other variables will result in different risk ratings (e.g., low, moderate, high).

Additionally, the personal bank accounts of professional service providers may not pose as high a risk as accounts used to conduct business on behalf of their clients or their firm if employed.

1599. What are some recent examples of potential money laundering and financial crimes involving a professional service provider?

In April 2016, over 11.5 million documents from Mossack Fonseca (MF), a Panama-based law firm specialising in the formation and management of entities in tax havens, were leaked by an anonymous source, identifying the beneficial owners of 214,000 offshore entities, according to the International Consortium of Investigative Journalists (ICIJ). In September 2016, the same source that leaked the Panama Papers also leaked information from the Bahamas corporate registry, linking approximately 140 international and local politicians to offshore companies in the Bahamas. The ICIJ published the leaked information in its Offshore Leaks Database. As a result of the leaks, investigations by regulatory and tax authorities have been launched in numerous countries (e.g., United States, United Kingdom, Germany, Australia, Sweden, Hong Kong, Chile, Singapore, India). According to media reports, in February 2017, the two founders of Mossack Fonseca were arrested for their alleged involvement in a separate money laundering investigation involving corruption in Latin America.

In May 2017, between 100,000 and 200,000 emails allegedly leaked by South African officials, known as the "Gupta Leaks," revealed hidden relationships between the high-net worth Gupta family, an Indian-born South African family with a multinational business empire including computer equipment, mining and media (e.g., Oakbay Group, Linkway Trading, Accurate Investments) with public officials in the South African government (e.g., Moses Kgosana, Faith Muthambi) and possibly corrupt activity involving, among other things, improper use of public funds and state resources, kickbacks and tax evasion, according to amaBhungane Center for Investigative Journalism and other media sources. In June 2017, the Independent Regulatory Board for Auditors (IRBA) announced that they would conduct an investigation into the auditors of Gupta's Oakbay Group under South African auditing laws and regulations, particularly as it related to alleged use of public funds for a Gupta family wedding in 2013, transactions that appeared as business expenses during Oakbay Group's audit in 2014. The auditors had terminated their auditing and advisory services to the Oakbay Group entities in April 2016.

These examples had corruption, tax evasion and cybersecurity implications. For further guidance, please refer to the sections:

- Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act;
- Anti-Bribery and Corruption Compliance Programs; and
- Cyber Events and Cybersecurity.

1600. Are professional service providers required to establish AML Programs pursuant to Section 352 of the USA PATRIOT Act?

Although not required to maintain an AML Program, professional service providers are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of

Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, professional service providers are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

Trade associations and FATF have highlighted the need for professional service providers to establish AML/CFT controls due to their positions as gatekeepers and intermediaries to the financial system. In order to establish accounts at financial institutions, professional service providers already may be required by their banks to implement basic AML/CFT controls to mitigate the risks associated with their professions.

For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1601. Is there a standard to regulate professional service providers, such as corporate service providers?

Yes. Building on previously issued guidance, the Group of International Finance Centre Supervisors (GIFCS) issued the Standard on the Regulation of Trust and Corporate Service Providers (2014) that addressed AML/CFT issues as well as licensing, corporate governance, controllership and conduct issues. All GIFCS members (e.g., Antigua and Barbuda, Aruba, Barbados, Bahamas, Bermuda, British Virgin Islands, Cayman Islands, Cook Islands, Curacao and Saint Maarten, Gibraltar, Guernsey, Isle of Man, Jersey, Labuan, Macau [China], Panama, Samoa, Turks & Caicos Islands, Vanuatu) elected to voluntary comply with the GIFCS Standards, conduct self-assessments and participate in assessments conducted by peers. In 2016, GIFCS published the Methodology for Assessing Compliance with the GIFCS Standard on the Regulation of Trust and Company Service Providers (TCSPs).

The objective of the GIFCS Standard is to ensure a comprehensive regulatory framework for TCSPs and to ensure access to beneficial owner information behind trust and other corporate vehicles by competent authorities. The GIFCS Standard is organised into three parts:

- **Part I: Definitions** (e.g., TCSP, client, controller, key person)
- **Part II: Principles for Regulation**
  - Principles Relating to the Regulator
  - Principles for Regulation
  - Principles for Co-operation
  - Principles for Enforcement
    - Other Requirements on Jurisdictions
- **Part III: The Standard**
  - Licensing
  - Corporate Governance

- Controllers of TCSPs (e.g., fit and proper standards, integrity, competence, financial soundness, conflicts of interest)
- Individuals – Key Persons and Other Employees
- Control Over Vehicles (e.g., professional duties, vehicle assets, client money rules)
- Conduct (e.g., integrity, conflicts of interest, interaction with clients, advertising and communication, terms of business, complaints handling)
- Prudential (e.g., capital and liquidity requirements, accounting and records maintenance, audit requirements, insurance, liquidations and receiverships)
- Administration (e.g., record keeping requirements, data security, data protection)
- Financial Crime and International Sanctions (e.g., AML/CFT policies, national co-operation and co-ordination, regulation and supervision, bribery and corruption, international sanctions, information sharing)

1602. How do the Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule) impact professional service providers?

FinCEN's Customer Due Diligence Requirements for Financial Institutions rule (Beneficial Ownership Rule) finalised in July 2016, requires financial institutions subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers. The Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future.

While professional service providers are not subject to CIP requirements, they will be under pressure to provide beneficial ownership information on clients when establishing financial accounts with financial institutions currently subject to AML/CFT requirements in the United States and possibly directly to regulatory authorities as the GIFCS Standards for TCSPs are implemented by GIFCS-member countries.

For further guidance, please refer to the Beneficial Owners section.

1603. What guidance has been issued on professional service providers?

The following key guidance has been issued on professional service providers:

- **Professional Service Providers – Overview** (2010) and Trust and Asset Management Services – Overview (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendations 22 - 23: Designated Non-Financial Businesses and Professions (DNFBPs)** (2012) by the Financial Action Task Force (FATF)

- **Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals** (2013) by FATF
- **Guardians at the Gate: The Gatekeeper Initiative and the Risk-Based Approach for Transactional Lawyers** (2009) by the American Bar Association (ABA)
- **Standard on the Regulation of Trust and Corporate Service Providers** (2014) by the Group of International Finance Centre Supervisors (GIFCS)
- **RBA Guidance for Trust and Company Service Providers (TCSPs)** (2008) by FATF
- **RBA Guidance for Real Estate Agents** (2008) by FATF
- **RBA Guidance for Accountants** (2008) by FATF
- **Risk-Based Approach Guidance for Legal Professionals** (2008) by FATF
- **Misuse of Corporate Vehicles Including Trust and Company Service Providers** (2006) by FATF
- **Wolfsberg FAQs on Intermediaries** (2012) by the Wolfsberg Group
- **OFAC Regulations for the Corporate Registration Industry** (2004) by the Office of Foreign Assets Control (OFAC)

Business Entities: Shell Companies, Private Investment Companies and Others

1604. What types of business entities pose heightened money laundering and terrorist financing risks?

The term "business entities" generally refers to partnerships, corporations, limited liability companies (LLCs), trusts and other entities that may be used for many purposes, such as tax and estate planning. The following business entity types pose heightened risk:

- **Shell Company** generally refers to an entity without a physical presence in any country.
- **International Business Corporations (IBCs)** are corporations established in offshore jurisdictions and generally licensed to conduct business only outside the country of incorporation.
- **Private Investment Companies (PICs)** are a subset of IBCs and generally refer to companies formed by one or more individuals to own and manage his/her/their assets. Like IBCs, PICs typically are established in offshore jurisdictions with lax AML/CFT laws and regulations. Ownership is often vested through bearer shares or trusts.
- **Nominee Incorporation Services (NIS)** are intermediaries that establish U.S. shell companies, open bank accounts and act as registered agents on behalf of foreign clients.

1605. Are "shelf companies" the same as "shell companies"?

"Shelf companies" generally refers to aged business entities with no business activity that "stay on the shelf" until purchased by an individual. Benefits of shelf companies include, but are not limited to, the following:

- Shortened timeline to incorporate a business; and
- Increased credibility with potential clients or creditors due to being "seasoned" or aged.

1606. What are the heightened money laundering and terrorist financing risks of these high-risk business entities?

The heightened risk of these business types lies in the lack of ownership transparency and minimal or no recordkeeping requirements, financial disclosures and supervision.

Additionally, the privacy and confidentiality adhered to by some of these service providers can be exploited by criminals, money launderers and terrorists.

1607. As customers, do all of the business entities described above pose the same degree of risk?

No. The risks of each business entity should be assessed based on a variety of factors (e.g., entity was created by the financial institution [e.g., trust], status as an affiliate of a trusted entity, products/services offered by the entity, associated geographies, transaction activity). Status as the aforementioned business entity types is only one risk factor. Evaluating the risks of the business entities in this manner will result in different risk ratings (e.g., low, moderate, high). For further guidance, please refer to the Risk Assessments section.

1608. Is there a legitimate purpose for establishing these types of business entities?

The legitimate reasons for establishing these businesses include:

- Asset protection
- Estate planning
- Privacy and confidentiality
- Reduction of tax liability
- Engagement in international business
- Assistance in organising complex legal entities
- Gaining access to investments in foreign jurisdictions that otherwise would be inaccessible due to the residency status of the investor

1609. What are "special purpose vehicles"?

A special purpose vehicle (SPV), also known as a special purpose entity (SPE), bankruptcy-remote entity or orphan company, is a corporation, trust, partnership or limited liability company that is

created for a limited purpose, generally to isolate financial risk. An SPE may be owned by one or more other entities. Similar to the business entities described above, SPEs can be exploited by criminals.

1610. What are offshore financial centres?

Offshore financial centres (OFCs) are jurisdictions that have a relatively large number of financial institutions engaged primarily in business with non-residents. OFCs are generally known for their favourable tax climate and bank secrecy laws. Some examples of OFCs include Bermuda, the British Virgin Islands, the Cayman Islands, Cyprus, the Isle of Man and Panama. Additional information, including assessments of OFCs, can be found on the International Monetary Fund's (IMF) website: www.imf.org.

1611. How is the term "beneficial owner" defined?

A "beneficial owner" generally is someone (an individual or a business) who has a level of control over, or entitlement to the funds or assets in the account that, as a practical matter, enables the individual, directly or indirectly, to control, manage or direct the account. The ability to fund the account or the entitlement to the funds of the account alone, without corresponding authority to control, manage or direct the account, such as an account in which a minority age child is the beneficiary, does not cause an individual to become a beneficial owner.

The term reflects recognition that a person in whose name an account is opened is not necessarily the person who ultimately controls such funds or who is ultimately entitled to such funds. "Control" or "entitlement" in this context is to be distinguished from mere legal title or signature authority.

Two key AML/CFT laws and regulations offer differing definitions and requirements for beneficial owners:

- USA PATRIOT Act Section 312 - Special Due Diligence for Correspondent Accounts and Private Banking Accounts
- FinCEN's "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule)

Section 312 defined "beneficial owners" as "individual[s] who [have] a level of control over [of 10 percent], or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual[s], directly or indirectly, to control, manage or direct the account."

The Beneficial Ownership Rule uses a two-pronged concept – ownership and effective control – by defining a "beneficial owner" as a natural person, not another legal entity, who meets the following criteria:

- **Ownership prong** – Each individual, up to four, who owns, directly or indirectly, 25 percent or more of the equity interest in a legal entity customer; and
- **Control prong** – At least one individual who exercises significant responsibility to control, manage or direct (e.g., a C-suite Executive, Managing Member, General Partner, President, Treasurer) the legal entity.

In cases where an individual is both a 25 percent owner and meets the control definition, that same individual can be defined as a beneficial owner under both prongs. From an industry perspective, the second prong improves upon the definition in the advanced notice of proposed rulemaking (ANPR) issued in 2012. The earlier definition would have required the identification of the individual who had "greater responsibility than any other individual."

1612. Are financial institutions currently required to identify and verify beneficial owners?

Yes. Prior to the finalisation of the Beneficial Ownership Rule, covered financial institutions were required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule now requires the following institutions currently subject to CIP requirements to identify and verify beneficial owners of legal entity customers:

- Banks
- Broker-dealers in securities
- Mutual funds
- Futures commission merchants (FCMs) and introducing brokers (IBs) in commodities

For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts. For further guidance on beneficial owners, please refer to the Beneficial Owners section.

1613. How is the term "bearer share ownership" defined?

Bearer share ownership is based on physical possession of the stock certificates.

1614. Are there specific AML/CFT requirements for bearer shares?

Yes. Bearer shares are included within the definition of "monetary instruments" that must be included on Reports of International Transportation of Currency or Monetary Instruments (CMIRs). For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

1615. Are there specific AML/CFT requirements for shell companies?

Yes. Under Section 313 of the USA PATRIOT Act, U.S. financial institutions are prohibited from establishing accounts with foreign shell banks. There are no specific requirements with respect to other types of shell companies. For further guidance, please refer to Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks.

1616. Are the aforementioned high-risk business entities required to establish AML Programs pursuant to the USA PATRIOT Act?

Although not required to maintain an AML Program, these high-risk business entities operating in the United States are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. companies, all businesses are required to comply with Office of Foreign Assets Control (OFAC) laws and regulations. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1617. What is an example of a case involving shell companies and potential money laundering?

In April 2016, over 11.5 million documents (Panama Papers) from Mossack Fonseca (MF), a Panama-based law firm specialising in the formation and management of entities in tax havens, were leaked by an anonymous source, identifying the beneficial owners of 214,000 offshore entities, according to the International Consortium of Investigative Journalists (ICIJ). In September 2016, the same source that leaked the Panama Papers also leaked information from the Bahamas corporate registry, linking approximately 140 international and local politicians to offshore companies in the Bahamas. The ICIJ published the leaked information in its Offshore Leaks Database. According to media reports, in February 2017, the two founders of Mossack Fonseca were arrested for their alleged involvement in a separate money laundering investigation involving corruption in Latin America. These leaks had corruption, tax evasion and cybersecurity implications. For further guidance, please refer to the sections:

- Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act;
- Anti-Bribery and Corruption Compliance Programs; and
- Cyber Events and Cybersecurity.

1618. What guidance has been issued on high-risk business entities?

The following are examples of information and guidance that have been issued on high-risk business entities:

- **Business Entities (Domestic and Foreign) – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendations 24 – 25: Transparency and Beneficial Ownership of Legal Persons and Arrangements** (2012) by the Financial Action Task Force (FATF)
- **Potential Money Laundering Risks Related to Shell Companies** (2006) by the Financial Crimes Enforcement Network (FinCEN)

- **Standard on the Regulation of Trust and Corporate Service Providers** (2014) by the Group of International Finance Centre Supervisors (GIFCS)
- **Company Formations – Minimal Ownership Information Is Collected and Available** (2006) by the U.S. Government Accountability Office (GAO)
- **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** (2006) by FATF
- **Wolfsberg FAQs on Beneficial Ownership** (2012) by the Wolfsberg Group
- **Wolfsberg FAQs on Intermediaries** (2012) by the Wolfsberg Group
- **Shell Banks and Booking Offices** (2003) by the Basel Committee on Banking Supervision
- **Failure to Identify Company Owners Impedes Law Enforcement** by the United States Senate Permanent Subcommittee on Investigations (2006)
- **Tax Haven Abuses: The Enablers, the Tools and Secrecy** by the United States Senate Permanent Subcommittee on Investigations (2006)
- **Failure to Identify Company Owners Impedes Law Enforcement** by the United States Senate Permanent Subcommittee on Investigations (2006)
- **OFAC Regulations for the Corporate Registration Industry** (2004) by the Office of Foreign Assets Control (OFAC)

Know Your Customer's Activities: Product Considerations

Currency Transactions

1619. What do the terms "currency" and "cash" mean?

Currency and cash are defined differently for Currency Transaction Reports (CTR) and Form 8300 reporting requirements.

- For CTRs, "currency" means the coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money.
- For Form 8300 purposes, "currency" is defined as:
  - U.S. and foreign coin and currency received in any transaction
  - A cashier's check, money order, bank draft or traveller's check having a face amount of US$10,000 or less received in a designated reporting transaction, or received in any transaction in which the recipient knows that the instrument is being used in an attempt to avoid reporting requirements

For further guidance, please refer to the sections: Currency Transactions, Currency Transaction Reports and Form 8300.

1620. How much U.S. currency is in circulation?

According to the U.S. Federal Reserve, approximately US$1.5 trillion, of which US$1.47 trillion was in Federal Reserve notes as of February 2017. According to The Use and Counterfeiting of United States Currency Abroad (Part 3) (2006), more than half of all U.S. currency is held in emerging markets: 25 percent in Latin America, 20 percent in Africa and the Middle East and approximately 15 percent in Asia.

According to the Financial Action Task Force (FATF) Report: Money Laundering Through the Physical Transportation of Cash, between 46 percent and 82 percent of all transactions are conducted in cash in each country.

1621. What are the heightened money laundering and terrorist financing risks of currency transactions?

The vast majority of criminal dealings are conducted in cash. The inability to trace the origin or owner heightens the money laundering and terrorist financing risk of currency transactions. Currency transactions are typically used during the placement phase of money laundering.

1622. Are there specific AML/CFT requirements for currency transactions?

Yes. The following are required for large currency transactions:

- **Currency Transaction Reports (CTRs)**: CTRs are reports filed by certain types of financial institutions for cash currency transactions of more than US$10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge the transactions are by or on behalf of the same person and result in cash-in or cash-out totalling more than US$10,000 in any one business day. For additional guidance, please refer to the Currency Transaction Reports section.
- **Form 8300**: Form 8300 should be completed and submitted to the IRS if a person engaged in trade or business who, in the course of that trade or business, receives more than US$10,000 in single or multiple related transactions in:
  - Cash; or
  - Covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

For additional guidance, please refer to the Form 8300 section.

- **Report of International Transportation of Currency or Monetary Instruments (CMIR)**: The CMIR is required to be filed by:
  - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000 at one time from the United States to any

place outside of the United States or into the United States from any place outside of the United States; and

- Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding US$10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.

For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a **Suspicious Activity Report (SAR)**. For further guidance, please refer to the Suspicious Activity Reports section.

1623. How many of the SARs filed in a calendar year involve cash/currency?

Using 2016 as the frame of reference, of the 1.98 million SARs filed from January 1, 2016 through December 31, 2016, reports involving cash/currency totalled more than 744,000 (38 percent) and were distributed across financial institution types as follows:

- Depository institutions: 483,000 cases (65 percent)
- Money services businesses (MSBs): 232,000 cases (31 percent)
- Casinos and card clubs: 21,200 cases (3 percent)
- Other types of financial institutions: 7,200 cases (1 percent) (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily)
- Securities and futures firms: 711 cases (0.1 percent)
- Insurance companies: 113 cases (less than 0.1 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 27 cases (less than 0.1 percent)
- Housing GSEs: 2 cases (less than 0.1 percent)

1624. How can currency transactions be monitored for potentially suspicious activity?

Financial institutions should examine currency transactions for suspicious activity by monitoring for common red flags such as:

- Deposits of currency just below the reportable threshold conducted with multiple branches, tellers, accounts and/or on different days
- Deposits of currency by multiple individuals into the same account
- Deposits of currency wrapped in currency straps that have been stamped by other financial institutions
- Frequent exchanges of small dollar denominations for large dollar denominations

For additional guidance, please refer to the sections: Currency Red Flags, Bulk Shipments of Currency Red Flags, Branch and Vault Shipments Red Flags, and Safe Deposit Box Red Flags.

1625. What is counterfeiting? What is the scale of counterfeiting of U.S. currency?

The League of Nation's Currency Counterfeiting Convention (CCC) (1929) defines "currency counterfeiting" as "the fraudulent making or altering of currency, whatever means are employed." According to the Federal Reserve Working Paper "Estimating the Worldwide Volume of Counterfeit U.S. Currency: Data and Extrapolation" (2003), approximately one in 10,000 notes is counterfeit, both globally and within the United States.

1626. Why is there heightened focus on the counterfeiting of currency?

With advancements in printing technology, the counterfeiting of currency has become more accessible, particularly to transnational criminal organisations or organised crime as noted in the FATF report Money Laundering and Terrorist Financing Related to Counterfeiting of Currency (2013). The FATF report discusses how counterfeit currency is used to support drug trafficking operations, terrorism and to wage economic warfare on countries (e.g., injecting counterfeit currency to destabilise a country's currency).

1627. Who is responsible for enforcing anti-counterfeiting laws?

In 1865, the U.S. Secret Service was created to investigate and prevent counterfeiting of currency. The key U.S. anti-counterfeiting law is the Counterfeit Deterrence Act of 1992 (Title 18 U.S. Code Chapter 25: Counterfeiting and Forgery) which prohibits the making, dealing or possessing of counterfeit currency or equipment to make counterfeit currency. The law is not limited to currency but includes "any obligation or other security of the United States" (e.g., government checks, bonds).

1628. What is the International Convention for the Suppression of Counterfeiting Currency?

The International Convention for the Suppression of Counterfeiting Currency (CCC), a League of Nations treaty signed by the United States in 1929, is the primary treaty that criminalises the counterfeiting of currency. Although not ratified by the United States, the U.S. has enacted laws consistent with the CCC (e.g., criminalising the counterfeiting of currency).

1629. How do U.S. AML/CFT laws for currency and counterfeiting correspond to FATF Recommendations?

FATF Recommendation 3 – Money Laundering and Confiscation suggests including counterfeiting of currency as a predicate offense to money laundering.

FATF Recommendation 32 – Cash Couriers suggests implementing measures to detect the cross-border transportation of currency and monetary instruments (e.g., declaration or disclosure system).

For further guidance on FATF Recommendations, please refer to the Financial Action Task Force section.

1630. What guidance has been issued on cash, bulk shipping and/or smuggling of currency?

The following guidance has been issued on cash, the bulk shipping and/or smuggling of currency:

- **FATF Recommendation 32: Cash Couriers** (2012) by the Financial Action Task Force (FATF)
- **Bulk Cash Smuggling Center (BCSC)**, a centralised source for information and support for identifying, investigating and disrupting bulk cash smuggling activities around the world established by the U.S. Immigration and Customs Enforcement (ICE) agency. Resources include, but are not limited to, the following:
  - **FAQ: Bulk Cash Smuggling**
  - **United States of America-Mexico: Bi-National Criminal Proceeds Study** (2010)
  - **Operation Firewall**, established in 2005 by the U.S. Immigration and Customs Enforcement (ICE), an international partnership of law enforcement authorities targeting bulk cash smuggling operations of U.S. currency.
  - **International Currency Awareness Program** (**ICAP**), established in 1994 to learn how and why US currency is used overseas and to better determine the use and extent of counterfeiting overseas and to aid the international introduction of the new-design 1996-series $100 note.
- **Money Laundering Through the Physical Transportation of Cash** (2015) by the Financial Action Task Force (FATF) and the Middle East & North Africa Financial Action Task Force (MENATAF)
- **Why is Cash Still King? A Strategic Report on the Use of Cash by Criminal Groups as a Facilitator of Money Laundering** (2015) by Europol
- **Money Laundering and Terrorist Financing Related to Counterfeiting of Currency** (2013) by FATF
- **Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organised Crime** (2011) by the United Nations Office on Drugs and Crime (UNODC)
- **Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments** (2010) by FATF
- **FinCEN Advisory: Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML** (2014) by Financial Crimes Enforcement Network (FinCEN)
- **FinCEN Advisory: Supplement on U.S. Currency Restrictions on Banks in Mexico** (2013) by FinCEN
- **FinCEN Advisory: Update on U.S. Currency Restrictions in Mexico** (2012) by FinCEN

- **Information on Narcotics and Bulk Currency Corridors** (2011) by FinCEN
- **Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency** (2010) by FinCEN
- **Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the U.S.** (2006) by the FinCEN
- **United States of America-Mexico: Bi-National Criminal Proceeds Study** (2011) by the U.S. Department of Homeland Security (DHS)
- **The Use and Counterfeiting of U.S. Currency Abroad (Part I: 2000), (Part II: 2003), (Part III 2006)** by the U.S. Department of the Treasury
- **A Path to the Next Generation of U.S. Banknotes: Keeping Them Real** (2007) by the National Research Council, funded by the U.S. Department of the Treasury
- **Is That Real? Identification and Assessment of the Counterfeiting Threat for U.S. Banknotes** (2006) by the National Research Council, funded by the U.S. Department of the Treasury
- **Counterfeit Deterrent Features for the Next Generation Currency Design** (1993) by the National Research Council, funded by the U.S. Department of the Treasury

Bulk Shipments of Currency and Bulk Cash Smuggling

1631. What does the term "bulk shipment of currency" mean?

The FFIEC Manual defines a bulk shipment of currency as "the use of common, independent, or postal service air/land/sea carriers to transport large volumes of bank notes (U.S. or foreign) from sources either inside or outside the United States to a bank in the United States. Often, but not always, shipments take the form of containerised cargo."

Financial institutions can receive bulk shipments of currency, directly or indirectly through cash letter notifications. When received through cash letters, the currency is received by the Federal Reserve Bank, where it is recorded as held on the financial institution's behalf.

1632. What are the heightened money laundering and terrorist financing risks of bulk shipments of currency?

Bulk shipments of currency are considered a higher risk service because of the following:

- Complex transactions involving multiple parties that may disguise the source of currency
- Involvement of foreign financial institutions (FFIs) that may or may not be complicit in the laundering of illicit currency
- An increase in the use of bulk shipments of currency as a method for reintegrating currency into U.S. financial institutions as observed by U.S. law enforcement

1633. Who are common shippers of bulk currency?

Common shippers of bulk currency include:

- **Currency originators** are individuals and businesses, foreign or domestic, who generate currency from cash sales of commodities or other products or services (including monetary instruments or exchanges of currency).
- **Intermediaries** are other banks, central banks, nondeposit financial institutions or agents of these entities that ship currency gathered from their customers who are currency originators or other intermediaries.

1634. What does the term "bulk cash smuggling" mean?

Bulk cash smuggling is defined as the smuggling of or the attempt to smuggle more than US$10,000 in currency or monetary instruments into or out of the United States, with the specific intent to evade the U.S. currency-reporting requirements.

1635. What is the scale of bulk cash smuggling?

According to the U.S. Immigration and Customs Enforcement (ICE), more than 4,000 individuals were arrested and nearly US$770 million was seized through bulk cash smuggling investigations between 2003 and 2016.

1636. How much cash has been confiscated by the United States?

According to the Bulk Cash Smuggling Center (BCSC) within Immigration and Customs Enforcement (ICE), in 2016, nearly 600 individuals were arrested for attempting to smuggle currency and nearly US$66.3 million in bulk currency and monetary instruments was seized.

1637. What are some methods of smuggling cash?

Common methods of smuggling cash include, but are not limited to, the following:

- Transport in commercial, rental and private passenger vehicles
- Commercial airline shipments
- Passengers and pedestrians crossing U.S. borders with Mexico and Canada, also known as "*ruta* hormiga" or "ant route"
- Funnel accounts

Smuggled cash is often repatriated into the United States through the receipt of bulk currency shipments from foreign financial institutions (FFIs) that may or may not be complicit in the laundering of illicit currency.

1638. What is a funnel account?

Funnel accounts are used to transfer funds to a third party in a different jurisdiction, often in an area known for criminal activity. FinCEN defines a "funnel account" as "an individual or business account in

one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals." Methods of withdrawal can include the use of ATMs, monetary instruments and wire transfers.

Funnel accounts are often used as part of a trade-based money laundering (TBML) scheme such as the Black Market Peso Exchange (BMPE).

1639. What is the Black Market Peso Exchange (BMPE)?

Generally, the Black Market Peso Exchange (BMPE) is an intricate trade-based money laundering (TBML) system in which transnational criminal organisations (TCOs) (e.g., Colombian drug cartels) sell drug-related U.S.-based currency to money brokers (e.g., peso brokers) in a foreign country (e.g., Colombia) who, in turn, "exchange" the illicit U.S. currency for a foreign currency (e.g., Colombian pesos) through a series of transactions involving multiple financial institutions that support legitimate international trade between foreign importers and U.S. exporters.

For example, once Colombian drug cartels deliver drug-related U.S. currency to peso brokers (directly or indirectly through the use of couriers or other transportation operators), peso brokers then may do the following:

- Place the illicit currency into U.S. bank accounts by structuring or smurfing transactions to evade BSA reporting requirements; and
- Sell monetary instruments drawn on their U.S. bank accounts to Colombian importers who use them to purchase U.S. goods; or
- Pay for U.S. goods directly (e.g., by delivering the illicit currency directly to U.S. exporters) on behalf of Colombian importers with reimbursement upon delivery of the goods in Colombia; or
- Smuggle drug-related U.S. currency out of the country for deposit into foreign financial institutions (FFIs) for repatriation to the peso broker or directly to a U.S. exporter through various methods (e.g., wire transfers, bulk shipments of currency), often involving correspondent banking relationships and/or *casas de cambio*; and
- Pay the Colombian drug cartels in pesos, less a fee, thereby completing the "foreign exchange" transaction, and effectively laundering drug-related currency.

The BMPE not only allows drug cartels to launder funds, it also assists importers/exporters in evading trade controls and taxes. Peso brokers often fail to file required reports on reportable currency transactions and increasingly use new methods to launder illicit funds (e.g., funnel accounts, prepaid cards, mobile payments, digital currencies, internet gambling sites). Due to the complex nature of the transactions and the involvement of multiple third parties, BMPE activity is difficult to detect.

Although the BMPE in Colombia is one of the more widely known informal value transfer systems (IVTSs), BMPEs operate in other parts of the world, too (e.g., Mexico, Panama).

1640. What is an example of a BMPE case?

In September 2014, U.S. federal agencies conducted "Operation Fashion Police," a raid busting a multi-million dollar BMPE scheme based out of Los Angeles' fashion district. Approximately US$65 million in cash and bank accounts were seized. Officials posed as cash couriers to catch participating businesses attempting to launder proceeds from narcotics sales by the Sinaloa drug cartel through legitimate trade in garment and clothing products.

Per U.S. federal agencies, Operation Fashion Police is part of a larger effort to crackdown on Mexican organised crime rings.

1641. What steps can a financial institution take to mitigate the risk of bulk shipments of currency?

To mitigate the risk of bulk shipments of currency, financial institutions may consider adding these provisions to the signed contract with the shipping party:

- Each party's responsibilities
- Expectations about due diligence
- Circumstances under which the financial institution will not accept bulk currency shipments
- Permitted third-party usage of the shipper's services

1642. Should enhanced controls be applied only to foreign shipments of bulk currency?

No. There are varying degrees of risks associated with interstate shipments and shipments along international borders as well as foreign shipments of bulk currency. Appropriate controls should be applied to bulk shipments of currency, whether of domestic or foreign origin.

1643. What can a financial institution do to assess the risk posed by a relationship that intends to conduct bulk shipments of currency?

To assess the risk of bulk shipments of currency, financial institutions should conduct a risk assessment to identify relationships and transactions that present a higher risk of money laundering or terrorist financing. The factors used to assess the risk of bulk shipments of currency may include the following:

- Ownership
- Geographies
- Nature and source of currency
- Control of bulk currency

In addition to conducting a risk assessment, financial institutions should use the risk assessment to drive the collection of due diligence on relationships that intend to conduct bulk shipments of currency, and monitor shipments for unusual activity.

1644. What types of due diligence can be collected on relationships that intend to conduct bulk shipments of currency?

The following are examples of the types of due diligence that may be collected on relationships that intend to conduct bulk shipments of currency:

- Intended use of the relationship
- Expected volumes
- Sources of funds
- Reasonableness of volumes based on originators and shippers

In addition to collecting the due diligence above, financial institutions should consider periodic site visits to assess the legitimacy of the source of funds.

1645. Are financial institutions required to file Reports of International Transportation of Currency or Monetary Instruments (CMIRs) on shipments of bulk currency?

Yes. Any shipment of currency outside of the United States that is greater than US$10,000 must be reported via FinCEN Form 105, Report of International Transportation of Currency or Monetary Instruments (CMIR). For additional guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

1646. Can a financial institution assume that the source of funds of a cross-border movement of currency or monetary instruments is legitimate if a CMIR accompanies the transport?

No. CMIRs serve to document the cross-border physical transportation of currency and monetary instruments. They have no bearing on the legitimacy of the source of funds of the bulk shipment of currency.

1647. Are financial institutions required to file CMIRs on shipments of currency via the postal service or common carrier?

The BSA exempts the CMIR reporting requirement for financial institutions if currency or monetary instruments are shipped via the postal service or common carrier. However, currency or monetary instruments shipped across the border by other methods, including via air courier or the airlines, is not exempt.

For additional guidance on CMIR requirements, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

1648. Are financial institutions required to file Currency Transaction Reports (CTRs) for currency shipments?

Yes. For all receipts or disbursement of currency in excess of US$10,000, financial institutions are required to file a CTR. For additional guidance, please refer to the Currency Transaction Reports section.

1649. Does the filing of CMIRs obviate the financial institution's responsibility for filing CTRs or vice versa for the same shipment of currency?

No. The reporting requirements of CMIRs and CTRs are independent of each other. The financial institution may have to file one or both, depending on the amount and how the bulk currency was transported.

1650. Does the filing of CMIRs or CTRs obviate the financial institution's responsibility to monitor for potentially suspicious activity in its shipments of bulk currency?

No. A financial institution is still responsible for monitoring for potentially suspicious activity, regardless of whether a CMIR or CTR is filed.

1651. How can bulk shipments of currency be monitored for suspicious activity?

Financial institutions can monitor bulk cash shipments for suspicious activity by conducting a comparison of expected versus actual shipping volumes, monitoring for spikes in activity with foreign currency dealers or exchangers also known as *casas de cambio*, and monitoring for significant changes in branch and vault shipments.

Since cash smuggling often occurs along the same routes as criminal activity (e.g., narcotics and bulk currency corridors), an unusual or high volume of bulk shipments of currency can serve as a strong indicator of potentially suspicious activity (e.g., drug trafficking, human trafficking), especially along U.S. borders.

For additional guidance on indicators of potentially suspicious activity, please refer to the sections: Suspicious Activity Red Flags, Bulk Shipments of Currency Red Flags and Branch and Vault Shipments Red Flags.

1652. Are financial institutions obligated to do anything beyond filing a report (e.g., CTR, SAR) on bulk cash activity when warranted?

Financial institutions may consider contacting the National Bulk Cash Smuggling Center (BCSC) through their BCSC Tip Form or calling 1.866.DHS-2-ICE.

1653. What is a "narcotics and bulk currency corridor"?

Narcotics and bulk currency corridors are established distribution channels or logistical highways for the transportation of narcotics and the illicit proceeds from the sale of narcotics. Visual presentations and descriptions of these corridors have been detailed in the following:

- National Drug Threat Assessment (NDTA)
  - **Appendix A (2010)** – Presents multiple maps with distribution channels by select drug trafficking organisations (DTOs) (e.g., Asian, Colombian, Cuban, Dominican, Mexican), by involvement of street gangs, and by drug threat (e.g., cocaine, heroin, methamphetamines, marijuana, prescription drugs);

- **Drug Transportation Corridors** (2006) – Describes drug transportation corridors within the United States by drug and by originating/destination cities.

1654. Are narcotics and bulk currency corridors the same as High Intensity Drug Trafficking Areas (HIDTAs)?

Narcotics and bulk currency corridors may or may not be located in High Intensity Drug Trafficking Areas (HIDTAs). HIDTAs were authorised in the Anti-Drug Abuse Act of 1988 to assist law enforcement with concentrating its efforts with drug control at the federal, state and local levels. HIDTAs are designated by area. Since the original designation of five HIDTAs in 1990, the program has expanded to 28 areas of the country.

For further guidance on high-risk geographies, please refer to the Geographic Risk Assessment section.

Restrictions on U.S. Currency Transactions with Mexican Financial Institutions

1655. How much cash is smuggled into Mexico from the United States?

According to the United States of America-Mexico: Bi-National Criminal Proceeds Study, published in 2010, between US$19 and US$29 billion in U.S. currency is smuggled into Mexico annually, of which between 25 percent and 50 percent was actually placed into the traditional financial system by the TCO. TCOs more often stored bulk cash in "stash houses."

1656. What types of restrictions has Mexico imposed on U.S. currency transactions at Mexican financial institutions?

In 2010, Mexico's finance ministry, Secretaría de Hacienda y Crédito Público (SHCP), imposed restrictions (e.g., prohibitions, daily/monthly limits) on U.S. currency transactions (e.g., currency exchanges, remittances, payments for services) at Mexican financial institutions (e.g., banks, exchange houses [*casas de cambio*], brokerage firms [*casas de bolsa*]) based on the following factors:

- Type of person (e.g., individual, legal entity)
- Location of business (e.g., within 20 miles of the U.S./Mexico border)
- Nationality (e.g., Mexican national, foreign tourist)
- Relationship with the financial institution (e.g., noncustomer)

For example, U.S. currency transactions with legal entities are prohibited for customers and noncustomers. An exception is made for legal entity customers operating in a tourist area, within twenty miles of the U.S. border or within the States of Baja California or South Baja California, in which case U.S. currency transactions up to US$14,000 in aggregate per month are permitted.

For individuals who are customers, U.S. currency transactions are limited to US$4,000 in aggregate per month. For noncustomers who are Mexican nationals, a daily limit of US$300 applies. For noncustomers who are foreign nationals (e.g., non-Mexican), in addition to the US$300 daily limit, a monthly limit of US$1,500 also applies. For all noncustomers, Mexican financial institutions are required to obtain identification.

The regulations also require covered Mexican financial institutions to submit quarterly reports on U.S. currency transactions to the Comisión Nacional Bancaria y de Valores (CNBV), Mexico's financial regulator. Some Mexican financial institutions have opted to implement additional measures such as prohibiting U.S. currency transactions at specific branches and requesting information on the source of funds.

For further details and updates on the Mexican regulation, please refer to the SHCP's website athttp://www.gob.mx/shcp/en.

1657. Are there any exceptions to the Mexican restrictions on U.S. currency transactions?

Yes. In 2014, the SHCP amended the 2010 regulations, lifting the US$14,000 monthly limit for businesses that meet the following criteria:

- Have been established for at least three years;
- Allow authorities to monitor their financial transactions; and
- Can prove their need to make deposits greater than US$14,000 per month to operate.

1658. What have been the reactions to this recent change to the Mexican restrictions on U.S. currency transactions?

While the Mexican business community welcomes the rollback of the regulation, U.S. officials have concerns that the anticipated increase in U.S. currency transactions will make it more difficult to detect illegal movements of funds.

1659. What is "MX Restriction" and when should financial institutions include this phrase in their SARs?

Financial institutions should include the phrase "MX Restriction" within the narrative of SARs when reporting suspicious transactions that include activities that may have been altered due to Mexico's regulation restricting U.S. currency transactions in Mexican financial institutions.

The "MX Restriction" phrase enables FinCEN to identify changes in money laundering methodologies by reporting on trends identified in SAR filings. Since the regulatory changes in Mexico, bulk cash smuggling has decreased and shifted to other methods to transfer funds (e.g., use of funnel accounts to move illicit proceeds).

1660. Have the Mexican regulations impacted currency flows between the U.S. and Mexico?

Yes. Since 2010, FinCEN has periodically released advisories detailing how Mexican regulations restricting U.S. currency in Mexican financial institutions have impacted currency flows and methods to move funds, both illicit and legitimate.

According to the CNBV, Mexico's financial regulator, Mexican banks' exports of U.S. currency dropped from a quarterly average of US$2.7 billion in 2009, to US$990 million in 2012, a 63 percent reduction.

Alternative methods to moving funds include, but are not limited to, the following:

- Increase in currency deposits at U.S. financial institutions followed by international wire transfers
- International wire transfers initiated by *casas de cambio*
- Use of funnel accounts
- Diversion through financial institutions with higher dollar thresholds than Mexican financial institutions or through financial institutions in intermediary jurisdictions
- Use of TBML schemes such as the BMPE

1661. What measures has the United States taken to combat bulk cash smuggling and associated criminal activity across the U.S./Mexico border?

Begun in 2008, the Merida Initiative is a partnership between the United States and Mexico to combat organised crime. Activities under the Merida Initiative include, but are not limited to, the following:

- Training of Mexican personnel (e.g., police, investigators, prosecutors, defence counsel) in support of justice sector reforms;
- Establishment of anti-corruption and whistleblowing programs;
- Delivery of equipment and trained canines to detect illicit goods at checkpoints and ports of entry;
- Establishment of cross-border telecommunications systems between U.S. and Mexico sister cities;
- Support for Mexican prisons to achieve independent accreditation from the American Correctional Association (ACA); and
- Establishment of Drug Treatment Courts across multiple Mexican states as an alternative to incarceration for drug abusers.

In August 2014, FinCEN issued a Geographic Targeting Order (GTO) that requires enhanced cash reporting by common carriers of currency (e.g., armoured car services) in the land border between San Diego County, California, United States and the United Mexican States at the San Ysidro and Otay Mesa Ports of Entry and Departure. The GTO outlines special reporting, recordkeeping, and customer identification obligations of common carriers of currency.

In October 2014, FinCEN issued a subsequent GTO requiring even more business types (e.g., garment and textile stores, transportation companies, travel agencies, perfume stores, electronic stores, shoe stores, lingerie stores, flower/silk flower stores, beauty supply stores, stores with "import" or "export" in their names) to report cash transactions greater than or equal to US$3,000. Nearly every business located in the "fashion district" of Los Angeles was impacted.

Funds Transfers

1662. How are "funds transfers" and "transmittal of funds" defined? What is the difference?

The term "funds transfer," which includes wire transfers, is used to describe the following series of transactions as executed by banks. The BSA defines "funds transfers" as:

- The "series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. The term includes any payment order issued by the originator's bank or an intermediary bank intended to carry out the originator's payment order.
- A funds transfer is completed by acceptance by the beneficiary's bank of a payment order for the benefit of the beneficiary of the originator's payment order."

The term "transmittal of funds" is used to describe the following series of transactions as executed by NBFIs. The BSA defines "transmittals of funds" as:

- The "series of transactions beginning with the transmittor's transmittal order, made for the purpose of making payment to the recipient of the order. The term includes any transmittal order issued by the transmittor's financial institution or an intermediary financial institution intended to carry out the transmittor's transmittal order.
- A transmittal of funds is completed by acceptance by the recipient's financial institution of a transmittal order for the benefit of the recipient of the transmittor's transmittal order."

Other than the executing parties, there is no difference between the terms "funds transfers" and "transmittal of funds."

1663. Are there any exemptions from the definition of "funds transfer" or "transmittal of funds"?

Yes. The following transactions are exempt from the definition of "funds transfer" and "transmittal of funds":

- Electronic fund transfers (EFTs) defined in Section 903(7) of the Electronic Funds Transfer Act of 1978 (EFTA) (as amended) as "any transfer of funds, other than a transaction originated by check, draft, or similar paper instrument, which is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorise a financial institution to debit or credit an account."
- Any other funds transfers that are made through an automated clearing house (ACH), an automated teller machine (ATM), or a point-of-sale (POS) system.

For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.

1664. What are the heightened money laundering and terrorist financing risks of funds transfers?

Wire transactions can move funds quickly and internationally, and in some instances, with limited transparency (e.g., online, remote access, cover payments). Funds transfers typically are used during the layering and integration phases of money laundering.

1665. Are there specific AML/CFT requirements for funds transfers?

Yes. The following are required for funds transfers:

- **Funds Transfer Recordkeeping Requirement**: The basic requirements of the Funds Transfer Recordkeeping Requirement vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution, beneficiary institution). For each funds transfer of US$3,000 or more, the originating institution is required to obtain and retain information including, but not limited to, the name and address of the originator, the amount of the payment order, the execution date of the payment order, and the name and address of the beneficiary.
- **Travel Rule**: The Travel Rule refers to the requirement for financial institutions that participate in funds transfers of US$3,000 or more to pass along certain information about the funds transfer to the next financial institution involved in the funds transmittal. The requirements of the Travel Rule vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution). For additional guidance, please refer to the Funds Transfer Recordkeeping Requirement and Travel Rule section.
- **Office of Foreign Assets Control (OFAC) Sanctions Screening**: All U.S. financial institutions are required to screen transactions, including funds transfers, for possible OFAC Sanctions violations. For additional guidance, please refer to the sections Office of Foreign Assets Control and International Sanctions Programs and Blocking and Rejecting Transactions.

In instances where potentially suspicious activity is detected, a financial institution may need to file a Suspicious Activity Report (SAR). For further guidance, please refer to the Suspicious Activity Reports section.

Additionally, in 2010, FinCEN issued a proposed rule that would impose additional reporting requirements of transmittal orders associated with "cross-border electronic transmittals of funds" (CBETFs). For further guidance, please refer to the Cross-Border Electronic Transmittal of Funds section.

1666. Does the CFPB's Remittance Transfer Rule impose additional AML/CFT-related requirements on funds transfers?

No. Pursuant to Section 1073 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the CFPB's Remittance Transfer Rule, which amends the Electronic Funds Transfer Act of 1978 (EFTA) implemented under Regulation E, is intended to protect consumers who send money electronically to foreign countries by providing more information about the costs of remittances. The rules apply to most international remittances regardless of their purpose, including, but not limited to funds transfers and automated clearing house (ACH) transactions. Specifically, they would require the following:

- Disclosures in English, including:
    - A prepayment disclosure at the time the person initiates that lists the following:

        - The exchange rate;
        - Fees and taxes collected by the companies;
        - Fees charged by the companies' agents abroad and intermediary institutions;
        - The amount of money expected to be delivered abroad, not including certain fees to be charged to the recipient or foreign taxes; and
        - If appropriate, a disclaimer that additional fees and foreign taxes may apply.
    - A receipt disclosure that must be provided to the sender once the payment has been made.

- A provision that consumers can cancel a transfer within 30 minutes (and sometimes more) of originating it;
- Provisions that companies must investigate problems consumers report about transfers and provide standards for error resolutions (e.g., refund, resending of transfer free of charge);
- That companies are made responsible for mistakes made by certain people who work for them; and
- Provisions relating to transfers pre-scheduled on a regular basis.

The rule is applicable to banks, thrifts, credit unions, money transmitters and broker-dealers that consistently execute 100 or more remittance transfers per calendar year and applies to remittance transfers that are more than US$15, made by a consumer in the United States, and sent to a person or company in a foreign country.

The Remittance Transfer Rule became effective October 28, 2013. The CFPB has provided model forms as well as an International Funds Transfer Small Entity Compliance Guide; these and other information related to the rules can be found on the CFPB's website at https://www.consumerfinance.gov/policy-compliance.

1667. How can funds transfers be monitored for potentially suspicious activity?

Financial institutions should examine funds transfers for suspicious activity by monitoring for common red flags such as:

- Frequent, large, round dollar wire transactions
- A large deposit followed by numerous, smaller wire transactions
- Several deposits, particularly in currency or monetary instruments, followed by international wire transactions
- Wire transfers to and from bank secrecy haven countries and countries known for or linked to terrorist activities, drug trafficking, illegal arms sales or other illegal activity
- Unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity

For additional guidance, please refer to the Wire Transfer Red Flags section.

1668. How many of the SARs filed in a calendar year involve funds transfers?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports involving funds transfers totalled nearly 736,000 (37 percent) and were distributed across financial institution types as follows:

- Depository institutions: 215,000 cases (29 percent)
- Money services businesses (MSBs): 496,000 cases (67 percent)
- Other types of financial institutions: 112 cases (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily)
- Securities and futures firms: 7,900 cases (1 percent)
- Casinos and card clubs: 1,100 cases (0.2 percent)
- Insurance companies: 441 cases (0.1 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 74 cases (0.1 percent)
- Housing GSEs: 13 cases (less than 0.01 percent)

1669. What guidance has been issued on funds transfers?

The following are examples of key guidance that has been issued on funds transfers:

- **Funds Transfers Recordkeeping — Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 16: Wire Transfers** (2012) by the Financial Action Task Force (FATF)
- **Final Rule: Amendment to the Bank Secrecy Act Regulations - Definitions of Transmittal of Funds and Funds Transfer Final Rule** (2013) by FinCEN
- **Notice of Proposed Rulemaking: Definitions of Transmittal of Funds and Funds Transfer** (2012) by FinCEN
- **Making Remittances Work: Balancing Financial Integrity and Inclusion** (2014) by the World Bank (WB).
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments Messages** (2009) by Wolfsberg
- **Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management** (2009) by the World Bank

- **Bilateral Remittance Corridor Analysis (BRCA)** (2007) by the World Bank
- **Regulatory Frameworks for Hawalas and Other Remittance Systems** (2005) by the International Monetary Fund (IMF)
- **Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act** (2010) by FinCEN
- **Implications and Benefits of Cross-Border Funds Transmittal Reporting** (2010) by FinCEN
- **Fact Sheet: Cross-Border Electronic Transmittal of Funds** (2010) by FinCEN
- **Funds "Travel" Regulations: Questions and Answers (Background Information and Notes)** (2010) by FinCEN

Monetary Instruments

1670. What does the term "monetary instrument" mean?

The definition of monetary instruments varies based on the specific AML/CFT requirement. For example, for the Report of International Transportation of Currency or Monetary Instruments (CMIR), monetary instruments are defined as:

- Coin or currency of the United States or of any other country;
- Traveller's checks in any form;
- Negotiable instruments (e.g., checks, promissory notes, money orders) in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery;
- Incomplete instruments (including checks, promissory notes, and money orders) that are signed but on which the name of the payee has been omitted; and
- Securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery.

For CMIRs, monetary instruments do not include:

- Checks or money orders made payable to the order of a named person which have not been endorsed or which bear restrictive endorsements;
- Warehouse receipts; or
- Bills of lading.

For the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, monetary instruments include:

- Bank check or draft
- Foreign draft

- Cashier's check
- Money order
- Traveller's check

For further guidance on the AML/CFT requirements for monetary instruments, please refer to the following sections: Report of International Transportation of Currency or Monetary Instruments and Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments.

1671. Have changes to the definition of "monetary instruments" been proposed?

Yes. In October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on Reports of International Transportation of Currency or Monetary Instruments (CMIRs). No final rule on this proposed change has yet been issued. Section 13 of the proposed bill Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017, introduced by the U.S. Senate in May 2017, proposed amending the definition of monetary instrument to include funds stored in a digital format (e.g., prepaid access devices, virtual currency). Whether this bill will ever be passed into law is unclear.

1672. How are "monetary instruments" defined by FATF?

FATF uses the term "bearer negotiable instruments (BNI)" to describe monetary instruments. BNIs are defined as "monetary instruments in bearer form such as: traveller's checks; negotiable instruments (including checks, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including checks, promissory notes and money orders) signed, but with the payee's name omitted."

For further guidance on international standards, please refer to the Financial Action Task Force section.

1673. What are the heightened money laundering and terrorist financing risks of monetary instruments?

Similar to cash, the inability to trace the origin or owner heightens the money laundering and terrorist financing risk of monetary instruments. Monetary instruments are typically used during the layering phase of money laundering (e.g., transfers between bank accounts of related entities or charities for no apparent reason).

1674. What are the specific AML/CFT requirements for monetary instruments?

The following is required for monetary instruments:

- **Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments**: A financial institution that issues or sells for currency a monetary instrument (e.g., bank check or draft, foreign draft, cashier's check, money order, traveller's check) for amounts between US$3,000 and US$10,000 inclusive must first obtain specific information if the individual has a

deposit account at the institution (e.g., name of the purchaser, date of purchase, type of instrument purchased, amount, serial numbers). For additional guidance, please refer to the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments section.

- **Form 8300**: Form 8300 should be completed and then submitted to the IRS if a person engaged in trade or business who, in the course of that trade or business, receives more than US$10,000 in single or multiple related transactions in:
  - Cash, or
  - Covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction.

  For additional guidance, please refer to the Form 8300 section.
- **Report of International Transportation of Currency or Monetary Instruments (CMIR)**: The CMIR is required to be filed by:
  - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
  - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding US$10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.
  - In October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on CMIRs; no final rule on this proposed change has yet been issued. For further guidance on CMIRs and prepaid access, please refer to the sections Report of International Transportation of Currency or Monetary Instruments and Prepaid Access and Stored Value.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a **Suspicious Activity Report (SAR)**. For further guidance, please refer to the Suspicious Activity Reports section.

1675. How can monetary instruments be monitored for potentially suspicious activity?

Financial institutions should examine monetary instruments for suspicious activity by monitoring for common red flags such as:

- Monetary instruments purchased on the same or consecutive days at different locations, and/or are numbered consecutively in amounts designed to evade reporting requirements (i.e., under US$3,000 or US$10,000), or are purchased in round amounts
- Blank payee lines

- Instruments which contain the same stamp symbol or initials

For additional guidance, please refer to the Monetary Instrument Red Flags section.

1676. How many of the SARs filed in a calendar year involved monetary instruments (e.g., money orders, traveller's checks, cashier's checks)?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports involving monetary instruments (e.g., bank/cashier's check, money orders, travellers check) totalled over 315,000 (16 percent) and were distributed across financial institution types as follows:

- Money services businesses (MSBs): 230,000 cases (73 percent)
- Depository institutions: 79,000 cases (25 percent)
- Other types of financial institutions (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily): 3,300 cases (1 percent)
- Securities and futures firms: 760 cases (0.2 percent)
- Casinos and card clubs: 700 cases (0.2 percent)
- Insurance companies: 1,000 cases (0.3 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 100 cases (less than 0.1 percent)
- Housing GSEs: 9 cases (less than 0.1 percent)

1677. What guidance has been issued on monetary instruments?

The following key guidance has been issued on monetary instruments:

- **Purchase and Sale of Monetary Instruments Recordkeeping – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 32: Cash Couriers** (2012) by the Financial Action Task Force (FATF)
- **Notice of Proposed Rulemaking: Bank Secrecy Act Regulations: Definition of "Monetary Instrument"** (2011) by FinCEN (related to Prepaid Access devices)
- **Guidance – International Best Practices: Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments** (2012) by FATF

Payable-Through Accounts

1678. What does the term "payable-through account" (PTA) mean?

A PTA, also known as a "pass-through" or "pass-by" account, is an account maintained for a respondent that permits the respondent's customers to engage, either directly or through a subaccount, in banking activities (e.g., check writing, making deposits) usually in the United States.

1679. What are the heightened money laundering and terrorist financing risks of PTAs?

PTAs do provide legitimate business benefits, but the operational aspects of the accounts make them particularly vulnerable to abuse as a mechanism to launder money. Multiple individuals can have signatory authority over a single correspondent account and can, therefore, conduct transactions with limited transparency. Often, PTA arrangements are customers in less-regulated financial markets. Unless a financial institution is able to identify adequately and understand the transactions of the ultimate users of the respondent's bank account, there is significant potential risk for money laundering and terrorist financing.

1680. What is the difference between PTAs and traditional correspondent clearing?

In traditional correspondent clearing, customers do not have the authority to transact through the respondent's account on their own. In order to send or receive funds through the respondent's account, the customer must send instructions to the respondent so that the respondent can transact on behalf of the customer. In other words, with PTAs, customers of the respondent have direct access to the account.

1681. What steps can a financial institution take to mitigate the risk associated with PTAs?

To mitigate the risk of PTAs, financial institutions may consider adding the following provisions to the signed contract with the respondent financial institution:

- Roles and responsibilities of each party
- Limits or restrictions on transaction types and amounts (e.g., currency deposits, funds transfers, check cashing)
- Restrictions on types of subaccount holders (e.g., *casas de cambio*, finance companies, funds remitters or other nonbank financial institutions)
- Prohibitions or restrictions on multi-tier subaccount holders
- Access to the foreign financial institution's internal documents and audits that pertain to its PTA activity
- Requirement to obtain the same account opening information from subaccount holders as required by the PTA holding institution for its own direct customers and to make this information available as needed

In addition to conducting a risk assessment, financial institutions should collect due diligence on respondents that intend to conduct PTA activity and monitor transactions for unusual activity.

1682. What are some examples of due diligence that should be collected on foreign financial institution respondents that intend to conduct PTA transactions?

PTAs are one of many foreign correspondent banking services used by foreign financial institutions, also known as foreign respondents. Due to the risks associated with foreign correspondent banking, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act outlines the following sample due diligence and enhanced due diligence that should be conducted on these high-risk relationships:

- Obtain and consider information related to the respondent's AML/CFT Compliance Program
- Conduct enhanced monitoring of transactions to and from the account
- Obtain and consider information about the identity of any person with authority to direct transactions through the PTA account
- Obtain and consider information on the identity of each owner of the respondent

For further guidance on the due diligence that should be conducted on foreign respondents, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.

1683. Are there specific AML/CFT requirements for PTAs?

Yes. Financial institutions may be required to comply with the following:

- Under **Section 311**, the Fifth Measure restricts or prohibits the provision of correspondent banking and PTA services to financial institutions designated as a money laundering concern. For further guidance, please refer to the Section 311 – Special Measures section.
- **Section 312** outlines specific due diligence and enhanced due diligence required to be conducted by financial institutions that have correspondent banking customers. For further guidance, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.
- **Section 313** prohibits U.S. financial institutions from establishing correspondent banking relationships with foreign shell banks. For further guidance, please refer to Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks.
- **Section 319** outlines circumstances in which funds can be seized from a U.S. interbank account; requirements to retrieve bank records of foreign respondents within "120 hours"; and "foreign bank certification" requirements of foreign respondents (e.g., certifies physical presence, regulated status, prohibition of indirect use of correspondent accounts by foreign shell banks). For further guidance, please refer to Section 319 – Forfeiture of Funds in U.S. Interbank Accounts.
- Although regulations have not been issued, **Section 325** outlines restrictions on the use of concentration accounts to prevent abuse similar to that conducted through correspondent banking accounts. For further guidance, please refer to Section 325 – Concentration Accounts at Financial Institutions.

- Some **OFAC sanctions** restrict or prohibit the provision of correspondent banking and PTA services to designated entities (e.g. Iranian-linked financial institutions, financial institutions providing services to Specially Designated Nationals [SDNs]). For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

Concentration Accounts

1684. What does the term "concentration account" mean?

Within the industry, a concentration account is an account that a financial institution uses to aggregate funds from different customers' accounts. Concentration accounts are also known as collection, intraday, omnibus, settlement, special-use or sweep accounts.

1685. What is the heightened money laundering and terrorist financing risk of concentration accounts?

Concentration accounts involve the commingling of different customers' funds. They also can involve the commingling of customer funds with a financial institution's funds in a way that conceals the identity of underlying parties to a transaction.

1686. How should concentration accounts be monitored for potentially suspicious activity?

Financial institutions should examine concentration accounts for suspicious activity by identifying and monitoring common red flags such as:

- Cash transactions for Currency Transaction Report (CTR) aggregation and filing purposes
- Employee access and use of concentration accounts
- Funds sent directly to a concentration account
- Exception reports for transactions processed in violation of the financial institution's policy

1687. Are there specific AML/CFT requirements for concentration accounts?

Under Section 325 – Concentration Accounts at Financial Institutions, the USA PATRIOT Act introduces the possibility of future regulation relating to concentration accounts; however, the U.S. Department of the Treasury has not issued regulations. Financial institutions are advised to recognise and take appropriate actions to control the risks of these accounts by:

- Prohibiting financial institutions from allowing customers to direct transactions through a concentration account
- Prohibiting financial institutions and their employees from informing customers of the existence of the institution's concentration accounts
- Establishing written procedures governing documentation of transactions involving concentration accounts (e.g., capturing customer transactions in the customer's account statements, retaining appropriate transaction and customer identifying information)

- Establishing controls over the opening, maintenance and reconcilement of concentration accounts
- Subjecting concentration accounts to suspicious activity monitoring

Pouch Activity

1688. What does the term "pouch activity" mean?

Pouch activity, also known as "pouch services" or "cash letters," is the use of a courier to transport currency, monetary instruments, loan payments and other financial documents from outside the United States to a U.S. financial institution. Pouches can be sent by another financial institution or by an individual and are commonly offered in conjunction with correspondent banking services.

1689. What does the term "cash letter" mean?

A cash letter, also known as a transit letter, is a group of negotiable items (e.g., checks, drafts) accompanied with documentation that lists the number of items, total dollar amount, and instructions for transmittal to a clearinghouse, a correspondent bank or a Federal Reserve Bank.

1690. What are the heightened money laundering and terrorist financing risks of pouch activity?

Financial institutions often do not have any information on underlying clients and transactions within a pouch, as their account relationship is with the foreign financial institution (FFI), also referred to as the foreign respondent, utilising the pouch services. As such, financial institutions must rely on foreign respondents to conduct appropriate due diligence to mitigate risks of doing illicit business. The commingling of multiple client funds in the pouch may make it difficult for a financial institution to understand the source and purpose of incoming and outgoing funds.

The increased risk of pouch activities is also attributed to a high volume of international transactions, high-risk products (e.g., money orders, traveller's checks and bank checks) and opportunities for layering (e.g., depositing of monetary instruments followed by funds transfers out in the same amount).

1691. What steps can a financial institution take to mitigate the risk of pouch activity?

To mitigate the risk of pouch activity, U.S. financial institutions should ensure they have the following in place:

- Documented procedures for approving and exiting pouch relationships
- A signed contract with the foreign financial institution that includes roles and responsibilities of each party
- Documented criteria for unacceptable transactions (e.g., monetary instruments with blank payee lines, unsigned monetary instruments and a large number of consecutively numbered monetary instruments)
- Procedures for processing the pouch and reviewing contents for suspicious activity

1692. What type of due diligence can be collected on foreign financial institution relationships that intend to utilise pouch services?

Pouch services are one of many foreign correspondent banking services used by foreign financial institutions, also known as foreign respondents. Due to the risks associated with foreign correspondent banking, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act outlines the following sample due diligence and enhanced due diligence that should be conducted on these high-risk relationships:

- Determine whether the account is subject to enhanced due diligence requirements under Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act.
- Assess the money laundering and terrorist financing risk posed, based on a consideration of relevant risk factors such as:
    - The nature of, and markets served by, the foreign respondent's business.
    - The type, purpose and anticipated activity of the foreign respondent's account.
    - The nature and duration of the relationship with the foreign respondent (and any of its affiliates)
    - The AML/CFT and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent.
    - The AML/CFT and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available).
    - Information known or reasonably available about the foreign respondent's AML/CFT record.
- Apply risk-based policies, procedures and controls to each such respondent reasonably designed to detect and report known or suspected money laundering or terrorist financing activity. Controls should include a periodic review of the respondent's account activity to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

For additional guidance on due diligence for foreign correspondent banking customers, please see sections: Due Diligence for Correspondent Accounts, Enhanced Due Diligence for Correspondent Accounts.

1693. How can pouch activity be monitored for potentially suspicious activity?

Financial institutions should examine pouch activity for suspicious activity by monitoring for common red flags such as:

- Monetary instruments purchased on the same or consecutive days at different locations, and/or are numbered consecutively in amounts designed to evade reporting requirements (i.e., under US$3,000 or US$10,000) or are purchased in round amounts

- Blank payee lines
- Instruments that contain the same stamp symbol or initials

For additional guidance, please see section: Suspicious Activity Red Flags.

1694. Are there specific AML/CFT requirements for pouch activities?

Yes. The content of pouches may be subject to the following reporting requirements:

- **Currency Transaction Reports (CTRs)**: CTRs are reports filed by certain types of financial institutions for cash currency transactions of more than US$10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge that they are by or on behalf of the same person and result in cash-in or cash-out totalling more than US$10,000 in any one business day. For additional guidance, please refer to the Currency Transaction Reports section.
- **Report of International Transportation of Currency or Monetary Instruments (CMIR)**: The CMIR is required to be filed by:
  - Each person who physically transports, mails or ships, or causes to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States; and
  - Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding US$10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States.

  For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Additionally, in instances where potentially suspicious activity is detected, a financial institution may need to file a **Suspicious Activity Report (SAR)**. For further guidance, please refer to the Suspicious Activity Reports section.

U.S. Dollar Drafts

1695. What is a U.S. dollar draft?

A U.S. dollar draft is a bank draft or check denominated in U.S. dollars, which is offered by foreign financial institutions (FFIs) and drawn on a U.S. correspondent account of the FFI.

1696. What are the heightened money laundering and terrorist financing risks of U.S. dollar drafts?

U.S. dollar drafts are considered higher risk because, historically, they have been susceptible to abuse by money launderers, particularly in the layering and integration phases. For example, criminals are able to convert smuggled cash into a U.S. dollar draft purchased at a foreign financial institution in

order to integrate the funds back into the U.S. financial system. Due to the limited information available about the parties involved, U.S. dollar drafts also pose heightened sanctions risk, especially if the FFI does not perform sanctions screening.

1697. What is an example of how U.S. dollar drafts can be used to launder money?

FinCEN, for instance, has long cautioned about schemes to launder smuggled currency from drug trafficking and other criminal activities back into the United States from Mexico through the purchase of a "Mexican bank draft" – a U.S. dollar denominated draft drawn on a Mexican bank's U.S. correspondent. The draft may be carried into the United States and negotiated or endorsed to a third party who negotiates the draft at the U.S. correspondent institution or uses the money to buy goods that are ultimately converted into cash. In all scenarios, the draft eventually finds its way back to the U.S. bank on which it was drawn.

1698. What steps can a financial institution take to mitigate the risk associated with its foreign financial institutions providing U.S. dollar drafts?

U.S. dollar drafts are one of many foreign correspondent banking services used by FFIs, also known as foreign respondents. Due to the risks associated with foreign correspondent banking, Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act outlines the following simple due diligence and enhanced due diligence that should be conducted on these high-risk relationships:

- Determine whether a correspondent account, because it allows U.S. dollar drafts or other high-risk products/services, is subject to enhanced due diligence requirements under Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts of the USA PATRIOT Act.
- Assess the money laundering and terrorist financing risk posed, based on a consideration of relevant risk factors such as:
    - The nature of, and markets served by, the foreign respondent's business.
    - The type, purpose and anticipated activity of the foreign respondent's account.
    - The nature and duration of the relationship with the foreign respondent (and any of its affiliates).
    - The AML/CFT and supervisory regime of the jurisdiction that issued the charter or license to the foreign respondent.
    - The AML/CFT and supervisory regime of the jurisdiction in which any company that is an owner of the foreign respondent is incorporated or chartered (if reasonably available).
    - Information known or reasonably available about the foreign respondent's AML/CFT record.

- Apply risk-based policies, procedures and controls to each such respondent reasonably designed to detect and report known or suspected money laundering or terrorist financing activity. Controls should include a periodic review of the respondent's account activity to determine consistency with information obtained about the type, purpose and anticipated activity of the account.

For additional guidance on due diligence for foreign correspondent banking customers, please see sections: Due Diligence for Correspondent Accounts, Enhanced Due Diligence for Correspondent Accounts.

1699. How should U.S. dollar drafts be monitored for potentially suspicious activity?

Financial institutions should examine accounts with U.S. dollar draft activity for suspicious activity by monitoring for common red flags such as:

- Significant variance in expected/historical activity versus actual activity in terms of the volume of U.S. dollar draft activity
- Dollar amounts that appear to be designed to evade reporting requirements (i.e., under US$3,000 or US$10,000) or are purchased in round amounts
- Multiple, sequentially numbered U.S. dollar drafts
- High volume of U.S. dollar drafts to the same payee or from the same remitter
- Drafts issued by *casas de cambio*
- Third-party endorsed drafts

In addition, financial institutions should obtain and consider information related to the respondent's AML/CFT Compliance Program and conduct enhanced monitoring of transactions to and from the account.

For additional guidance on red flags for potentially suspicious activity, please refer to the Suspicious Activity Red Flags section.

Trade Finance Activities

1700. What does the term "trade finance" mean?

The term "trade finance" generally refers to the use of short-term financing to facilitate the import and export of goods. Such arrangements can involve payment if documentary requirements are met, such as through the use of a letter of credit, or through a commitment to make payment in the event the original party with the obligations defaults on the terms of the transaction (e.g., through use of a guarantee or a standby letter of credit). In such cases the bank's involvement in the finance activities helps to minimise risk of payment to importers and exporters.

Banks often participate in trade financing by providing pre-export financing, assisting the process of collection, confirming or issuing letters of credit, discounting drafts and acceptances, or offering fee-based services such as providing credit and country information on the buyers. Most trade financing is

short term and self-liquidating; however, medium-term loans of one to five years, or even longer-term loans, may be used to finance the import and export of capital goods such as machinery or equipment.

The Financial Action Task Force (FATF) defines trade finance to include nondocumentary trade activities (e.g., management of open account trading), whereas the Wolfsberg Group's definition limits trade finance to documentary trade finance activities (i.e., documentary letters of credit, documentary bills of collection).

1701. Are "exports" limited to physical goods?

No. Exports can include digital or virtual goods (e.g., email, downloads), technology and services, and be subject to a multitude of export and trade restrictions (e.g., Office of Foreign Assets Control [OFAC], Export Administration Regulations [EARs]). Depending on the definition, exports might also include financial products, thereby subjecting financial institutions to additional export and trade restrictions.

1702. Is "trade finance" limited to international commerce?

In its broadest terms, trade finance can include both domestic and international commerce; however, in terms of addressing the risks of trade finance activities, more emphasis has been placed on the financing activities that facilitate international trade.

1703. What are "free trade zones"?

Free trade zones are designated areas within countries that offer a free trade environment with minimal regulation. According to the Financial Action Task Force (FATF), free trade zones are now located in more than 130 countries. Financial institutions may consider conducting enhanced due diligence on parties and transactions associated with free trade zones. The FATF issued guidance on the vulnerabilities of free trade zones in its publication, *The Money Laundering Vulnerabilities of Free Trade Zones*. For additional guidance on geographic considerations, please refer to the Geographic Risk Assessment section.

1704. What are the heightened money laundering and terrorist financing risks of trade finance activities?

The heightened risk of trade finance activities lies in the following:

- Difficulty in conducting adequate due diligence on multiple trade parties, including screening for possible sanctions violations and/or export prohibitions
- Use of shell/front companies to further thwart efforts to conduct due diligence on trade parties
- Trade parties located in jurisdictions with lax AML/CFT laws and regulations
- Susceptibility to documentary fraud due to complex, documentary-based transactions
- Diverse and complex financing arrangements
- Lack of transparency in complex transactions
- Increased frequency of international transactions

- Potential involvement with high-risk or illicit goods (e.g., drugs, humans, bulk cash, counterfeit cash, weapons, nuclear materials or equipment, sensitive technical data, precious gems, crude oil)
- Difficulty in sharing trade information across international borders
- Among employees responsible for executing and monitoring trade finance transactions, lack of required specialised knowledge to determine effectively if a trade transaction is potentially suspicious for all types of goods

Transactions related to the potential breach of sanctions, including the proliferation of weapons of mass destruction (WMDs), has underscored the need to scrutinise trade finance activities for potentially suspicious activity.

1705. How is the term "trade-based money laundering" defined?

Trade-based money laundering (TBML) refers to the process of disguising the proceeds of illegal activity and moving value through the use of trade transactions so that they appear to come from legitimate sources or activities. Examples of TBML include the Black Market Peso Exchange (BMPE) and reintegro schemes.

1706. What are common trade finance instruments?

Common trade finance instruments include, but are not limited to, the following:

- **Letter of credit,** the most widely used trade finance instrument**,** is a formal commitment issued by a bank on behalf of and at the request of a customer, to pay a named beneficiary a stipulated amount of money upon presentation of specified documents set out in the terms and conditions detailed in the letter within a specified time frame. There are two types of letters of credit:
  - The **documentary or commercial letter of credit** is most commonly used to finance a commercial contract for the shipment of goods from seller to buyer by providing for the prompt payment of money to the seller when shipment is made as specified under its terms.
  - The **standby letter of credit** guarantees payment to the beneficiary by the issuing bank in the event of default or non-performance by the account party (the bank's customer). Although a standby letter of credit may arise from a commercial transaction, it is not linked directly to the shipment of goods from seller to buyer.

Documentary letters of credit are generally short-term payment instruments for trade finance, while standby letters of credit are written for any maturity or purpose (e.g., credit enhancement, loan guarantees, advance payment bonds, performance bonds).

- An "**irrevocable letter of credit**" is a commitment by the issuing bank to pay, provided the beneficiary complies with the terms and conditions of the letter of credit that cannot be changed unless all parties agree. Conversely, revocable letters of credit can be cancelled or amended without notice to the beneficiary.

- A "**confirmed letter of credit**" is a letter of credit guaranteed by a second bank, in addition to the bank originally issuing the credit. The confirming bank agrees to pay or accept drafts against the credit even if the issuer refuses.
- A "**back-to-back letter of credit**" is a letter of credit issued on the strength of another letter of credit involving a related transaction and nearly identical terms.
- **A banker's acceptance** is a time draft drawn on and accepted by a bank that is often used as a short-term discount instrument in international trade. A bank in the importer's country acts on behalf of the exporter for collecting and remitting payments for shipment. The exporter presents the shipping and collecting documents to his or her own bank (in his or her own country), which then sends them to its correspondent bank in the importer's country. The foreign bank (called the presenting bank) hands over the shipping and title documents required for taking delivery of the shipment to the importer in exchange for cash payment (in the case of "documents against payments instructions") or a firm commitment to pay on a fixed date (in case of "documents against acceptance" instructions). The banks involved in the transaction act only in a fiduciary capacity to collect the payment but, unlike a documentary credit, make no guarantees. They are liable only for correctly carrying out the exporter's collection instructions and may, under certain circumstances and where so instructed, sue the non-paying or non-accepting importer on the exporter's behalf. In general, by accepting the draft, a bank makes an unconditional promise to pay the holder of the draft a stated amount at a specified date.
- **Documentary collection** refers to the trade finance instrument in which the exporter entrusts the collection of a payment to the remitting bank (exporter's bank), which sends documents to a collecting bank (importer's bank), along with instructions for payment. Funds are received from the importer and remitted to the exporter through the use of a draft that requires the importer to pay the face amount either on sight (document against payment) or on a specified date in the future (document against acceptance) once the specified terms have been met.
- **Open account trading** describes unsecured trade transactions in which the buyer and seller agree on the terms of the contract. Goods are delivered to the buyer, who then arranges a payment through the financial system. In other words, goods are shipped before payment is due (typically within 30 to 90 days). The majority of trade transactions are executed in this manner as opposed to financing involving prepayments, collections, and letters of credit.

1707. What are examples of standard documentation in letter of credit transactions?

According to the "OCC Handbook: Trade Finance," standard documentation in letter of credit transactions generally falls into four primary categories: transfer, insurance, commercial and other.

- **Transfer documents** are issued by a transportation company when moving merchandise from the seller to the buyer.
    - The **bill of lading**, the most common transfer document, is a receipt given by the freight company to the shipper. A bill of lading serves as a document of title and specifies who is to receive the merchandise at the designated port (as specified by the

exporter). It can be in non-negotiable form (straight bill of lading) or in negotiable form (order bill of lading).

- In a **straight bill of lading**, the seller (exporter) consigns the goods directly to the buyer (importer). Because it allows the buyer to obtain possession of the merchandise without regard to any bank agreement for repayment, a straight bill of lading may be more suitable for prepaid or open account transactions as opposed to a letter of credit transaction.
- With an **order bill of lading**, the shipper can consign the goods to the bank, which retains title until the importer acknowledges liability to pay. This method is preferred in documentary or letter of credit transactions since the bank maintains control of the merchandise until the buyer completes all the required documentation. After the bank releases the order bill of lading to the buyer, the buyer presents it to the shipping company to gain possession of the merchandise.

- **Insurance documents**, normally an insurance certificate, cover the merchandise being shipped against damage or loss. The terms of the merchandise contract may dictate that either the seller or the buyer obtain insurance. Open policies may cover all shipments and provide for certificates on specific shipments.
- The **commercial documents**, principally the invoice, are the seller's description of the goods shipped and the means by which the buyer gains assurances that the goods shipped are the same as those ordered. Among the most important commercial documents are the invoice and the draft or bill of exchange.
  - Through the **invoice**, the seller presents to the buyer a statement describing what has been sold, the price and other pertinent details.
  - The **draft** or **bill of exchange** is a negotiable instrument that supplements the invoice as the means by which the seller charges the buyer for the merchandise and demands payment from the buyer, the buyer's bank or some other bank. The customary parties to a draft are the drawer (usually the exporter), the drawee (the importer or a bank), and the payee (usually the exporter), who is also the endorser.
    - A draft can be "clean" (an order to pay) or "documentary" (with shipping documents attached).
    - In a letter of credit, the draft is drawn by the seller, usually on the issuing, confirming or paying bank, for the amount of money due under the terms of the letter of credit.
    - In a collection, this demand for payment is drawn on the buyer.
- **Other documentation** includes official documents that may be required by governments to regulate and control the passage of goods through their borders (e.g., inspection certificates, consular invoices, certificates of origin).

Financial institutions should review available trade documentation to assist in identifying potentially suspicious activity including, but not limited to, invoices and copies of official U.S. or foreign government import and export forms to assess the reliability of documentation provided (e.g., U.S. Customs and Border Protection Form 7501 (Entry Summary), U.S. Department of Commerce Form 7525-V (Shipper's Export Declaration)).

1708. Who are the typical participants in a trade transaction?

The complex nature of trade activities requires the active involvement of multiple parties on both sides of the transaction. Participants typically include the following:

- **Trader** refers to anyone who facilitates the exchange of goods and related services across national borders, international boundaries or territories. Importers/exporters are businesses specifically organised to facilitate international trade; however, the term is commonly used to describe any business that conducts international trade transactions.
- **Trade Finance Parties** refers to the institutions that facilitate the financial component of a trade transaction (e.g., the financial institutions of the importer and exporter, intermediary financial institutions and nonfinancial institutions that provide conduits and services to expedite the payment flows and delivery of underlying documents associated with trade transactions).
- **Shipping Agents/Couriers** refers to the companies who prepare shipping documents, arrange shipping space and insurance, and deal with customs requirements.
- **Insurers** refers to the companies who provide insurance to protect against loss or damage of shipments. Many financial institutions require insurance to provide select trade financing services (e.g., letter of credit).
- **Trade/Customs Authorities** refers to the authorities who are responsible for collecting, analysing or storing trade data. Trade data refers to information collected from import-export forms or supporting documentation (e.g., description of the goods being imported or exported, quantity, value, weight, customs or tariff code number, the mode of transportation by which the goods are being imported or exported, name and address of the exporter, importer, shipping company, financial or banking data). It is important to note that the collection, use and sharing of trade data is subject to international agreements between two or more countries.
- **Investigative Authorities** refers to the authorities who are responsible for investigating money laundering, terrorist financing and/or the underlying predicate offense (e.g., customs fraud, smuggling, narcotics trafficking). In some cases, customs authorities will not have the responsibility or authority to conduct such investigations.

1709. What is the role of correspondent banking in trade finance transactions?

From a business perspective, financial institutions should ensure that collection and penalty procedures stipulated in contracts are enforceable in foreign countries in which business is conducted. In addition, many financial institutions rely on the local expertise and knowledge of their foreign correspondent banking relationships to assist in mitigating the associated risks and executing trade

finance transactions. For further guidance on correspondent banking, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Correspondent Banking.

1710. What roles can banks play in trade finance transactions?

According to the FFIEC BSA/AML Examination Manual, banks can play the following roles:

- **Issuing Bank**. The bank that issues the letter of credit on behalf of the Applicant (e.g., buyer, importer) and advises it to the Beneficiary (e.g., buyer, exporter) either directly or through an Advising Bank. The Applicant is the Issuing Bank's customer.
- **Confirming Bank**. Typically in the home country of the Beneficiary, at the request of the Issuing Bank, the bank that adds its commitment to honour draws made by the Beneficiary, provided the terms and conditions of the letter of credit are met.
- **Advising Bank**. The bank that advises the credit at the request of the Issuing Bank. The Issuing Bank sends the original credit to the Advising Bank for forwarding to the Beneficiary. The Advising Bank authenticates the credit and advises it to the Beneficiary. There may be more than one Advising Bank in a letter of credit transaction. The Advising Bank may also be a Confirming Bank.
- **Negotiation**. The purchase by the nominated bank of drafts (drawn on a bank other than the nominated bank) or documents under a complying presentation, by advancing or agreeing to advance funds to the beneficiary on or before the banking day on which reimbursement is due to the nominated bank.
- **Nominated Bank**. The bank with which the credit is available or any bank in the case of a credit available with any bank.
- **Accepting Bank**. The bank that accepts a draft, providing a draft is called for by the credit. Drafts are drawn on the Accepting Bank that dates and signs the instrument.
- **Discounting Bank**. The bank that discounts a draft for the Beneficiary after it has been accepted by an Accepting Bank. The Discounting Bank is often the Accepting Bank.
- **Reimbursing Bank**. The bank authorised by the Issuing Bank to reimburse the Paying Bank submitting claims under the letter of credit.
- **Paying Bank**. The bank that makes payment to the Beneficiary of the letter of credit.

1711. What consideration should financial institutions give to sanctions, export prohibitions and licensing requirements?

To assist in mitigating the risks associated with trade finance activities, financial institutions should consider the sanctions, export prohibitions and licensing requirements of each jurisdiction in which they conduct business.

For example, in the United States, the following government agencies have primary responsibility for sanctions and export prohibitions and licensing:

- All U.S. persons are required to comply with **Office of Foreign Assets Control (OFAC) regulations**. The purpose of OFAC is to promulgate, administer and enforce economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. OFAC Sanctions Programs target, for example, terrorists and terrorist nations, narcotics traffickers, proliferators of weapons of mass destruction (WMDs) and noncompliant participants in the rough diamond trade.
- The **Denied Persons List (DPL)**, administered by the Bureau of Industry and Security (BIS), is a list of individuals and entities that have been denied export privileges. No exporter may participate in an export or re-export transaction involving items subject to the Export Administration Regulations (EAR) with a person or entity whose export privilege has been denied by the BIS.
- The **Commerce Control List (CCL)**, administered by the Commerce Department pursuant to the Export Administration Act of 1979 (EAA) (as amended), is used to regulate the export and re-export of items that have commercial uses but also have possible military applications (dual-use items). Examples of items on the CCL include, but are not limited to, the following:
    - Nuclear materials, chemicals, microorganisms and, toxins
    - Computers
    - Telecommunications
    - Information security
    - Navigation and avionics
    - Aerospace and propulsion
- The **U.S. Munitions List (USML)**, administered by the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs within the State Department pursuant to the Arms Export Control Act of 1976 (AECA) and the International Traffic in Arms Regulations (ITAR), is used to control the export of defence articles, services and related technologies. Examples of items on the USML list include, but are not limited to, the following:
    - Firearms, such as close assault weapons, combat shotguns, guns over calibre 0.50 and flamethrowers
    - Launch vehicles, guided missiles, ballistic missiles, rockets, torpedoes, bombs and mines
    - Explosives, propellants and incendiary agents
    - Armored combat ground vehicles, special naval equipment, fighter bombers, attack helicopters, unmanned aerial vehicles (UAV)
    - Military training equipment
    - Personal protective equipment, such as body armour, helmets and select face paints
    - Military electronics, such as radios and radar systems

The Defense Department is actively involved in the interagency review of those items controlled on both the CCL and the USML. The agencies work together when there is a question about whether a proposed export is controlled on the CCL or the USML.

- The **AECA Debarments list**, also administered by the Directorate of Defense Trade Controls within the State Department pursuant to AECA and ITAR, includes persons who have been convicted for violations (or conspiracy to violate) the AECA in court (statutory debarments) or have violated (or conspired to violate) the AECA during an administrative proceeding (administrative debarment). The Energy Department, through the National Nuclear Security Administration (NNSA) is responsible for the security of the U.S. nuclear weapons, nuclear proliferation and naval reactor programs. This includes controlling nuclear technology and technical data for nuclear power.

  The U.S. Department of Energy controls nuclear technology and technical data for nuclear power.

For further guidance on the aforementioned lists, please refer to the following sections: OFAC Sanctions Listings and Other U.S. and International Sanctions Programs. For further guidance on licensing, please refer to the OFAC Licensing section.

1712. What is OFAC's Rough Diamond Trade Controls Sanctions program and how does it impact importers/exporters?

Established by the Clean Diamond Trade Act (CDTA), IEEPA, NEA, UNPA, and Executive Order 13312 – Implementing the Clean Diamond Trade Act, OFAC's Rough Diamond Trade Controls Sanctions Program prohibits the import and export of rough diamonds from countries that do not participate in the Kimberley Process Certification Scheme (KPCS) and prohibits any transaction that evades or attempts to evade these prohibitions on or after July 30, 2003.

Importers/exporters of rough diamonds directly must comply with KPCS and the Rough Diamond Trade Control Program rules, which include registration, reporting and other trade control requirements.

1713. What is the Kimberley Process Certificate Scheme (KPCS)?

Launched in 2003, the Kimberley Process Certificate Scheme (KPCS) is an international program that implements certification requirements and other import/export controls to prevent the production and trade in rough diamonds that are used to finance violence in countries in conflict (e.g., Democratic Republic of the Congo, Cote d'Ivoire). These diamonds are also known as "conflict diamonds" or "blood diamonds."

The Kimberley Process Certificate is a unique tamper- and forgery-resistant document that certifies that a shipment of rough diamonds was handled in accordance with the KPCS. Kimberley Process Certificates can only be obtained from entities licensed by the U.S. Kimberley Process Authority (USKPA).

For imported rough diamonds, the ultimate consignee is required to report receipt of the shipment to the relevant foreign exporting authority (e.g., the agency with the authority to validate the Kimberley

Process Certificate). Reports must be made within 15 calendar days of the date that the shipment arrived at a U.S. port of entry.

For exported rough diamonds, exporters must report the shipment to the U.S. exporting authority, the U.S. Bureau of Census, through the Automated Export System (AES).

U.S. Customs will not release shipments of rough diamonds without formal and complete documentation.

For further guidance on the sanctions related to rough diamonds, please refer to the Rough Diamond Trade Controls Sanctions Program section.

1714. How can trade finance activities be monitored for potentially suspicious activity?

Due to the complex and fragmented nature of trade finance, financial institutions often do not have access to the necessary information to monitor trade transactions effectively for potentially suspicious activity. For example, trade data may not be publicly available or current, or the particulars of a specific business arrangement may not be apparent (e.g., legitimate discounts, bartering deals). If credit services are not provided, financial institutions may only facilitate the transmission of funds with no knowledge of the purpose of the payment. Financial institutions should conduct appropriate due diligence prior to the inception of the customer relationship, and conduct ongoing monitoring of trade transactions that may pose risks.

"The Wolfsberg Group, ICC and BAFT Trade Finance Principles (2017)" provides guidance on due diligence specific to documentary credits, bills for collection, guarantees and standby letters of credit. The "OCC Handbook: Trade Finance" provides common errors in letter of credit documentation (e.g., bills of lading, invoices, insurance documents, drafts).

To the extent feasible, financial institutions should review trade documentation, not only for compliance with the terms of the trade and/or financial agreement (e.g., letter of credit), but also for red flags that could indicate unusual or suspicious activity. Examples of potentially suspicious activity include obvious under- or over-invoicing, lack of government licenses (when required), and discrepancies in the description of goods on various documents.

Cooperation among the multiple financial institutions involved in each trade finance transaction, as well as other participants involved in the trade transaction, can facilitate the effective identification of potentially suspicious activity. A strong correspondent banking due diligence program is instrumental in mitigating the risks associated with trade finance.

For further examples of red flags of potentially suspicious activity, please refer to the following sections: Suspicious Activity Red Flags and Trade Finance Red Flags. For further guidance on correspondent banking, please refer to the following sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Correspondent Banking.

1715. In circumstances where a Suspicious Activity Report (SAR) is warranted, are financial institutions expected to stop trade or discontinue processing the transaction(s)?

Unless there is a potential OFAC violation that may require the blocking or rejecting of one or more transactions, generally, in circumstances where a SAR is warranted, financial institutions are not required to stop trade or discontinue processing the transactions. However, financial institutions proceed at their own risk when continuing to allow suspect transactions to occur.

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including but not limited to ongoing money laundering schemes or detection of terrorist financing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

Additionally, FinCEN has established a hotline, 1.866.556.3974, for financial institutions to report voluntarily to law enforcement suspicious transactions that may relate to recent terrorist activity against the United States.

1716. What is an example of trade-based money laundering (TBML)?

Generally, the Black Market Peso Exchange (BMPE) is an intricate TBML system in which transnational criminal organisations (TCOs), as an example, Colombian drug cartels sell drug-related U.S.-based currency to money brokers (e.g., peso broker) in a foreign country (e.g., Colombia) who, in turn, "exchanges" the illicit U.S. currency for a foreign currency (e.g., Colombian peso) through a series of transactions involving multiple financial institutions that support legitimate international trade between foreign importers and U.S. exporters.

For example, once Colombian drug cartels deliver drug-related U.S. currency to a peso broker (directly or indirectly through the use of couriers or other transportation operators), the peso broker may then do the following:

- Place the illicit currency into U.S. bank accounts by structuring or smurfing transactions to evade BSA reporting requirements; and
- Sell monetary instruments drawn on its U.S. bank accounts to Colombian importers who use them to purchase U.S. goods; or
- Pay for U.S. goods directly (e.g., by delivering the illicit currency directly to U.S. exporters) on behalf of Colombian importers with reimbursement upon delivery of the goods in Colombia; or
- Smuggle drug-related U.S. currency out of the country for deposit into foreign financial institutions (FFIs) for repatriation to the peso broker or directly to a U.S. exporter through various methods (e.g., wire transfers, bulk shipments of currency), often involving correspondent banking relationships and/or *casas de cambio*; and
- Pay the Colombian drug cartels in pesos, less a fee, thereby completing the "foreign exchange" transaction, and effectively laundering drug-related currency.

The BMPE not only allows drug cartels to launder funds, it assists importers/exporters in evading trade controls and taxes. Peso brokers often fail to file required reports on reportable currency transactions and increasingly use new payment methods to launder illicit funds (e.g., prepaid cards,

mobile payments, digital currencies, internet gambling sites). Due to the complex nature of the transactions and the involvement of multiple third parties, BMPE activity is difficult to detect.

Although the BMPE in Colombia is one of the more widely known informal value transfer systems (IVTSs), BMPEs operate in other parts of the world, too (e.g., Mexico, Panama).

1717. What does the term "reintegro" mean?

"Reintegro" refers to a trade-based, reverse-BMPE laundering scheme that hinges on trade document manipulation and often includes the corruption of a bank employee or customs official. Unlike traditional BMPE activities that operate with goods (not funds) crossing the border, in reintegro transactions, peso exchange brokers repatriate drug proceeds by disguising them as payments for non-existent or overvalued goods using purchased export papers, similar to letters of credit, to make the payments appear legitimate. This is known as "reintegro" or "reintegrate papers."

1718. What is the International Chamber of Commerce?

The International Chamber of Commerce (ICC), established in 1919 with members in more than 120 countries, is a world business organisation with a mission to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalisation by establishing rules and policies to facilitate international trade and facilitating arbitration.

The ICC has issued standard rules and practices to facilitate international trade (e.g., The Uniform Customs and Practice for Documentary Letters of Credit (2007 Revision), ICC Publication No. 600; and The Uniform Rules for Collections, ICC Publication No. 522). These standard rules and practices assist financial institutions in establishing controls to mitigate the risks of trade finance without hindering business.

The ICC has also established the Commercial Crime Services (CCS) and Business Action to Stop Counterfeiting and Piracy (BASCAP) to assist in combating maritime piracy, financial fraud and counterfeiting.

1719. What guidance has been issued on trade finance?

The following key guidance has been issued on trade finance and TBML/FT:

- **Trade Finance Activities – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **Trade-Based Money Laundering** (2012) by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing through Trade in Diamonds** (2013) by FATF
- **Money Laundering Vulnerabilities of Free Trade Zones** (2010) by FATF
- **Best Practices Paper on Trade-Based Money Laundering** (2008) by FATF

- **The Wolfsberg Trade Finance Principles** (2011) by the Wolfsberg Group of Banks (Wolfsberg Group)
- **The Wolfsberg Group, ICC and the BAFT Trade Finance Principles** (2017) by the Wolfsberg Group
- **Guiding Principles for Sanction Issues Related to Shipping and Financial Products** (2017) by Banker's Association for Finance and Trade (BAFT) and The Clearing House Association LLC (TCH)
- **Trade-Based Money Laundering: Overview and Policy Issues** (2016) by the Congressional Research Service, Rena S. Miller, Liana W. Rosen and James K. Jackson
- **Guidance for Identifying Potentially Suspicious Activity in Letters of Credit and Documentary Collections** (2015) by BAFT
- **Advisory to Financial Institutions on Filing Suspicious Activity Reports regarding Trade-Based Money Laundering** (2010) by the Financial Crime Enforcement Network (FinCEN)
- **Application of a Section 311 Special Measure to Payments under a Stand-By Letter of Credit** (2009) by FinCEN
- **Black Market Peso Exchange Update** (2002) by FinCEN
- **Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States** (2006) by FinCEN
- **Comptroller's Handbook: Trade Finance** (1998) by the Office of the Comptroller of Currency (OCC)
- **Comptroller's Handbook: Banker's Acceptances** (1999) by the OCC

The following key OFAC guidance has been issued for importers and exporters:

- **Foreign Assets Control Regulations for Exporters & Importers** (2012) by OFAC
- **Frequently Asked Questions for Importers and Exporters** (2012) by OFAC
- **Frequently Asked Questions on Licensing** (2012) by OFAC
- **Ask the TIC: Guide to Export Controls** (2000) by the Trade Information Center (TIC)
- **Letter of Credit Update: OFAC Regulations: The Countries Aren't Enough!** (2002) by OFAC
- **Notice to Mariners** (2006) by the National Geospatial-Intelligence Agency (NGA)
- **Part 1 and Part 2 - Export Controls Compliance: Don't Neglect OFAC** (1999) by the Society for International Affairs, Inc.

Additional organisations providing guidance on trade transactions, trade finance and TBML include, but are not limited to, the following:

- The **Export Enforcement Coordination Center (E2C2)** is a multi-agency center created to coordinate and enhance criminal, administrative, and related export enforcement activities. The center acts as a primary point of contact between enforcement authorities, public outreach and government-wide statistical tracking, which serves to minimise the duplication of effort and strengthens the link between law enforcement, the intelligence community, and export licensing entities. Participating agencies include the following:
    - U.S. Department of Homeland Security—Immigration and Customs Enforcement, Homeland Security Investigations (HSI)
    - U.S. Department of Homeland Security—Customs and Border Protection (CBP)
    - U.S. Department of Commerce—Office of Export Enforcement (OEE)
    - U.S. Department of Justice—Federal Bureau of Investigations (FBI)
    - U.S. Department of Justice—National Security Division (DOJ/NSD)
    - U.S. Department of Defense—Defense Criminal Investigative Service (DCIS)
    - Office of the Director of National Intelligence—Office of the National Counterintelligence Executive (ODNI)
    - U.S. Department of Energy—National Nuclear Security Administration
    - U.S. Department of State—Directorate of Defense Trade Controls (DDTC)
    - U.S. Department of Treasury—Office of Foreign Asset Control (OFAC)
    - U.S. Department of Justice—Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)
    - U.S. Department of Defense—Air Force Office of Special Investigations (OSI)
    - U.S. Department of Defense—Defense Intelligence Agency (DIA)
    - U.S. Department of Defense—Defense Security Service (DSS)
    - U.S. Department of Defense—Naval Criminal Investigative Service (NCIS)
    - U.S. Postal Service—U.S. Postal Inspection Service (USPIS)
    - U.S. Export-Import Bank—Office of the Inspector General
- The **U.S. Customs and Border Protection (CBP)** agency is one of the Department of Homeland Security's largest divisions responsible for securing the borders of the United States while simultaneously facilitating the flow of legitimate trade and travel.
- **Trade Transparency Units (TTUs)** were established by the U.S. Immigration and Crime Enforcement (ICE) agency. TTUs conduct financial, money laundering and trade fraud investigations, and have access to customs information on cargo movements, trade data and financial information collected by financial intelligence units (FIU) of participating jurisdictions.

- The **Trade Information Center (TIC)** is operated by the International Trade Administration of the U.S. Department of Commerce for the 20 federal agencies comprising the Trade Promotion Coordinating Committee.
- The **International Chamber of Commerce (ICC)**, established in 1919 with members in more than 130 countries, is a world business organisation with a mission to promote trade and investment across frontiers and help business corporations meet the challenges and opportunities of globalisation by establishing rules and policies to facilitate international trade and facilitating arbitration. The ICC has established the Commercial Crime Services and Business Action to Stop Counterfeiting and Piracy to assist in combating maritime piracy, financial fraud and counterfeiting.
- The **World Trade Organisation (WTO)**, established in 1995, is an international body with more than 150 member countries that deals with the rules of trade between nations, ranging from liberalising trade to negotiating trade agreements to settling trade disputes.
- The **World Customs Organisation (WCO)** (formerly the Customs Co-operation Council), established officially in 1952, is an intergovernmental organisation with more than 170 member countries. It focuses exclusively on customs matters such as the development of global standards, the simplification and harmonisation of customs procedures, trade supply chain security, the facilitation of international trade, the enhancement of customs enforcement and compliance activities, anti-counterfeiting and piracy initiatives, public-private partnerships, integrity promotion, and sustainable global customs capacity building programs. The WCO also maintains the international Harmonised System goods nomenclature, and administers the technical aspects of the WTO Agreements on Customs Valuation and Rules of Origin as well as the Customs Enforcement Network (CEN), a central depository for enforcement-related information to assist the customs enforcement community in producing and exchanging intelligence.
- The **Global Trade Finance Program (GTFP)** was established by the International Finance Corporation, a private arm of the World Bank. The GTFP extends and complements the capacity of banks to deliver trade financing by providing risk mitigation in new or challenging markets where trade lines may be constrained.

Electronic Banking and Digital Value

1720. What does the term "electronic banking" mean?

Electronic banking, or e-banking, is a broad term used to describe financial services provided to customers through various electronic delivery mechanisms or channels. Examples of e-banking include, but are not limited to, the following:

- Automated teller machine (ATM) transactions;
- Online account opening and banking transactions;
- Mobile banking;
- Telephone banking; and

- Remote deposit capture (RDC) services.

Further guidance on each of these electronic banking services is provided below.

1721. What does the term "e-cash" mean? Is it included within the definition of electronic banking?

"E-cash," also known as e-wallets or e-money, is a digital representation of currency (e.g. legal tender, in circulation, accepted as a medium of exchange in the country of issuance) that can be stored and retrieved in several forms, including computer-based, mobile telephone-based and prepaid cards.

Electronic banking generally refers to the method of access, whereas prepaid access refers to the actual "value" that can be accessed through electronic banking.

Computer-based e-cash is usually accessed via a computer or stored in an online repository. Mobile phone e-cash is often accessed through an individual's mobile phone number. Prepaid access and e-cash may be held in a pooled account at a bank. Such accounts may be used to transfer funds between users (e.g., people to people, people to business, business to business), make payments to merchants, allow for cash withdrawals and many other functionalities.

Like e-cash, virtual currencies are digital representations of value but they are not the same, as they do not represent legal tender. For further guidance, please refer to the sections: Prepaid Access and Stored-Value and Virtual Currencies.

Additional information on types of e-cash products is available in the FFIEC Information Technology Examination Handbook.

1722. What are the heightened money laundering and terrorist financing risks of electronic banking?

The lack of face-to-face contact in e-banking transactions heightens the risks of transactions conducted through this method. This introduces vulnerabilities such as exposure to unauthorised users and foreign jurisdictions.

Additionally, the reliance on third-party services, and in some cases providers, elevates the risk.

1723. What steps can a financial institution take to mitigate the risk associated with electronic banking?

To mitigate the risks associated with electronic banking, financial institutions may consider implementing the following:

- Limiting the types of transactions that can be conducted through electronic banking (e.g., information only, initiation of transactions)
- Imposing risk-based transaction limits and/or monitoring thresholds (e.g., per transaction, monthly)
- Limiting the opening of new accounts online to existing customers who have established relationships through a branch or other process involving face-to-face contact with an employee

- Applying additional controls (e.g., authentication) prior to executing transactions initiated through electronic banking methods

1724. How do the FATF Recommendations address new and emerging technologies in financial services?

FATF Recommendation 15 – New Technologies advises countries and financial institutions conduct risk assessments to identify and evaluate the ML/TF risks and vulnerabilities of new technologies. FATF uses the term new payment products and services (NPPS) to describe some of the new product offerings (e.g., prepaid cards, mobile payments, electronic money, digital currencies).

FATF also published "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Systems" in 2013.

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

Online and Mobile Banking

1725. What does the term "online banking" mean?

Online banking, also known as internet banking, refers to the method of e-banking in which a customer accesses financial services through an internet connection, typically through a computer. Mobile banking, also known as m-banking, refers to the method of e-banking accessed through a mobile device (e.g., mobile phone, tablet).

1726. What steps can a financial institution take to mitigate the risks associated with online banking?

Financial institutions offering internet-based products and services should use risk-based methods (e.g., transaction limits, unless specified information is provided, multifactor security processes) to authenticate the identity of customers using these products and services to safeguard customer information, prevent money laundering and terrorist financing, reduce fraud, and inhibit identity theft. For further guidance on identity theft, please refer to the Identity Theft and Identity Theft Prevention Program section.

1727. Is "authentication" the same as "verification" as defined in Section 326 – Verification of Customer Information, also known as the Customer Identification Program (CIP)?

No. Authentication attempts to ensure that the individual providing the information, or accessing the account(s), is the person he or she claims to be. Authentication is accomplished by requesting information that is not necessarily "found in a wallet" (e.g., previous address, previous employer).

Verification confirms that the information provided by a customer is valid (e.g., an individual with the provided name, address and TIN matches with an independent source, such as a credit reporting database).

Often, once an individual has been verified, financial institutions will ask customers to create custom security questions (e.g., mother's maiden name, favourite movie, pet's name) that serve to authenticate customers.

1728. Is requiring a username and password an adequate control for online banking transactions?

No. Single-factor authentication (e.g., username/password) is inadequate for high-risk transactions (e.g., access to customer information and the movement of funds) as it is easier to compromise than multi-factor authentication methods. Additional methods of authentication include, but are not limited to, the following:

- Shared-secret techniques (e.g., personal identification numbers [PINs])
- Physical devices such as smart cards, one-time passwords (OTPs), USB plug-ins or other types of "tokens"
- Biometric identification (e.g., fingerprint recognition, face recognition, voice recognition, retinal scan)
- Customer verification techniques
    - Positive verification ensures that material information provided by customers matches information from third-party sources.
    - Negative verification ensures that information provided is not linked to previous fraudulent activity.
    - Logical verification ensures that the information is consistent (e.g., area code of the home number is within the ZIP code of the address provided by the customer).

Automated Teller Machines

1729. What is an "automated teller machine (ATM)"?

An automated teller machine (ATM) is an electronic banking device that can be used by customers without the aid of a representative (e.g., teller) for the following types of services:

- Accessing account information (e.g., balance inquiry, account statements)
- Withdrawing and/or depositing funds (e.g., cash, monetary instruments)
- Transferring funds between linked accounts
- Bill payment

1730. In some instances, customers may be able to manage value on prepaid access cards through ATMs. Is single-factor authentication an adequate control for ATM transactions?

No. Two-factor authentication is most widely used with ATMs. For example, to withdraw money from an ATM, customers must present both an ATM card and a PIN.

1731. What is a "privately owned automated teller machine"?

A privately owned ATM is not owned by a financial institution. Privately owned ATMs are often found in convenience stores, bars, restaurants, grocery stores and check-cashing establishments.

1732. What are the heightened money laundering and terrorist financing risks associated with ATMs?

Due to the nature of non-face-to-face interactions of ATMs, they are of heightened risk for money laundering and terrorist financing. Examples of suspicious activity conducted through ATMs include, but are not limited to, the following:

- Structuring/smurfing transactions, domestically and internationally to evade BSA reporting requirements (e.g., Currency Transaction Reports [CTRs], Report of International Transportation of Currency or Monetary Instruments [CMIRs])
- Abuse as an informal money transmitter (e.g., deposit funds in one jurisdiction for withdrawal by a third-party in another jurisdiction)
- Fraud (e.g., check fraud, identity theft, personal identification number [PIN] theft, account takeover)

Privately owned ATMs are considered high risk because U.S. law enforcement has observed an increase in their use in money laundering, identity theft and fraud schemes. For example, owners or operators of privately owned ATMs may use illicit cash (of their own or from their customers) to replenish their ATMs, as opposed to legitimate sources (e.g., cash from sales or a financial institution).

Additionally, most states do not monitor or require registration of owners of privately owned ATMs, thereby making it difficult to track current ownership.

For additional guidance on privately owned ATMs, please refer to the sections: Third-Party Payment Processors and Owners/Operators of Privately Owned ATM Red Flags.

Remote Deposit Capture

1733. What does the term "remote deposit capture" mean?

Remote deposit capture (RDC) is an electronic deposit delivery system by which customers deposit checks or monetary instruments into a bank account from a remote location via transmission to the financial institution of digital information or a scanned image, rather than delivery of the physical item (e.g., check, monetary instrument).

Scanning and transmission activities can take place at branches, ATMs, domestic and foreign correspondents, and locations owned or controlled by customers, as well as through the use of mobile technology such as mobile phones.

1734. How does RDC occur at remote locations controlled by customers?

Customers make deposits by scanning items from their homes or on the premises of their businesses utilising RDC processing technology, and send images of deposit items for processing through check-clearing networks or the deposit data for processing and clearing through the ACH network.

1735. Are RDC services limited to checks and monetary instruments?

No. Some RDC services facilitate the electronic capture of cash and card payments.

1736. How can cash be deposited through RDC?

RDC also may include the electronic capture of deposit information comprised of cash through remote safekeeping arrangements at customer locations or at other participating intermediaries (e.g., a grocery store).

1737. Are RDC services limited to scanning items from the home or premise of the customer?

No. Customers can make deposits utilising RDC processing technology at their home or place of business, through a lockbox arrangement, through a mail drop or kiosk.

1738. Are RDC services limited to business customers?

No. Many RDC services allow individuals to make remote deposits utilising smartphone technology.

1739. What are the heightened money laundering and terrorist financing risks of RDC?

RDC is considered a higher-risk service since the financial institution never receives original physical items from customers, thereby increasing the risk of checks, money orders and traveller's checks being physically altered. This may increase the difficulty of complying with recordkeeping and reporting requirements and monitoring for potentially suspicious activity, such as sequentially numbered documents. RDC services increasingly are being utilised by foreign correspondent banking customers and money services businesses (MSBs) to replace pouch services and certain instrument processing and clearing activities.

Further, because RDC equipment is portable, it is difficult to ensure that the equipment is actually being used by the registered owner.

Additionally, operational risks at a business location include unauthorised access to technology systems and electronic data images, ineffective controls over physical deposit handling and storage procedures, and inadequate background checks on employees who have access to physical deposit items or technology.

1740. What can a financial institution do to mitigate the risk posed by RDC customers?

To mitigate the risk associated with customers utilising RDC services, a financial institution should conduct a suitability review on the customer prior to establishing the RDC relationship. Following are examples of factors that may be used to assess a customer's suitability:

- Nature of the customer's business compared to a list of acceptable types of businesses
- Credit history
- Financial statements
- Ownership structure
- Customer's risk management processes
- Geographic location of the operations

In addition to information collected during the suitability review, following are examples of due diligence that may be collected on customers who wish to establish an RDC relationship:

- Customer base
- Expected activity
- Type of activity (e.g., payroll checks, third-party checks or traveller's checks)

A financial institution may consider adding the following provisions to the signed contract with customers establishing an RDC relationship:

- Each party's roles, responsibilities and liabilities
- Record retention expectations for RDC data
- Location and physical security of RDC equipment and original documents
- Expectations regarding controls to prevent the inappropriate use of RDC equipment
- Authority to request original documents, conduct audits and/or terminate RDC relationships

A financial institution may consider conducting site visits in order to evaluate the customer's operational controls in place, as well.

1741. How should RDC activities be monitored for potentially suspicious activity?

In addition to money laundering and terrorist financing risks, other risks include check fraud, check kiting and duplication of deposits through different channels, so financial institutions should train employees to be aware of these activities when monitoring RDC transactions. Common red flags include, but are not limited to, the following:

- High volume of rejected and returned items
- High volume of deposit items from foreign correspondent accounts, particularly those associated with money services businesses (MSBs) and *casas de cambio*

- Consistently poor image quality of scanned deposits
- High volume of checks missing endorsements or appearing altered
- Significant variance in expected/historical activity versus actual activity in terms of the volume and types of transactions conducted through the account
- Dollar amounts that appear to be designed to evade reporting requirements (i.e., under US$3,000 or US$10,000) or are purchased in round amounts
- Multiple, sequentially numbered monetary instruments

The utilisation of interdiction software based on "negative databases" of customers previously associated with fraudulent activity is another effective method for detecting potentially suspicious activities. For additional guidance on red flags, please refer to the sections: Suspicious Activity Red Flags and Pouch Activity and Remote Deposit Capture.

1742. What can a financial institution do to mitigate the risks posed by RDC vendors?

Financial institutions should conduct due diligence on their RDC technology service providers and RDC hardware and software suppliers as part of their overall vendor management program. For additional guidance, please refer to the Third-Party Payment Processors section.

Prepaid Access and Stored-Value

1743. What does the term "prepaid access" mean?

The BSA defines "prepaid access" as the following:

- Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number.

1744. What is the difference between prepaid access and stored value cards?

Prepaid access refers to all the different ways funds that have been paid in advance can be accessed, while stored value is generally used to describe the prepaid card market.

FinCEN stated that prepaid access is not itself a device or vehicle, but that devices or vehicles are means through which prepaid funds are accessed. The two main elements of prepaid access are:

- Funds that have been paid in advance; and
- Those funds that can be retrieved or transferred at some point in the future. FinCEN also clarified that it intended its definition to include the necessary regulatory elasticity to survive future technological advancements.

1745. What are the heightened money laundering and terrorist financing risks of prepaid access?

Transactions may involve funds that have been transferred to or from an unknown party or from a party that wants to engage in illicit transactions or money laundering. Law enforcement has voiced concerns in part due to the ease with which prepaid access can be obtained, the high velocity of money that potentially can be moved with prepaid access and the anonymous use of some prepaid access. However, unlike cash, there are records available for all of the transactions performed for a particular prepaid access device.

Following are examples of types of factors that may increase the risk associated with a prepaid access product:

- Reloadability
- High value/unlimited load amount
- Lack of account relationship with issuer and/or seller of the products
- Lack of identification of purchaser
- Source used to fund product is cash, credit card or another stored-value product
- Ability to conduct cross-border transactions
- Ability to make cash withdrawals

1746. Is the definition of prepaid access limited to cards?

No. The regulatory definition of prepaid access was designed to be applicable to emerging and developing technologies, which may include but are not limited to the following:

- Near field communications (NFCs) (set of short-range wireless technologies that establish electromagnetic radio fields that enable devices to communicate with each other when touching or in close proximity)
- Chip technology
- Magnetic strips
- Cellular phones
- Prepaid access through the internet using PINs/codes
- Prepaid access through fobs, tokens, chips or other technology
- E-cards
- Virtual currency

Prepaid access products encompass a large number of current and most of the emerging growth products, such as open-loop general purpose reloadable (GPR) cards, certain closed-loop cards, cellular phone access, fob or barcode access.

1747. Do all types of prepaid access products pose the same degree of risk?

No. FinCEN has issued guidance suggesting that the following types of prepaid access products pose lower risk:

- Closed-loop prepaid access – Prepaid access to funds or the value of funds with a maximum dollar threshold of US$2,000 that can be used only for goods or services involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system;
- Devices that do not permit international use (e.g., use at foreign merchants via the internet or face to face);
- Non-reloadable devices

1748. What is the difference between a closed-loop and open-loop prepaid access product?

Closed-loop prepaid access products are usable only at a specific merchant, or a group of merchants using the same branding, such as a Starbucks card. They may be in a fixed amount or reloadable. Open-loop prepaid access products may be used at multiple merchants, such as a prepaid card that contains a Visa logo and can be used at any merchant that accepts Visa debit cards. Open-loop cards may also come in fixed or reloadable amounts.

1749. Can a closed-loop prepaid access product be used to launder illicit funds?

As with any type of payment product or service, it is possible for a closed-loop prepaid access product to be misused. Law enforcement has identified instances where drug dealers used illicit funds to purchase closed-loop gift cards, and the cards were then used to purchase retail items. In early 2016, perpetrators of terrorist attacks in Brussels, Belgium reportedly used prepaid cards to pay for daily living expenses (e.g., hotel).

1750. Are banks required to comply with the final rule related to Providers and Sellers of Prepaid Access?

No. The final rule exempts banks and financial institutions regulated by the Securities and Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTC) from the definition of "provider" of prepaid access.

1751. How many of the SARs filed in a calendar year involve prepaid access?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports involving prepaid access totalled nearly 41,000 (2 percent) and were distributed across financial institution types as follows:

- Depository institutions: 25,000 cases (62 percent)
- Money services businesses (MSBs): 13,000 cases (32 percent)
- Other types of financial institutions (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily): 2,700 cases (7 percent)

- Securities and futures firms: 59 cases (0.1 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 3 cases (less than 0.1 percent)
- Insurance companies: 1 cases (less than 0.1 percent)
- Housing GSEs: 0 cases (0 percent)
- Casinos and card clubs: 0 cases (0 percent)

1752. What are the components of an effective risk management program for prepaid access programs?

On June 28, 2011, the Office of the Comptroller of the Currency (OCC) issued "Risk Management Guidance and Sound Practices" for prepaid programs. As with AML Programs, the OCC suggests financial institutions implement a risk-based program to manage the AML/CFT, sanctions, fraud and third-party risks of their prepaid access programs. An effective risk management program for prepaid access programs should include the following:

- Policies and procedures addressing the following:
  - Risk assessment of prepaid access products including product capabilities, regulatory requirements, competitive factors and other factors of the business model that would impact the risk/reward analysis of the program;
  - Due diligence on purchasers of prepaid access products;
  - Disclosures to purchasers about pricing, fees, transaction limits and credit features; and
  - Due diligence for selecting third-party service providers (TPSP) and oversight of TPSPs, including ongoing monitoring of regulatory obligations, information sharing, business continuity/disaster recovery and termination policy.
- Ongoing audit, self-assessment and compliance functions;
- Comprehensive management reporting to senior management and the board of directors.

1753. What steps can be taken to mitigate the risks associated with prepaid access products?

Following are examples of the types of steps that may be taken to mitigate the risk of prepaid access products:

- Monitor purchases, reloads and withdrawal activities for potentially suspicious activity;
- Limit the amount of money that can be loaded over a specified period of time for higher-risk products;

- Limit the number of cards that can be purchased by an individual, or require enhanced due diligence to determine the reason for purchasing a large number of cards (for example, as holiday gifts for teachers or a charity event);
- Limit the dollar amount or location of ATM withdrawals on high-risk products; and
- Obtain identifying information from the purchaser or recipient for higher-risk products.

1754. What due diligence should be conducted on third-party service providers of prepaid access products?

Financial institutions that issue prepaid access products through a third-party service provider (TPSP) should manage risks by monitoring performance, suspicious activities and fraud losses of its third-parties. Financial institutions should also consider their consumer protection obligations when selecting a TPSP and design an effective prepaid access and compliance program.

The OCC suggests the following details be outlined in contracts/agreements with TPSPs:

- Regulatory obligations of each party, including monitoring and reporting of suspicious activity;
- Business continuity/disaster recovery plans for service disruptions and/or security breaches;
- Right of the financial institution to audit and monitor performance of the TPSP (e.g., review the prepaid access program and compliance program);
- Termination parameters (e.g., conditions under which the relationship with the TPSP can be terminated); and
- Process to share information about suspicious activities and fraud losses, and indemnify losses.

Following are examples of the types of due diligence that may be conducted on TPSPs, depending on the risks posed by both the products offered and the third-party itself:

- Review of corporate documentation, licenses, permits, contracts or references;
- Review of financial documentation such as credit reports, financial statements and tax returns;
- Background checks, including running all parties against the OFAC and sanctions lists;
- On-site visits;
- Review of TPSP's compliance program that includes the following:
    - Due diligence on purchasers
    - AML/CFT, sanction and fraud policy and procedures
    - Training
    - Independent assessments of program
    - Reports to the board of directors or senior management
- Review of AML/CFT audits/reviews of company-prepared self-assessments.

Some financial institutions develop training programs for TPSPs to assist in complying with AML/CFT laws and regulations. Some participants of prepaid access programs are now required to maintain an AML Program. For further guidance, please refer to the Providers and Sellers of Prepaid Access section.

1755. Have additional regulations been proposed for prepaid access?

Yes. Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protect Act, the Consumer Financial Protection Bureau (CFPB) held a hearing in May 2012 regarding prepaid access, particularly general purpose reloadable (GPR) cards. Pursuant to DFA, in 2016, the CFPB finalised the rule "Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)." However, this rule (which was scheduled to become effective on October 1, 2017, but has been put on hold under the Trump administration) focuses on prepaid consumer protection issues, not AML/CFT.

In October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on Reports of International Transportation of Currency or Monetary Instruments (CMIRs). No final rule on this proposed change has yet been issued. Section 13 of the proposed bill Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017, introduced by the U.S. Senate in May 2017, proposed amending the definition of monetary instrument to include funds stored in a digital format (e.g., prepaid access devices, virtual currency). Whether this bill will ever be passed into law is unclear.

Virtual Currencies

1756. How is the term "virtual currency" defined?

FinCEN defines "**virtual currency**" as "a medium of exchange that operates like currency in some environments, but does not have all the attributes of real or fiat currency."

"**Currency**" is defined as the coin and paper money (including Federal Reserve notes and circulating notes of Federal Reserve banks and national banks) of the United States or of any other country that:

- Is designated as legal tender (i.e., form of payment defined by law which must be accepted by creditors as payment for debts);
- Circulates; and
- Is customarily used and accepted as a medium of exchange in the country of issuance.

"**Fiat currency**" is another term used to describe "real" currency that is government-issued.

Similarly, in its report "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," FATF defines "virtual currency" as a "digital representation of value that can be digitally traded and functions as:

- A medium of exchange; and/or
- A unit of account; and/or

- A store of value that does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction."

1757. Who are the typical participants of a virtual currency system?

FinCEN identifies three types of participants in a virtual currency system:

- A "**user**" is defined as "a person that obtains virtual currency to purchase [real or virtual] goods or services on the user's own behalf;" in other words, a consumer.
- An "**exchanger"** is defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency."
- An "**administrator**" is defined as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."

FATF also notes that other third parties that participate and support virtual currency systems, including, but not limited to "**merchants**" that accept virtual currency in exchange for goods and services, "**wallet providers"** that provide a virtual currency wallet (e.g., software application, data file) for holding, storing and transferring virtual currency, "**third party payment senders**" that facilitate merchant acceptance, and "**software developers**" which provide applications to facilitate merchant payment processing. Collectively, FATF refers to these products as virtual currency payments products and services (VCPPS).

1758. What is a "convertible virtual currency"? Is it a type of e-cash?

FinCEN defines "convertible virtual currency," also known as open virtual currency, as a type of virtual currency that has "an equivalent value in real currency or acts as a substitute for real currency." It is not a form of e-cash.

"E-cash," also known as e-wallets or e-money, is a digital representation of fiat currency that can be stored and retrieved in several forms, including computer-based, mobile telephone-based and prepaid cards.

For further guidance on e-cash, please refer to the Electronic Banking and Digital Value section.

1759. Are there disputes as to whether virtual currency should be treated as fiat currency as it relates to financial crimes (e.g., money laundering)?

There are conflicting cases on whether virtual currency should be treated as fiat currency and therefore be used as evidence in criminal prosecutions. Examples include:

- Ross William Ulbricht, founder of Silk Road, a web-based criminal marketplace that enabled users to conduct illegal activity anonymously, operated his website from 2011 through 2013. Silk Road attempted to anonymise its users by using techniques such as an onion router (i.e., encrypted messages passed through a network of servers where each intermediary is only aware of the preceding and following nodes) to disguise IP addresses and utilising a bitcoin-based payment system. Despite efforts to stay hidden, the FBI was able to locate Silk Road's servers, identify users

and ultimately build a case against Ulbricht. Though transactions were conducted in bitcoins, in February 2015, the Manhattan court was able to successfully prosecute Ulbricht on charges of Narcotics Trafficking Conspiracy, Continuing Criminal Enterprise, Computer Hacking Conspiracy and Money Laundering Conspiracy.

- In July 2016, a Miami-Dade Circuit judge ruled that, under Florida law, virtual currency (e.g., bitcoin) is not a fiat currency and dismissed money laundering charges against a defendant who sold bitcoins to undercover detectives who stated their intent to use the bitcoins to purchase stolen credit card numbers.
- In early 2017, the Netherlands suggested proposing laws and regulations to recognise the use of a virtual currency mixer (a mechanism that "mixes" bitcoins to obscure the digital trail/ownership of bitcoins) as money laundering without having to prove a reasonable suspicion of an underlying crime. The Netherlands ultimately decided not to ban the use of virtual currency mixers but to include their use as a high-risk indicator for potentially suspicious activity.

1760. What are the heightened money laundering and terrorist financing risks of virtual currencies and virtual currency systems?

Virtual currencies and virtual currency systems pose heightened ML/TF risk due to the following factors:

- Rise in use in financial crimes (e.g., fraud, identity theft/account takeover, money laundering), especially by transnational criminal organisations
- Rise in use to finance illicit activities, purchase illicit goods and services and receive donations from anonymous donors
- Use of fraudulent methods to "mine" (generate) virtual currencies (e.g., botnets)
- Ease of funds movement across borders
- Lack of transparency (e.g., facilitation of anonymous virtual currency transfers through the use of avatars with fake identities)
- Inadequate screening against applicable sanctions listings (e.g., Office of Foreign Assets Control [OFAC] Sanctions Listings) due to limited or inaccurate user information
- Lack of historical regulatory oversight
- Lack of depth in AML/CFT compliance experience of operators/employees of virtual currency systems, especially those operating in multiple jurisdictions with varying regulatory requirements
- System weaknesses in technological infrastructure of virtual currency systems
- Lack of familiarity/understanding of financial/technical infrastructure and roles of participants of virtual currency systems
- In decentralised systems, the lack of a single administrator inhibits obtaining user and transaction information for further investigation by law enforcement authorities

- User of third-party service providers (e.g., exchangers, wallet providers) further obscures the money trail

1761. Are virtual currency exchangers and administrators required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

Yes. FinCEN has issued multiple guidance on the application of the definition of "money transmitters" and "money transmission services" to virtual currency activities.

A money transmitter is defined as the following:

- Any person engaged in the transfer of funds
- A person who provides money transmission services

"Money transmission services" is defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."

"By any means" includes money transmission through the following:

- A financial agency or institution;
- A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both;
- An electronic funds transfer network; or
- An informal value transfer system (IVTS).

Exchangers and administrators of convertible virtual currencies transfer "value that substitutes for currency to another location or person," and, therefore, fall under the regulatory definition of a money transmitter. As money transmitters, exchangers and administrators of convertible virtual currencies are required to establish AML Programs and comply with other AML/CFT reporting and recordkeeping requirements (e.g., currency transaction reports [CTRs], suspicious activity reports [SARs]).

Other participants using/engaging virtual currencies (e.g., miners, investors, software developers, businesses that rent computer systems for mining) did not fall under the definition of money transmitter. For further guidance, please refer to the FinCEN rulings provided below.

For further guidance, please refer to the Virtual Currency Systems and Participants section.

1762. What guidance has been issued on electronic banking, remote deposit capture, prepaid access, virtual currencies and related topics?

The following are examples of information and guidance that have been issued on electronic banking, remote deposit capture, prepaid access, virtual currencies and related topics:

- **Electronic Banking – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **"E-Banking" and "Emerging Retail Payment Technologies"** within the "Retail Payment Systems" section within the FFIEC Information Technology Examination Handbook by the FFIEC
- **FATF Recommendation 15: New Technologies** (2012) by the Financial Action Task Force (FATF)
- **Consumers and Mobile Financial Services** (2014) by the Board of Governors of the Federal Reserve System
- **Report on Money Laundering Using New Payment Methods** (2012) by FATF
- **Report on New Payment Methods** (2010) by FATF
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** (2010) by the World Bank (WB)
- **The 2008 Survey of Consumer Payment Choice** by the Federal Reserve Bank of Boston
- **Consumer Payment Choice: A Central Bank Perspective** by the Consumer Payments Research Center at the Federal Reserve Bank of Boston
- **Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues** (2010) by the Federal Reserve Bank of Boston
- **Understanding Risk Management in Emerging Retail Payments** (2008) the Federal Reserve Bank of New York
- **Money Laundering in Cyberspace** (2006) by the World Bank (WB)
- Electronic Banking, Remote Deposit Capture, Internet and Mobile Banking Systems and Related Topics:
    - **E-Banking Booklet** (2003) by the FFIEC
    - **"Remote Deposit Capture" within Retail Payment System Overview** (2010) within the FFIEC IT Examination Handbook by the FFIEC
    - **Guidance Addressing Risk Management of Remote Deposit Capture Activities** (2009) by FFIEC
    - **Wolfsberg Guidance on Mobile and Internet Payment Services** (MIPS) (2014) by the Wolfsberg Group of Banks (Wolfsberg Group)
    - **Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions** (2011) by the World Bank (WB)
    - **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by FATF

- **Emerging Risk Forum "Cash, Check, or Cell Phone?" Protecting Consumers in a Mobile Finance World** (2010) by the Federal Reserve Bank of Boston
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** (2004) by the Bank of International Settlements (BIS)
- **Interagency Guidance on Authentication in an Internet Banking Environment** (2005) by the FFIEC
- **Risk Management for Electronic Banking and Electronic Money Activities** (1998) by the Bank for International Settlements (BIS)
- **Mobile Phone Financial Services** (2008) Paper by the WB

- Prepaid Access, Stored Value:
  - **"Prepaid Cards/Stored-Value Cards" subsection within Electronic Cash – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
  - **Application of the Prepaid Access Rule to Closed Loop Prepaid Access Sold or Exchanged in a Secondary Market** (2013) by FinCEN
  - **Application of the Prepaid Access Rule to Bank-Controlled Programs** (2012) by FinCEN
  - **Outreach to the Prepaid Access Industry** (2012) by FinCEN
  - **Frequently Asked Questions Related to Prepaid Access Final Rule** (2011) by FinCEN
  - **Notice of Proposed Rulemaking: Bank Secrecy Act Regulations: Definition of "Monetary Instrument"** (2011) by FinCEN (related to Prepaid Access devices)
  - **Prepaid Cards: Vulnerable to Money Laundering?** (2007) by the Federal Reserve Bank of Philadelphia
  - **The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards** (2008) by the Federal Reserve Bank of Philadelphia
  - **Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs** (2008) by the Network Branded Prepaid Card Association (NBPCA)

- Virtual Currencies:
  - **Guidance for a Risk-Based Approach to Virtual Currencies** (2015) by Financial Action Task Force (FATF)

- **Virtual Currencies: Key Definitions and Potential AML/CFT Risks** (2014) by FATF
- **Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Systems** (2013) by FATF
- **Virtual Currency Schemes** (2012) by the European Central Bank (ECB)
- **Council Framework Decision: Combating Fraud and Counterfeiting of Non-Cash Means of Payment** (2001) by the Council of the European Union
- **Internet Organised Crime Threat Assessment** (IOCTA) (2011, 2014, 2015, 2016) by Europol's European Cybercrime Center (EC3)
- **BitLicense Framework (proposed regulation Title 23, Chapter I, Part 200: Virtual Currencies** (proposed in 2014, finalised in 2015) by the New York State Department of Financial Services (DFS)
- **Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies** (FIN-2013-G001) (2013) by FinCEN
- **Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity** (FIN-2014-R002) (2014) by FinCEN
- **Application of FinCEN's Regulations to Virtual Currency Mining Operations** (FIN-2014-R001) (2014) by FinCEN
- **Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency** (FIN-2014-R007) (2014) by FinCEN
- **Emerging Regulatory, Law Enforcement and Consumer Protection Challenges** (2014) by the U.S. Government Accountability Office (GAO)
- **Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity** (2012) by the Federal Bureau of Investigation (FBI)
- **Cyber Criminal Exploitation of Electronic Payment Systems and Virtual Currencies** (2011) by the FBI
- **Cyber Criminal Exploitation of Real-Money Trading** (2011) by the FBI
- **The Digital Economy: Potential, Perils, and Promises: A Report of the Digital Economy Task Force** (2014) by Thomson Reuters and the International Centre for Missing & Exploited Children

- Financial Inclusion:
  - **Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion** (2013) by FATF in partnership with the World Bank and the Asia/Pacific Group on Money Laundering (APG)

- **Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers** (2014) by the Consumer Financial Protection Bureau (CFPB)
- **Payroll Cards: An Innovative Product for Reaching the Unbanked and Underbanked** (2005) by the Office of the Comptroller of Currency (OCC)

Automated Clearing House Transactions

1763. How has the use of ACH transactions evolved?

ACH transactions are commonly utilised for direct deposits of payroll, government benefits and tax refunds and payments of consumer bills (e.g., mortgages, utility bills, insurance premiums). The most significant growth in the use of ACH transactions has occurred with nonrecurring payments including, but not limited to, the following:

- Accounts receivable conversion (ARC)
- Point-of-purchase (POP)
- Internet-initiated (WEB)
- Telephone-initiated (TEL)
- Re-presented check (RCK) entries

1764. Are ACH transactions limited to domestic payments?

No. ACH transactions can be processed for both domestic and international (cross-border) payments.

1765. What are the heightened money laundering and terrorist financing risks of ACH transactions?

The risks of ACH transactions differ depending on whether the entity is originating, receiving or processing ACH transactions, or outsourcing these activities to a third party.

An ACH transaction may be conducted with a high degree of anonymity, especially since an originator is not obligated to conduct an ACH transaction with a financial institution with which that originator has an account. This increases the product's risk. Additionally, ACH activity permits the originator to execute numerous payments for multiple receivers in one transaction, helping to disguise the source and beneficiary of the movement of funds. This same function of ACH enables large volumes of funds to be moved and can be done very rapidly. As a result, the ability of an individual or entity to hide the source of illicit funds is great with ACH transactions, thus heightening its risk of money laundering and terrorist financing.

1766. Do all ACH transactions pose the same risk?

No. There is increased risk with nonrecurring ACH payments, ACH transactions processed on behalf of high-risk customers (e.g., online gambling operations, payday lenders, mail order and telephone order

companies, adult entertainment businesses), ACH transactions initiated through non-face-to-face methods (e.g., telephone, internet), ACH transactions initiated through third-party payment providers and cross-border ACH transactions.

1767. What is the role of the Electronic Payments Association (formerly known as the National Automated Clearing House Association)?

The Electronic Payments Association (NACHA) issues rules and guidance for acceptable business, operating and risk management practices within electronic payment systems, including the ACH network. NACHA also provides training, facilitates communication between ACH Network members, and acts as a liaison between regulatory and government bodies.

Additional information on NACHA's role and responsibilities is available at http://www.nacha.org/.

1768. Who are the participants in an ACH system?

According to the FFIEC BSA/AML Examination Manual, participants within an ACH system include the following:

- The **originator** is an organisation or person that initiates an ACH transaction to an account either as a debit or credit.
- The **originating depository financial institution (ODFI)** forwards the ACH transaction into the national ACH network through an ACH operator.
- The **ACH operator** processes all ACH transactions that flow between different financial institutions. An ACH operator serves as a central clearing facility that receives entries from the ODFIs and distributes the entries to the appropriate receiving depository financial institution (RDFI).
- The **receiving depository financial institution (RDFI)** receives the ACH transaction from the ACH operators and credits or debits funds from their receivers' accounts.
- The **receiver** is an organisation or person that authorises the originator to initiate an ACH transaction, either as a debit or credit to an account.
- The **gateway operator (GO)** is a financial institution, ACH operator or ODFI that acts as an entry or exit point to or from the United States. A formal declaration of status as a gateway operator is not required. ACH operators and ODFIs acting in the role of gateway operators have specific warranties and obligations related to certain international entries. A financial institution acting as a gateway operator generally may process inbound and outbound debit and credit transactions. ACH operators acting as gateway operators may process outbound debit and credit entries, but can limit inbound entries to credit entries only and reversals.

For international ACHs, the NACHA operating rules define the following two additional participants:

- A **foreign correspondent bank** is defined as a participating depository financial institution (DFI) that holds deposits owned by other financial institutions and provides payment and other services to those financial institutions.

- A **foreign gateway operator (FGO)** acts as an entry point to or exit point from a foreign country.

1769. How many ACH operators exist in the United States?

There are currently two ACH operators:

- **FedACH** is a central clearing facility for transmitting and receiving domestic ACH payments.
    - **Electronic Payments Network (EPN)** is the only private-sector version of the FedACH.
- **FedGlobal** sends cross-border ACH credits payments to more than 35 countries around the world, plus debit payments to Canada only. Both the FedACH and FedGlobal are operated by the Federal Reserve.

1770. What roles can third-party service providers and third-party senders play in the ACH Network?

According to the OCC, a third-party service provider (TPSP) is "an entity other than an originator, ODFI or RDFI that performs any functions on behalf of the originator, the ODFI or the RDFI with respect to the processing of ACH entries. The functions of these TPSPs can include, but are not limited to, the creation of ACH files on behalf of the Originator or ODFI, or acting as a sending point of an ODFI (or receiving point on behalf of an RDFI)."

Third-party senders, a subset of TPSPs, are "bank customers to which originators outsource payment services, but the bank has no direct customer or contractual relationship with the originator. The third-party sender provides services to the originator and, in that capacity, acts as an intermediary between the originator and the ODFI."

1771. Are there specific AML/CFT requirements for ACH transactions and/or ACH operators?

Businesses that function solely as operators of ACH systems/third-party payment processors (per AML/CFT laws and regulations) are currently not required to maintain AML Programs. ACH operators are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, ACH operators are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

However, in order to establish accounts at financial institutions, payment processors already may be required to implement basic AML/CFT controls to mitigate the risks associated with their services.

OFAC has issued very specific regulations with respect to cross-border ACH transactions, formally known as International Automated Clearing House Transactions (IAT). For further guidance, please refer to the Automated Clearing House Transactions and IATs section.

Additionally, participants in some payment systems (e.g., ACH systems, card systems, check collection systems, money transmitting businesses, wire transfer systems) are required to comply with the

Unlawful Internet Gambling Enforcement Act (UIGEA) and Regulation GG. For further guidance, please refer to the Illegal Internet Gambling and Fantasy Sports Wagering section.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. For further guidance on professional service providers, please refer to the Professional Service Providers section.

1772. Does filing an ACH Data Breach Form relieve a financial institution's obligation to file a SAR?

No. The ACH Data Breach Form is designed to identify instances where non-proprietary information (e.g., account numbers) may have been compromised during the processing of an ACH transaction. If the financial institution is required to file SARs, the ACH Data Breach Form would not relieve a financial institution's obligation to file a SAR when potentially suspicious activity has been detected. For further guidance on SARs, please refer to the Suspicious Activity Reports section.

1773. How can ACH activity be monitored for potentially suspicious activity?

Financial institutions should examine ACH transactions for suspicious activity by monitoring for common red flags such as:

- There are high rates of returns/charge-back history (e.g., ACH debit transactions returned for insufficient funds and/or as unauthorised). A high charge-back history is often indicative of merchants processing fraudulent transactions such as unauthorised ACH debits (e.g., customer discontinues a service, therefore stops payment; however, merchant continues to process ACH debits).
- There is significant variance in expected/historical activity versus actual activity in terms of the volume and types of transactions conducted through the account.

Since many financial institutions will not have access to the underlying details of many ACH transactions, they may have to rely on the monitoring conducted by third-party payment processors to detect potentially suspicious activity. As stated above, financial institutions should conduct appropriate due diligence of third-party payment processors at the inception of the relationship, including their due diligence and monitoring programs. For further guidance on red flags, please refer to the Suspicious Activity Red Flags section.

In addition, financial institutions should consider incorporating NACHA's Originator Watch List into their due diligence and monitoring program. Administered by NACHA's Risk Investigations & Services, the Originator Watch List identifies originators and third-party senders that are considered high-risk. Inclusion on the Originator Watch List does not imply any prohibition on initiating entries for entities listed and is only available to employees of financial institutions that utilise the ACH network, regional payments associations and ACH operators. For further guidance on due diligence for third-party payment processors, please refer to the Third-Party Payment Processors section.

1774. Do the CFPB's remittance rules impose additional AML/CFT-related requirements on automated clearing house transactions?

No. The CFPB's remittance rules, which amend Regulation E, are intended to protect consumers who send money electronically to foreign countries by providing more information about the costs of remittances. The rules apply to most international remittances regardless of their purpose, including, but not limited to, funds transfers and automated clearing house (ACH) transactions. Specifically, the rules would require the following:

- Disclosures including:
  - A prepayment disclosure (listing the exchange rate, fees and taxes, and the amount to be delivered abroad) at the time the person initiates; and
  - A receipt disclosure which must be provided to the sender once the payment has been made.
- A provision that consumers can cancel a transfer within 30 minutes (and sometimes more) of originating it;
- Provisions that companies must investigate problems consumers report about transfers and provide standards for error resolutions;
- That companies are made responsible for mistakes made by certain people who work for them; and
- Provisions relating to transfers pre-scheduled on a regular basis.

The rules are applicable to banks, thrifts, credit unions, money transmitters and broker-dealers that consistently execute 100 or more remittance transfers per calendar year and apply to remittance transfers that are more than US$15, made by a consumer in the United States, and sent to a person or company in a foreign country. The rules are effective February 7, 2013, though at the time of the publication of this Guide there continues to be significant industry pressure to delay the implementation given the perceived burden on the industry, particularly smaller institutions. The CFPB has provided model forms as well as an International Funds Transfer Small Entity Compliance Guide; these and other information related to the rules can be found on the CFPB's website at https://www.consumerfinance.gov/policy-compliance/rulemaking.

1775. What key guidance has been issued on ACH activities?

The following are examples of guidance that has been issued on ACH activities:

- **Automated Clearing House Transactions – Overview** (2010) within the FFIEC BSA/AML Examination Manual by the FFIEC
- **Automated Clearing house Activities – Risk Management Guidance** (2006) by the Office of the Comptroller of the Currency (OCC)
- **International ACH Transaction (IAT) Frequently Asked Questions** (2012) by the Federal Reserve Financial Services

- **FedGlobal® Frequently Asked Questions** (2010) by the Federal Reserve Financial Services
- **Guidance to National Automated Clearing House Association (NACHA) on Domestic and Cross-border ACH Transactions** (2004) by OFAC
- **Update on OFAC Requirements for Gateway Operators' Processing of Inbound IAT Debits** (2009) by NACHA
- **NACHA Operating Rule & Guidelines** (2012) by NACHA
- **Comptroller's Handbook: Merchant Processing** (2001) by the OCC
- **FFIEC IT Examination Handbook on Retail Payment Systems** (2006) by the FFIEC

Trust and Asset Management Services

1776. What role can a financial institution play in trust and asset management arrangements?

A financial institution can play multiple roles in trust and asset management arrangements, including, but not limited to, the following:

- Provider of trust and asset management services (e.g., through a separate department or division specialising in these types of service offerings)
- Provider of trust account-types to their customers (e.g., interest only on lawyer trust accounts [IOLTA])
- Provider of financial services to third-party trust and asset management service providers (unaffiliated with the financial institution) who may be subject to their own AML/CFT laws and regulations

The following guidance primarily addresses the risks of trust and asset management services provided directly by the financial institution; however, similar principles apply to customers who provide trust and asset management services.

1777. What are the heightened money laundering and terrorist financing risks of trust and asset management services?

The heightened risk of trust and asset management services lies in the lack of transparency with regard to ownership. Additionally, the privacy and confidentiality adhered to by some trust and asset management service providers can be exploited by criminals.

1778. Do all trust and agency accounts pose the same degree of risk?

Typically, employee benefit accounts and court-supervised accounts are among the lowest risk. Factors that can be used to assess the level of risk associated with trusts include, but are not limited to, the following:

- Type of trust or agency account

- Types, size and frequency of transactions
- Geographic considerations (e.g., country of residence of the principals or beneficiaries, country where the trust was established, origination/destination country of incoming/outgoing funds)
- Relationship with high-risk entities (e.g., politically exposed persons [PEPs], private investment companies [PICs], charitable organisations or other nongovernmental organisations [NGOs])

1779. What are the legitimate purposes for utilising trust and asset management services?

The legitimate reasons for utilising these services may include the following:

- Asset protection
- Estate planning
- Privacy and confidentiality
- Reduction of tax liability

1780. How are "trust accounts" defined?

The FFIEC BSA/AML Examination Manual defines "trust accounts" as legal arrangements in which one party (the trustor or grantor) transfers ownership of assets to a person or financial institution (the trustee) to be held or used for the benefit of others. These legal arrangements include:

- Broad categories of court-supervised accounts (e.g., executorships and guardianships)
- Personal trusts (e.g., living trusts, trusts established under a will, charitable trusts)
- Corporate trusts (e.g., bond trusteeships)

1781. What is the difference between "fiduciary capacity" and "trust"?

"Fiduciary capacity" is more broadly defined than "trust" as it includes the following:

- A trustee, an executor, an administrator, a registrar of stocks and bonds, a transfer agent, a guardian, an assignee, a receiver, or a custodian under the Uniform Gifts to Minors Act
- An investment adviser, if the bank receives a fee for its investment advice
- Any capacity in which the bank possesses investment discretion on behalf of another

1782. How are "agency accounts" defined?

According to the FFIEC BSA/AML Examination Manual, unlike trust arrangements, "agency accounts are established by contract and governed by contract law. Assets are held under the terms of the contract, and legal title or ownership does not transfer to the bank as agent. Agency accounts include custody, escrow, investment management and safekeeping relationships. Agency products and services may be offered in a traditional trust department or through other bank departments."

1783. How are "asset management services" defined?

The FFIEC BSA/AML Examination Manual defines "asset management accounts" as trust or agency accounts that are managed by a financial institution, including, but not limited to, the following:

- Personal and court-supervised accounts
- Trust accounts formed in the private banking department
- Asset management and investment advisory accounts
- Global and domestic custody accounts
- Securities lending
- Employee benefit and retirement accounts
- Corporate trust accounts
- Transfer agent accounts

1784. How are "asset protection trusts" defined?

The FFIEC BSA/AML Examination Manual defines asset protection trusts (APTs) as "a special form of irrevocable trust, usually created (settled) offshore for the principal purpose of preserving and protecting part of one's wealth against creditors. Title to the asset is transferred to a person named as the trustee. APTs are generally tax neutral with the ultimate function of providing for the beneficiaries."

1785. Who are the common participants in a trust?

Common participants in a trust include the following:

- **Trustee** – Person or entity that holds legal title to the trust and is obliged to administer the trust in accordance with both the terms of the trust document and the governing law
- **Trustor/Settlor/Grantor/Donor** – Creator of the trust who entrusts some or all of his or her property to people of his or her choice
- **Beneficiaries** – Beneficial owners of the trust

1786. Who is the customer of the financial institution, the trust or the beneficiaries of the trust?

For the purpose of the CIP rule, the "customer" is the trust that opens the account with the financial institution, whether or not the financial institution is the trustee for the trust.

1787. Should other parties to the trust beyond the account holder be subject to the CIP rule?

Although not currently required, financial institutions should determine the identity of other parties that may have control over the account or have authority to direct the trustee, such as grantors, co-trustees and settlors.

FinCEN's "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) does not amend what financial institutions must collect pursuant to Section 326, but it does expand the parties for which they would be expected to collect information.

Prior to the Beneficial Ownership Rule, covered financial institutions were required to obtain beneficial ownership in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule requires financial institutions currently subject to Customer Identification Program (CIP) requirements to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers. For further guidance, please refer to the Beneficial Owners section.

1788. Since beneficiaries of trusts are not currently subject to verification under the CIP rule, are financial institutions required to screen them against OFAC Sanctions Listings (e.g., Specially Designated Nationals and Blocked Persons List [SDN List])?

Beneficiaries who have a future or contingent interest in funds in an account should be screened against OFAC Sanctions Listings. Some institutions opt to screen beneficiaries at the time funds are transferred as opposed to the inception of the relationship.

Screenings against OFAC Sanctions Listings should be risk-based and consistent with the risk profile of the financial institution.

For additional guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1789. Are financial services companies offering trust and asset management services required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML/CFT requirements to include trust companies and investment advisers. Additionally, in other countries, certain professional service providers are subject to AML/CFT requirements as well. In short, the legal entity type and the types of trust and asset management services offered will dictate the AML/CFT requirements of those businesses offering these services.

For example, a trust company is a corporation organised to perform as the fiduciary of trusts and agencies. Many trust companies are owned by commercial banks and, as such, would be required to comply with the following AML/CFT requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program and conducts an independent review of the AML Program

- Establishment of a Customer Identification Program (CIP)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information sharing (314(a) [mandatory], 314(b) [optional])
- Complying with Special Measures
- Obtaining Foreign Bank Certifications
- Establishing an enhanced due diligence (EDD) program for foreign correspondent account relationships, private banking relationships and politically exposed persons (PEPs)

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to investment providers is provided in the Registered Investment Advisers and Unregistered Investment Companies section. For further guidance on professional service providers, please refer to the Professional Service Providers section.

Interest on Lawyers Trust Account

1790. What is an "Interest on Lawyers' Trust Account"?

An "Interest on Lawyers' Trust Account" (IOLTA) is a bank account that contains funds for various clients held in trust by the attorney where interest earned on the account is ceded to the state bar association or another entity for public interest and pro bono purposes.

1791. What are the heightened money laundering and terrorist financing risks of IOLTAs?

In addition to its association with high-risk professional service providers who may mask the identity of underlying clients, the heightened risk of an IOLTA lies in the commingling of multiple client funds in the IOLTA. This makes it difficult for a financial institution to understand the source and purpose of incoming and outgoing funds. Additionally, since many IOLTA accounts for different attorneys can be assigned the same taxpayer identification number (TIN) (e.g., of the state bar association or another entity for public interest), this makes it difficult to identify activity that may warrant Currency Transaction Report (CTR) and/or Suspicious Activity Report (SAR) filing.

Nondeposit Investment Products

1792. What does the term "nondeposit investment product" mean?

Nondeposit investment products (NDIPs) include various types of investment products (e.g., securities, bonds, fixed or variable annuities, mutual funds) that may be offered by a financial institution directly through proprietary programs with subsidiaries or affiliates, or indirectly through third-party networking arrangements. Third-party networking arrangements may include relationships with third-party financial services corporations (e.g., investment firms, securities broker-dealers, insurance companies) to offer NDIP on the premises of the financial institution. These may include co-branded products and dual-employee arrangements where products are co-sponsored by the financial institution and a third-party institution, or third-party arrangements where a third-party institution leases space from the financial institution to offer its NDIPs independent of the hosting financial institution.

1793. What are the heightened money laundering and terrorist financing risks of NDIPs?

The heightened risk of NDIPs lies in the following:

- Reliance on third parties to conduct adequate due diligence and monitoring for potentially suspicious activity in third-party networking arrangements
- Use of front/shell companies to obscure the beneficial owner
- Large volume of transactions
- Potentially rapid movement of funds

1794. Do all NDIPs pose the same degree of risk?

Third-party networking arrangements pose a greater money laundering and terrorist financing risk than proprietary programs. Additionally, NDIP portfolios managed and controlled directly by customers pose a greater risk than those managed by the financial institution or financial services provider(s).

1795. What steps can a financial institution take to mitigate the risk associated with NDIPs?

To mitigate the risk of NDIPs provided through third-party networking arrangements, financial institutions may consider executing the following at the inception of the relationship and on an ongoing basis:

- Limiting business to financial services corporations with an established relationship with the financial institution or other trusted entity
- Conducting background checks on the financial services corporation and its management team/owners, including a review of all services offered, methods of soliciting new clients, applicable licensing, regulatory obligations, reputation, and history of consumer complaints
- Evaluating whether the service provider's AML/CFT and OFAC Sanctions Compliance Program, when required, is adequate and consistent with the policies of the financial institution

For all NDIPs, financial institutions may consider restricting offerings for certain high-risk products, such as private investment companies (PICs) or other special purpose vehicles (SPVs) located in high-risk jurisdictions and offshore hedge funds, and/or providing high-risk products only to established customers.

1796. Who is responsible for conducting due diligence and monitoring for potentially suspicious activities of NDIPs?

The manner in which the NDIP relationship is structured affects the AML/CFT responsibilities:

- **Co-Branded Arrangements**: AML/CFT responsibilities for completing Customer Identification Program (CIP), customer due diligence (CDD), and suspicious activity monitoring and reporting can vary. Financial institutions should clearly outline each party's contractual responsibilities and ensure compliance by all parties.
- **Dual-Employee Arrangements**: When the dual employee is providing investment products and services from the primary company, the third-party financial services corporation (e.g., investment firm, securities broker-dealer, insurance company) is responsible for monitoring the registered representative's compliance with applicable securities laws and AML/CFT regulations. When the dual employee is providing products or services from the financial institution, responsibility for monitoring the employee's performance and compliance with AML/CFT requirements falls on the financial institution.
- **Third-Party Networking Arrangement**: All AML/CFT responsibilities are assumed by the third-party financial services corporation.
- **Proprietary NDIPs**: All AML/CFT responsibilities are assumed by the financial institution offering the proprietary NDIPs.

1797. How should NDIPs be monitored for suspicious activity?

Financial institutions should examine NDIPs for suspicious activity by monitoring for common red flags such as:

- An account shows an unexplained high level of funds transfer activity with a very low level of securities transactions
- Client deposits or attempts to deposit cash at a financial institution that does not routinely accept cash
- Client takes both a short and a long position in a security or contract for similar amounts and similar expiration dates with no apparent business purpose
- Customer appears to be acting as an agent for an undisclosed third party, but declines or is reluctant to provide information relating to the third party
- Customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account

- Early termination of investment contracts

For a list of red flags related to account activity and transaction executions, please refer to the section Suspicious Activity Red Flags.

1798. Are there specific AML/CFT requirements for financial service corporations offering NDIPs?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML/CFT requirements to include:

- Broker-dealers
- Mutual funds
- Insurance companies

For additional guidance on the AML/CFT requirements of broker-dealers, mutual funds and insurance companies, please refer to the sections: Broker-Dealers in Securities, Mutual Funds and Insurance Companies.

Lending Activities

1799. What types of lending activities have been identified as having heightened money laundering and terrorist financing risks?

Lending activities identified as higher risk exhibit one or more of the following:

- High-risk borrower type (e.g., special purpose vehicle [SPV])
- Complexity (e.g., the involvement of multiple parties: guarantors, signatories, principals, or loan participants who may manipulate the transaction[s])
- Payments made in cash or by third parties
- High frequency of international transactions, and/or historical susceptibility to abuse by criminals.

Examples include, but are not limited to, the following:

- Consumer, commercial and agricultural loans collateralised with cash and/or certificates of deposit (CDs)
- Assets owned by third parties and/or located in foreign jurisdictions
- Commercial and residential real estate
- Trade finance
- Online lending activities

Mortgage fraud, generally defined as any material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan, rose during and after the U.S.

financial crisis of 2007 - 2008. For additional guidance on mortgage fraud, please refer to the Mortgage Fraud section.

1800. What are some examples of due diligence that should be conducted on customers of the aforementioned lending products?

Historically, although more information was collected on lending customers than deposit customers, the due diligence included a review of credit risks but failed to evaluate money laundering and terrorist financing risks. Financial institutions should consider conducting the following due diligence on lending customers:

- Review source of funds used for collateral and/or payments
- Determine if transaction activity is consistent with the nature of the customer's business and the stated purpose of the loan

1801. How can lending activities be monitored for potentially suspicious activity?

Financial institutions should examine lending activities for suspicious activity by monitoring for common red flags such as:

- Early repayment of a loan in currency or monetary instruments (particularly for problem loans)
- Unexpected payments to cure past due status
- Structured payments of loans in currency or monetary instruments
- Disbursement of loan proceeds via structured currency withdrawals or monetary instruments
- Disbursement of loan proceeds to a third party
- Third-party payment of a loan
- Unwillingness to provide information about the purpose of the loan and/or source of repayment and/or collateral

For additional guidance on red flags, please refer to the sections: Lending Red Flags, Mortgage and Real Estate Red Flags, Credit Card Red Flags, and Trade Finance Red Flags.

1802. What due diligence should financial services companies consider when they provide services to other lenders?

For providers of lending products, the following due diligence should be conducted:

- Limiting business to service providers with an established relationship with the financial institution or other trusted entity
- Conducting background checks on service providers, including a review of all services offered, methods of soliciting new clients, applicable licensing, regulatory obligations and reputation
- Restricting services for certain high-risk customer types, such as non-resident aliens (NRAs) or politically exposed persons (PEPs), or customers located in high-risk jurisdictions

- Evaluating whether the service provider's AML/OFAC Compliance Program is adequate and consistent with the policies of the financial institution

1803. Are there specific AML/CFT requirements for nonbank lenders and/or other participants in the lending process?

FinCEN has issued or proposed rules for the following participants:

- Housing Government-Sponsored Enterprises (GSEs) (e.g., Federal National Mortgage Association [Fannie Mae], Federal Home Loan Mortgage Corporation [Freddie Mac], Federal Home Loan Banks [FHL Banks])
- Persons involved in real estate settlements and closings (e.g., real estate brokers, attorneys representing buyers/sellers, title insurance companies, escrow agents, real estate appraisers)

Housing GSEs are required to establish AML Programs, file suspicious activity reports (SARs) and comply with other AML/CFT requirements.

The 2003 proposed rulemaking for persons involved in real estate settlements and closings has yet to be finalised. Although not required to establish an AML Program, they are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, they are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

Together, these regulations, along with the requirements for RMLOs, are expected to increase the number of SAR filings from the mortgage industry and provide regulators and law enforcement with more information on mortgage fraud.

For further guidance, please refer to the Nonbank Residential Mortgage Lenders and Originators, Housing Government-Sponsored Enterprises and Persons Involved in Real Estate Closing and Settlements sections.

Some of the above are considered "professional service providers" who/that act as an intermediary between a client and a third-party financial institution who/that may conduct or arrange for financial dealings and services on their client's behalf (e.g., management of client finances, settlement of real estate transactions, asset transfers, investment services, trust arrangements). For additional guidance, please refer to the Professional Service Providers section.

1804. What AML/CFT guidance has been issued on lending activities?

Examples of key guidance on lending activities include the following:

- **Lending Activities – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **An OFAC Primer for the Real Estate Settlement and Title Insurance Industry** (2003) by the Office of Foreign Assets Control (OFAC)

- **SRC Insights: From the Examiner's Desk: Suspicious Activity Monitoring in the Lending Function** (2011) by the Federal Reserve Bank of Philadelphia
- **RBA Guidance for Real Estate Agents** (2008) by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing Through the Real Estate Sector** (2007) by FATF
- **Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis** (2008) by the Financial Crimes Enforcement Network (FinCEN)

Insurance Products

1805. What types of insurance products have been identified as having increased money laundering and terrorist financing risks?

The following insurance products have been identified as higher ML/TF risk because they exhibit one or more of the following: complexity (e.g., the involvement of multiple parties: guarantors, signatories, beneficiaries, or professional service providers who may manipulate the transaction[s]), ability to transfer value without the knowledge of the issuer, payments made in cash or by third parties, high frequency of international transactions, and/or historical susceptibility to abuse by criminals:

- Permanent life insurance policies, other than group life insurance policies
- Annuity contracts, other than group annuity contracts
- Any other insurance products that have cash value or investment features

1806. Are there specific AML/CFT requirements for financial services companies offering these types of insurance products?

The USA PATRIOT Act expanded the definition of "financial institutions" subject to AML/CFT requirements to include insurance companies offering the aforementioned covered products. The definition of insurance company currently excludes group insurance products, term (including credit), life, title, health, and many property and casualty insurers. It also excludes products offered by charitable organisations (e.g., charitable annuities), as well as reinsurance and retrocession contracts. It also excludes entities that offer annuities or other covered products as an incidental part of their business.

For additional guidance on the AML/CFT requirements of insurance companies, please refer to the Insurance Companies section.

1807. How do the U.S. AML/CFT measures for insurance products correspond to FATF Recommendations?

FATF Recommendation 10 – Customer Due Diligence suggests financial institutions offering insurance products and services (including intermediaries such as agents and brokers) implement measures to guard against money laundering and terrorist financing (e.g., conduct due diligence on beneficiaries of

life or other investment-related insurance business). Simplified measures can be applied toward low-risk insurance products (e.g., life insurance policies with annual premiums less than US/EUR 1,000, single premiums of less than US/EUR 2,500).

While U.S. AML/CFT requirements are narrower in scope, covered U.S. insurance companies are required to establish AML Programs, report potentially suspicious activities and comply with other BSA requirements as detailed further below.

1808. Who is responsible for conducting due diligence and monitoring for potentially suspicious activities of insurance products?

The manner in which the insurance products are offered affects the AML/CFT responsibilities.

- **Co-Branded Arrangements** – AML/CFT responsibilities for completing Customer Identification Program (CIP), customer due diligence (CDD), and suspicious activity monitoring and reporting can vary. Financial institutions should clearly outline each party's contractual responsibilities and ensure compliance by all parties.
- **Dual-Employee Arrangements** – When the dual employee is providing investment products and services from the insurance company, the insurance company is responsible for monitoring the registered representative's compliance with applicable securities laws and AML/CFT regulations. When the dual employee is providing products or services from the financial institution, responsibility for monitoring the employee's performance and compliance with AML/CFT requirements falls on the financial institution.
- **Third-Party Networking Arrangement** – The insurance company assumes all AML/CFT responsibilities.
- **Proprietary Insurance Products** – The financial institution offering the proprietary insurance products assumes all AML/CFT responsibilities.

1809. How can insurance products be monitored for potentially suspicious activity?

Financial institutions should examine insurance products for potentially suspicious activity by monitoring for common red flags such as:

- Customer's lack of concern with the cost of the policy
- Customer's lack of concern with the performance of an insurance product
- Customer's lack of concern with the penalties/fees
- Large single-payment premiums for life and annuity policies
- Unusual methods of payment, particularly cash or cash equivalents

For additional guidance, please refer to the sections: Suspicious Activity Red Flags and Insurance Products Red Flags.

1810. What guidance has been issued on insurance companies and covered products?

The following are examples of key guidance that has been issued:

- **Insurance – Overview within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual** by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 10 – Customer Due Diligence** (2012) by FATF
- **Frequently Asked Questions: Customer Identification Programs and Banks Serving as Insurance Agents** (2006) by FinCEN
- **Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings** (2010) by the Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions from the Insurance Industry** (2012) by the Office of Foreign Assets Control (OFAC)
- **Risk-Based Approach for the Life Insurance Sector** (2009) by the Financial Action Task Force (FATF)
- **Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism** (2004) by the International Association of Insurance Supervisors (IAIS)
- **Anti-Money Laundering Guidance Notes** (2003) by the IAIS

Know Your Customer's Customer

1811. What is a third-party transaction?

A third-party transaction is defined as a transfer of funds to/from the account holder to/from an individual/entity that is different than the customer/account holder. It includes all types of transactions (e.g., wires, checks), regardless of direction (i.e., incoming, outgoing). "Third party" distinguishes the recipient/sender of the funds from the account holder. The individual/entity also can be a customer of the same financial institution, although the risk is greater when the individual/entity is not a customer of the financial institution, as the latter was not subject to the same customer acceptance procedures. Examples of third-party transactions are provided below:

- **Example 1**: Customer John sends a wire to beneficiary Jane from his deposit account. The deposit account allows third-party activity.
- **Example 2**: Customer John establishes a loan with Bank ABC and wishes to disburse the proceeds of the loan to his business partner, Jane. The financial institution's policy does not allow loan proceeds to be disbursed to a third party, as Jane is a third party.
- **Example 3**: Customer John established a certificate of deposit (CD) account with Bank ABC and wishes to liquidate the CD and disburse the funds to his wife, Jane. The financial institution's policy does not allow funds from the CD to be disbursed to a third party.

- **Example 4:** Correspondent bank (respondent bank) established a payable-through account (PTA) and either conducts transactions on behalf of its customers or allows customers to conduct transactions directly through the PTA. The customer's customers are third parties.

1812. Are financial institutions expected to conduct due diligence on their customers' customers?

While there is no U.S. law or regulation that requires it, in certain situations (e.g., where a financial institution provides clearing services for a correspondent), financial institutions may be expected to demonstrate an understanding of their customers' customers. This may be accomplished by conducting due diligence directly or indirectly by requesting information from the correspondent banking customer (e.g., respondent). This policy is known as Know Your Customer's Customer (KYCC).

Due to the uncertainty around KYCC, many financial institutions have opted to de-risk by terminating high-risk correspondent accounts instead of managing the high compliance burden of such relationships. To counter de-risking activities, several agencies (e.g., U.S. federal banking regulators) have issued guidance that KYCC is not required under current AML/CFT laws and regulations.

For further guidance on due diligence requirements for correspondent banking, please refer to the sections: Correspondent Banking and Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts. For further guidance on de-risking, please refer to the Risk Assessments section.

Know Your Employees

1813. Should CDD and EDD standards for customers be applied to the employees of financial institutions as well?

In addition to screening new employees during the standard hiring process, financial institutions should consider conducting ongoing due diligence and EDD on employees in positions perceived to have greater exposure to money laundering (e.g., relationship managers of private banking or institutional clients). Additionally, the history of an employee's investigations and reports of potentially suspicious activity should be noted. For instance, a general reluctance to report suspicious activity should serve as a red flag to an institution to monitor closely client relationships associated with the employee in question. A financial institution should consult with its counsel on how to conduct such due diligence and to help ensure labour laws are not violated.

Knowing both customers and employees and creating a strong internal referral and transaction monitoring (as allowed by law) system for potentially suspicious activity will help mitigate the risk of a financial institution being used for money laundering or terrorist financing.

1814. Should CDD and EDD exceptions be made for senior management or owners of the financial institution?

No. CDD and EDD standards should be applied to all employees of a financial institution, regardless of status or position within the financial institution.

1815. What additional risks do employees of the financial institution pose?

As a result of their access, employees pose considerable risks related to insider abuse (e.g., the ability to override or manipulate CTRs and SARs, the utilisation of knowledge regarding the AML/CFT policies and procedures to evade controls designed to prevent money laundering and terrorist financing).

Accordingly, CDD and EDD standards should be applied to all employees of a financial institution, regardless of status or position within the financial institution.

1816. Should a financial institution file a Suspicious Activity Report (SAR) on insider abuse?

Yes. SAR regulations specifically require the filing of SARs on insider abuse. For further guidance, please refer to the Suspicious Activity Reports section.

Know Your Third Parties

1817. Apart from customers and employees, are there other parties whose performance could jeopardise an AML/CFT Compliance Program?

Yes. The following parties, among others, could jeopardise an AML/CFT Compliance Program:

- **Other financial institutions relied upon to support the AML/CFT Compliance Program** (e.g., Customer Identification Program [CIP], sanctions screening) may not adequately execute their AML/CFT or OFAC sanctions review and responsibilities consistent with regulatory and/or internal standards.
- **Companies providing products/services, such as insurance products, to the financial institution's customers** may not identify risk or monitor activity adequately for potentially suspicious activity.
- **Companies that offer a financial institution's products to its customers and employees**, such as prepaid access program managers, may not adequately oversee the AML Program and internal controls.
- **Companies, such as deposit brokers or registered representatives, referring customers to a financial institution** may not conduct adequate due diligence on acquired customers.
- **Third-party payment processors (TPPPs)** (e.g., ACH network providers, ATM network providers, remote deposit capture [RDC] service providers, gateway processors) may not identify and manage AML/CFT risks appropriately.
- **Agents** of money services businesses (MSBs) may not appropriately manage AML/CFT risk and may expose an MSB to reputational risk as well as legal risk.
- **Vendors** (e.g., AML/CFT technology providers, courier services, consultants conducting independent tests of the AML/CFT Compliance Program) may provide products/services that fail to meet a financial institution's requirements or needs.

1818. What can financial institutions do to mitigate third-party risk?

Financial institutions should conduct due diligence and ongoing monitoring of third-party relationships to mitigate third-party risk, including, but not limited to, the following:

- Limiting business to service providers that have an established relationship with the financial institution or other trusted entity or are referred from highly respected sources
- Conducting background checks on service providers, including a review of all products/services offered, methods of soliciting new clients, licensing, regulatory obligations and reputation (e.g., customer complaints)
- Performing sanctions screening on service providers, their owners and principal officers
- Reviewing the AML/CFT Compliance Program, where applicable, for adequacy and consistency with internal policies and procedures (e.g., due diligence and monitoring conducted on acquired customers, merchants, agents)
- Monitoring activity originated from the third party, where applicable, for common red flags or potentially suspicious activity that may suggest inattention or inadequacies in the third party's own compliance program or contractual obligations

For further guidance on managing third-party risk, please refer to the following sections: Nondeposit Investment Products, Deposit Brokers, Third-Party Payment Processors, Owners/Operators of Privately Owned Automated Teller Machines (ATMs), Remote Deposit Capture, Agents of MSBs and Anti-Bribery and Corruption Compliance Programs.

1819. Can a financial institution rely upon a third party to conduct all or part of the financial institution's CIP?

A financial institution may rely on another federally regulated institution to conduct all or part of the financial institution's Customer Identification Program (CIP). Such reliance is permitted only when all of the following apply:

- Such reliance is reasonable.
- The other financial institution is regulated by a federal functional regulator.
- The other financial institution is subject to an AML/CFT program, reporting and recordkeeping requirements.
- The other financial institution shares the customer with the financial institution.
- The two institutions enter into a reliance contract.

1820. What obligations are imposed upon third parties that conduct part or all of the financial institution's CIP?

The financial institution conducting the CIP must provide an annual certification that it has implemented its AML/CFT Compliance Program and that it will perform (or its agent will perform) the specified requirements of the financial institution's CIP.

For additional guidance on CIP, please refer to the Section 326 – Verification of Identification section.

1821. Can financial institutions rely on third parties for other elements of an AML/CFT Compliance Program beyond CIP (e.g., suspicious activity reporting)?

Financial institutions may outsource other elements of their AML/CFT Compliance Programs (e.g., monitoring, collection and verification of customer information, OFAC screening, 314(a) searches) to third parties (e.g., car dealers who accept loan applications on behalf of a bank or technology service providers). In these instances, financial institutions cannot rely on the third parties in the same manner as they may if they delegate elements of their CIP programs to regulated financial institutions. Rather, financial institutions that do outsource parts of their AML/CFT Compliance Program to a third party must do the following:

- Ensure they have obtained a written agreement for the services to be performed by the service provider and that the terms of the agreement meet the financial institution's requirements.
- Monitor the third party's performance under the contract on a continuing basis.
- Conduct adequate due diligence on the third party's AML/CFT Compliance Program and/or its understanding of AML/CFT requirements.
- Perform adequate due diligence of the third party's operations on a periodic basis.

It is important to note that the institution is ultimately responsible for its compliance with AML/CFT requirements, whether or not it relies upon a third party.

1822. Should third-party service providers be included in the independent testing of a covered financial institution's AML/CFT Compliance Program?

Yes. The independent test should consider how the covered financial institution conducted its due diligence of third party service providers and how it assures itself that the third party is meeting its obligations effectively on a continual basis.

1823. What guidance has been issued on third-party service providers (TPSP)?

The following are examples of guidance that has been issued on third-party service providers:

- **Third-Party Payment Processors – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 17: Reliance on Third Parties** (2012) by the Financial Action Task Force (FATF)
- **Risks Associated With Third-Party Payment Processors** (2012) by FinCEN
- **Revised Guidance on Payment Processor Relationships** (2012) by the Federal Deposit Insurance Corporation (FDIC)

- **Retail Payment Systems** and **Wholesale Payment Systems Booklet** (2004) within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Third-Party Senders and the ACH Network: An Implementation Guide** (2012) by the Electronic Payments Association (NACHA) (formerly National Automated Clearing House Association)
- **Bank Use of Foreign-Based Third-Party Service Providers** (2002) by the Office of the Comptroller of the Currency (OCC)
- **Risk Management Principles for Third-Party Relationships** (2001) by the OCC
- **Payment Processor Relationships** (2012) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance on Managing Third-Party Risk** (2008) by the FDIC

TRANSACTION MONITORING, INVESTIGATIONS AND RED FLAGS

Monitoring Process

1824. What does the term "monitoring" mean with regard to detecting potentially suspicious activity?

Monitoring is a general term used to describe processes designed to detect and identify potentially suspicious activity.

Monitoring is not limited to reviews of transaction activity. Potentially suspicious activity can be detected in other types of customer activities (e.g., provision of fraudulent or inaccurate documentation during account opening, enhanced due diligence reviews).

Monitoring should be risk-based and ongoing.

1825. What is "suspicious activity"?

Generally, "suspicious activity" refers to unusual activity that a financial institution suspects may be connected to illicit activity (e.g., predicate crimes), violations of the BSA, or activities with no lawful or understandable purpose. BSA regulations outline the following types of potentially suspicious activities that should be reported on a Suspicious Activity Report (SAR) by depository institutions:

- Insider abuse involving any amount;
- Violations aggregating to US$5,000 or more where a suspect can be identified;
- Violations aggregating to US$25,000 or more regardless of a potential suspect;
- Transactions aggregating to US$5,000 or more that involve potential money laundering or violations of the BSA; or
- Unauthorised electronic intrusion.

For further guidance, please refer to the Suspicious Activity Reports section.

1826. Which types of "predicate crimes" give rise to a charge of money laundering?

Although money laundering is often equated with drug trafficking, the proceeds of many crimes can be associated with money laundering. The United States, as an example, lists hundreds of specified unlawful activities (SUAs) including the following partial listing:

- Racketeering activity (e.g., any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter, or dealing in a controlled substance or listed chemical as defined by the Controlled Substances Act), which is chargeable under state law and punishable by imprisonment for more than one year;
- Terrorist financing;

- Counterfeiting (e.g., currency, goods);
- Fraud (e.g., securities fraud, wire fraud);
- Slavery, trafficking in persons and alien smuggling;
- Illegal arms sales (e.g., chemical weapons, nuclear material); and
- Illegal gambling.

These SUAs are consistent with those suggested by the Financial Action Task Force (FATF). For further guidance, please refer to the section Key FATF Definitions with Comparisons to U.S. Definitions.

1827. Is a financial institution required to identify the underlying predicate crime of potentially suspicious activity?

No. A financial institution is required to report suspicious activity that may involve illicit activity; a financial institution is not obligated to determine, confirm or prove the underlying predicate crime (e.g., terrorist financing, money laundering, identity theft, wire fraud). The investigation of the underlying crime is the responsibility of law enforcement.

When investigating potentially suspicious activity, financial institutions should, to the best of their ability, describe the suspicious activity.

It is helpful for those responsible for conducting investigations in a financial institution to have a basic understanding of certain crimes to assist in detecting and reporting relevant information to law enforcement. Additional guidance on select predicate crimes have been provided in the following sections:

- Drug Trafficking
- Terrorism and Terrorist Financing
- AML/CFT and Anti-Fraud Programs
- Mortgage Fraud
- Identity Theft and Identify Theft Prevention Program
- Cyber Events and Cybersecurity
- Elder Financial Abuse
- Anti-Corruption and Bribery Compliance Program
- Offshore Tax Evasion, Voluntary Tax Compliance and Foreign Account Tax Compliance Act
- Human Trafficking and Migrant Smuggling
- Illegal Internet Gambling and Fantasy Sport Wagering

1828. Are financial institutions required to notify law enforcement of potentially suspicious activity beyond the filing of a SAR?

Under certain circumstances, financial institutions are expected to notify law enforcement or a regulatory authority of activities including, but not limited to, the following:

- Terrorist activity
- Cyber attacks
- Sanctions evasion

FinCEN and OFAC have established hotlines for financial institutions in an effort to stop ongoing criminal activity related to the aforementioned. For further guidance, please refer to the Suspicious Activity Reports section.

1829. What are some of the key considerations, beyond adequate staffing, that financial institutions should consider when designing their transaction monitoring programs?

A financial institution should consider the following non-exhaustive objectives:

- Complying with AML/CFT laws and regulations:
  - Bank Secrecy Act (BSA) Suspicious Activity Report (SAR) requirements
  - Office of Foreign Assets Control (OFAC) sanctions embargoes
  - State-level AML/CFT laws and regulations such as the New York State Department of Financial Services (NYDFS) Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications
- Incorporating international standards, including, but not limited to, the following:
  - Financial Action Task Force (FATF) Recommendations
  - Wolfsberg Anti-Money Laundering Principles for Correspondent Banking (2014)
  - Wolfsberg Anti-Money Laundering Principles for Private Banking (2012)
- Aligning the transaction monitoring program with the institution's own AML risk assessment
- Understanding technology available (and the limitations thereof) to monitor customer transaction activity including both internal and third-party solutions
- Understanding the extent to which public data sources can be used to obtain reliable information to support monitoring and investigation processes

1830. How does the Financial Action Task Force (FATF) address monitoring?

FATF's use of the term "monitoring" includes the following types of activities:

- Monitoring customer transactions for potentially suspicious activity

- Monitoring business units for day-to-day compliance with AML/CFT policies and procedures by financial institutions
- Monitoring financial institutions for compliance with AML/CFT laws and regulations by competent authorities

The following FATF Recommendations suggest measures, and in some instances, enhanced monitoring for higher-risk customer types and activities:

- Recommendation 10 – Customer Due Diligence
- Recommendation 12 – Politically Exposed Persons
- Recommendation 13 – Correspondent Banking
- Recommendation 16 – Wire Transfers
- Recommendation 14 – Money or Value Transfer Services
- Recommendations 22 and 23 – DNFBPs: Customer Due Diligence and Other Measures
- Recommendation 8 – Non-profit Organisations
- Recommendation 19 – Higher-risk Countries
- Recommendation 29 – Financial Intelligence Units (e.g., large cross-border and domestic movement of currency)
- Recommendation 32 – Cash Couriers
- Recommendation 36 – International Instruments

FATF Recommendation 20 – Reporting of Suspicious Transactions specifically recommends financial institutions be required by law to report suspicious transactions involving funds derived from all predicate offenses for money laundering through suspicious transaction reports (STRs) to its financial intelligence unit (FIU).

For further guidance on suspicious activity reporting requirements, please refer to the Suspicious Activity Reports section. For further guidance on international standards, please refer to the Financial Action Task Force section.

1831. What protocols should a financial institution establish when developing its suspicious transaction monitoring program?

A financial institution's suspicious transaction monitoring process is often dictated by its suspicious activity monitoring software solution. Once a technology solution has been implemented, financial institutions should establish the following monitoring protocols:

- Assignment of alerts (e.g., by manager, by risk score, by self-assignment)
- Time frames for conducting reviews (e.g., review automated alerts within 30 days of generation, filing of SARs within 30 days from the date of detection), and appropriate tracking and reporting procedures to detect any backlogs

- Prioritisation and escalation of cases
- Documentation standards (e.g., supported reasoning for cleared alerts, appropriate use of a case management system, effective use of the internet) that cover the "Five W's":
    - Who conducted the activity?
    - What instruments were used?
    - Where did the activity occur?
    - When did the activity occur?
    - Why is the activity suspicious or not suspicious?
- Quality assurance procedures (e.g., secondary review of select alerts, cases and SARs filed)
- Law enforcement notification, if required

1832. How can a financial institution utilise a risk-based approach to its suspicious transaction monitoring program?

Regulators expect that financial institutions use the results of their AML/CFT risk assessments (e.g., horizontal risk assessment, line of business/legal entity risk assessment, product/service risk assessment, geographic risk assessment, customer risk assessment) as factors in determining the appropriateness of their suspicious transaction monitoring programs. New York State Department of Financial Services (DFS) "Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certifications" explicitly requires that covered financial institutions demonstrate the linkage between their risk assessments and their transaction monitoring programs to meet transaction monitoring program compliance standards.

Some financial institutions assign more resources (e.g., staff, monitoring reports, monitoring system enhancements) to higher-risk products, geographies and lines of business (as assigned during the financial institution's line of business/legal entity risk assessment process). In addition, many financial institutions adjust monitoring thresholds based upon a customer's risk level (as assigned during the financial institution's customer risk assessment process) to place more scrutiny on higher-risk customers.

Some suspicious activity monitoring software solutions also include a feature that allows financial institutions to risk rate or prioritise alerts to enable prioritisation (e.g., assignment of high risk or more complex alerts to more seasoned investigators).

1833. What is a "profile" and how can financial institutions develop a profile to help identify unusual or potentially suspicious activity?

Many financial institutions, during the account opening process, ask for the customer's expected activity (e.g., products, geographic locations, frequency, dollar volume), as one component of a customer's profile. The financial institution should, however, review this expected transaction profile for appropriateness (e.g., comparison against expectations for customer's occupation and salary/business and revenue).

When developing profiles for existing customers, many financial institutions use historical data once they have determined that this data is indeed reasonable and appropriate for the customer. As mentioned earlier, the financial institution should review the profile created using historical data with the institution's expectations for the customer.

FinCEN's final rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) defines "customer risk profile" as "the information gathered about a customer to develop the baseline against which customer activity is assessed for suspicious transaction reporting." While the Beneficial Ownership Rule does not explicitly require covered financial institutions to risk rate each customer and update this profile on an on-going basis, it does expect institutions to understand the ML and TF risks posed by their customers and be able to demonstrate their understanding.

Overall, the profile is expected to include information gathering during onboarding and throughout the customer relationship, on a periodic and event-driven basis against which customer activity will be reviewed for potentially suspicious activity.

1834. Are financial institutions required to link "customer risk profiles" into their automated transaction monitoring systems?

Federal and some state regulators have made clear their positions that customer profiles are foundational to an effective transaction monitoring program. Therefore, it is important that financial institutions be able to evidence clearly how customer profiles are used to inform transaction monitoring systems and that analysts have ready access to customer profiles to support the monitoring and investigation processes.

1835. Should all transactions and customers be monitored for potentially suspicious activity?

Yes. All transactions and customers should be subject to monitoring, but the extent, nature and frequency of monitoring should be risk-based. Financial institutions should periodically take an inventory of all products and services offered by the institution and determine how each of the products is monitored to identify unusual or potentially suspicious activity. In addition, the financial institution should have a mechanism in place to ensure newly added products and services are incorporated into the monitoring process; this usually is accomplished through compliance representatives participating in new product development committees.

1836. Should all transactions and customers be monitored in a similar fashion?

No. A "one-size-fits-all" approach is usually insufficient when trying to identify unusual or potentially suspicious activity. Financial institutions should, when identifying all of the products and services offered (as outlined above), also identify where the transaction activity and customer profile information are stored. This exercise should identify the format, location, content and quality (e.g., level of detail, completeness, usefulness) of the electronically stored data. This exercise also should include identification of non-electronic sources of information (e.g., customer files maintained by relationship managers, letters of credit files). The factors identified during this exercise will impact the

way in which the transactions can be monitored (e.g., through automated monitoring systems, through manual monitoring reports, with support from customer information).

1837. What is an "alert"?

An alert is a potential indicator of unusual or potentially suspicious activity based on various factors, such as expected activity thresholds, account history, customer types, product types and geography.

1838. What is a cross channel alert?

A cross channel alert involves the sharing of information between groups that has utility for all involved groups (e.g., AML/CFT and anti-fraud units).

1839. In addition to alerts produced through suspicious activity monitoring software and manual monitoring, how else might a financial institution become aware of potentially suspicious activity?

An institution may become aware of potentially suspicious activity through the following:

- Internal referrals from business units performing real-time transaction monitoring or with direct customer contact;
- Whistleblower programs;
- 314(a)/(b) requests;
- Subpoenas;
- National Security Letters (NSLs);
- The media (e.g., radio, television, newspaper);
- Regulatory updates released by FinCEN or other applicable agencies;
- Reports from third parties such as credit reporting agencies or negative database operators (e.g., check fraudsters, charge-offs).

1840. On what level should transactions be monitored for potentially suspicious activity (e.g., account, customer)?

Transactions should be monitored on a customer level in order to follow properly the money trail when conducting an investigation. Monitoring rules/parameters can be applied on different "levels" to detect potentially suspicious activity:

- **Transaction level** (typically driven by type/code [e.g., cash, wire] and date[s] and amount[s] of the transaction)
- **Account level** (typically driven by account type, such as checking, savings or loan)
- **Customer level** (typically driven by aggregate transactions/profiling on a taxpayer identification number [TIN] level or other number used to uniquely identify a customer)

- **Household level** (typically an entity consisting of two or more distinct customers who share a common factor such as an address, phone number or business owner; similar to related accounts on a customer level, but on a broader level involving two or more parties)
- **Geographic level** (typically driven by higher-risk geographic locations or unusual patterns of activity in particular locations)

A strong suspicious transaction monitoring program may include monitoring on a combination of levels. Factors that may determine the level of monitoring include available customer information and specific capabilities of the transaction monitoring software utilised by the financial institution.

1841. Is it enough for financial institutions to monitor on a customer level?

While it's common to monitor on a customer level, as criminals grow increasingly sophisticated in their laundering schemes, there's an expectation that financial institutions consider both explicit and underlying relationships in their suspicious activity monitoring programs, including, but not limited to, accounts linked through transaction activity.

In July 2016, FinCEN issued the "Customer Due Diligence Requirements for Financial Institutions" final rule (Beneficial Ownership Rule) that requires financial institutions currently subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers.

Previously, covered financial institutions were required to obtain beneficial ownership information in the following situations as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

As criminals use legal arrangements (e.g., trusts, private investment companies [PICs]) and straw men to disguise their interests, it is becoming increasingly important to conduct monitoring beyond the nominal customer.

For further guidance on the final rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

1842. Who should perform suspicious transaction monitoring?

Individuals who either deal directly with customers or process customer transactions are in the best position to perform effective suspicious transaction monitoring on a real-time basis. Within an organisation, these individuals tend to know the most about the customers and their typical patterns of transaction activity. In addition, many financial institutions have developed centralised investigative

units, which are responsible for reviewing alerts generated by the suspicious transaction monitoring program in place.

1843. How can technology be used to support a financial institution's suspicious transaction monitoring program?

Much has been written about the use of AML/CFT technology to support a financial institution's suspicious transaction monitoring efforts. Technology can be used, for example, to support:

- Monitoring for suspicious transactions and facilitating SAR filings
- Storage of customer information (e.g., CIP, due diligence [DD], enhanced due diligence [EDD])
- Calculation of customer risk ratings
- Searching against special lists of prohibited and/or high-risk individuals/entities (e.g., Office of Foreign Assets Control [OFAC], 314(a), subpoenas, media searches, internal "deny" lists, politically exposed persons [PEPs]) for customers and transactions
- Case management

For further guidance on AML/CFT technology, please refer to the sections: Monitoring, Investigating and Filing of Suspicious Activity Reports (SARs), Customer and Transaction List Screening, KYC Process and Risk Assessment Automation.

1844. How is transaction monitoring conducted in institutions that do not have suspicious activity monitoring software?

It would be unusual in the current environment for an institution not to have an automated monitoring system. However, institutions that do not have automated systems and/or that need to supplement their automated systems often use reports from various internal systems that may be generated for other purposes. For example, reports on loan prepayments, currency activity, funds transfers, nonsufficient funds, large items, significant balance changes, monetary instruments and closed deposit accounts are commonly generated by institutions for management reporting and business development purposes, and reports on off-market transactions are produced to monitor trading activity. The information included within these reports also could be invaluable for AML/CFT monitoring.

Though institutions should maximise the efficiency of transaction monitoring by utilising existing reports, additional reports and review procedures may be required to ensure all of an institution's transactions are being captured in its monitoring efforts. Periodic transaction-monitoring reports may include, but are not limited to, cash and wire transactions that exceed a predetermined amount, check transactions, loan payments and prepayments, and closed deposit accounts. Employees in high-risk areas, such as trade finance and correspondent banking, should receive in-depth and customised training on the identification of potentially suspicious activity and red flags because, to a large extent, these areas involve real-time manual monitoring by those employees.

1845. Why would institutions with automated monitoring systems create manual monitoring reports?

As sophisticated as technology has become, it often does not provide all the monitoring necessary to cover all customer types and products, services and transactions offered by a financial institution. Reasons for creating manual monitoring reports generally include data issues or a need for more enhanced methods of detection. Common examples include, but are not limited to, the following:

- Certain customer types (e.g., trusts) or transaction processing (e.g., loan payments) are processed on different platforms
- Products with red flags cannot be monitored by an automated system (e.g., trade finance)
- Clearing or omnibus accounts require more drill-down than single customer accounts
- Activities, such as human trafficking, require data analytics and not just traditional transaction monitoring

1846. How can a financial institution incorporate the use of the media into its monitoring system?

Many AML/CFT compliance departments subscribe to news services offered by some of the major search engines and list providers and/or designate personnel to screen local and national news sources on a continual basis for information that may link customers to money laundering and terrorist financing, and to conduct investigations for any matches.

For further guidance, please refer to the AML/CFT Technology section.

1847. What is a "look back"?

A look back is a regulator or self-directed review performed for a certain period and/or of certain types of accounts or transactions to identify any usual or potentially suspicious activity that may have been previously overlooked. Regulators may require that a look back be performed if they conclude that a financial institution has a poorly designed or implemented transaction monitoring program. Self-directed look backs are often performed when a financial institution identifies a pattern of unusual or potentially suspicious activity and decides that it should conduct a more in-depth review to determine when the activity began and how pervasive it has been.

1848. Are there lessons that can be learned from look backs that have been performed at financial institutions?

Look backs can be costly, time-consuming and disruptive to day-to-day business. Among the important lessons learned, especially relating to regulator-mandated look backs include, but are not limited to, the following:

- **Select the Right Party** –Make sure the party performing the look back is credible with the regulators and has experience relative to the customer types, geographic markets and products and services relevant to your financial institution.

- **Understand the Approach** – Take time to under what approach will be used to achieve maximum efficiency, e.g., what transaction data will and will not be in scope, how alerts will be produced, how alerts will be triaged and assigned for review, what documentation will be developed and where this documentation will be stored, and what the final deliverables will be.
- **Be Candid and Open about the Challenges** – If you know that the party that will be performing the look back is underestimating the number of potential alerts, that certain information (e.g., check details) will be challenging to retrieve or that certain customers/counterparties are likely not to be cooperative in responding to questions, share that information. This will help ensure that they build a realistic project plan and timetable and will avoid unpleasant surprises relating to costs if you are using a third party.
- **Get Regulator Buy-In** – Where appropriate, ask for the regulators' feedback on the planned approach and deliverables to ensure the methodology and final deliverables will align with regulatory expectations.
- **Ensure Availability, Access and Understanding of the Data** – To minimise the possibility that opinions may be based on incomplete or misunderstood data, take time at the beginning of the project to ensure the party performing the look back has access to all required systems and understands how and where relevant data are stored.
- **Establish and Communicate Operating Protocols** – At the beginning of the look back, establish protocols for the escalation of issues and protocols, identifying to whom these should be directed and the acceptable timeline for response.
- **Stay Engaged** – To avoid surprises, make sure you stay informed throughout the look back through regular status reports and status meetings.
- **Consider How the Results of the Look back Will be Integrated** – Look backs are often performed outside of your production environment so make sure you understand how the information developed during the look back will be integrated into your case management system so you have a complete audit trail.
- **Ask for Recommendations** – The party performing the look back will learn a lot about your customers, their activity and your existing transaction monitoring processes and capabilities so ask for recommendations on changes you can make to enhance transaction monitoring.
- **Respect the Independence of the Third Party** – Where an independent third party is performing the look back as a regulatory requirement, it is important to the credibility of the process that both you and the third party respect the boundaries of independence.

Investigation Process

1849. What is an investigation?

Monitoring refers to the initial process to detect potentially suspicious activity. An investigation (sometimes called a case) is the review of transactions/conduct, which may have been identified in

routine monitoring or brought to an institution's attention by regulators or law enforcement, in order to classify the alert as a "false positive" or a "true positive," which will require further analysis and could result in the filing of a SAR.

1850. Who should investigate unusual or potentially suspicious activity once it is identified?

Once unusual or potentially suspicious activity has been identified by either a business unit or through manual or automated monitoring, many financial institutions require the activity to be referred to a central investigative unit. The central investigative unit can either be a stand-alone department or be housed within the compliance department or a security department. Centralised investigations help to ensure that standards are applied uniformly, that confidentiality is maintained, and that there is consistency of documentation. Centralisation also may aid in the detection of larger-scale money laundering problems that span more than one business unit. Since this centralised unit does not generally have in-depth knowledge of a particular customer and its transaction profile, business units must be involved, at a minimum, to provide insight and explanation.

1851. Who should make the decision to file/not file a SAR?

Investigators, at the conclusion of an investigation, generally submit the findings to a member of management (e.g., AML compliance officer), who would then (a) agree with the decision to close the investigation without a Suspicious Activity Report (SAR) filing, (b) request additional investigation and/or clarification, or (c) agree with the decision to file a SAR. Financial institutions have varying levels of review regarding investigations warranting a SAR filing. Some financial institutions allow the AML compliance officer, or his or her delegate, to make the final decision whether or not to file a SAR; others require approval from the chief compliance officer and/or general counsel. Whatever the quality control process, the financial institution should ensure it submits high-quality SARs in a timely manner.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

1852. Is the AML compliance officer for a financial institution required to receive approval to file a SAR from senior management or the board of directors?

No. The AML compliance officer should not seek approval from senior management, the board of directors or any business line for SAR filings. Though the compliance department may involve the business to aid in its investigation of unusual or potentially suspicious activity, the compliance department must make its own determination as to whether the activity identified warrants a SAR filing. In many instances, the AML compliance officer makes the final decision to file or not file a SAR. In some instances, a committee is established to review the case and decide to file or not file a SAR.

It is important to note, however, that the board of directors and senior management should be notified of SAR filings. Since regulations do not mandate a particular notification format, financial institutions have flexibility in structuring their format and may opt to provide summaries, tables of SARs filed for specific violation types, or other forms of notification as opposed to providing actual copies of SARs.

1853. When selecting personnel to staff the investigative unit, what skills should be required by the financial institution?

There are a number of different skills and experiences that are useful for investigating suspicious activity, including, but not limited to, the following:

- Relevant industry/product knowledge
- Understanding of applicable AML/CFT risks
- Fraud and forensic training/healthy dose of scepticism
- Researching skills, including using the internet to develop information
- Ability to work effectively with the business lines to gather information
- Experience with suspicious transaction monitoring software, including an understanding of system functionality and detection logic
- Ability to identify patterns and spot anomalies
- Ability to draw and support conclusions and summarise them in a logically organised report

1854. Should one investigator be assigned to a case from the initiation to the conclusion of an investigation?

Financial institutions with small investigation teams are more likely to take a "cradle-to-grave" approach in which one analyst selects an alert, investigates it and sees the case through to resolution.

Other, particularly larger, institutions may take more of a triage approach, such as the following:

- Analysts perform the initial review of alerts to determine whether an activity may be potentially unusual and an investigation should be opened
- Investigators perform a detailed review of customer activity and recommend whether an investigation should be closed or a SAR filed
- Managers perform final review and make a decision to file or not file a SAR

The triage approach potentially allows better alignment of responsibilities with people's skills and experience, but in either scenario there can be a process or at least an understanding that the more complex alerts should go to the most experienced people.

1855. What are some keys to an effective investigation process?

Keys to an effective investigation process include, but are not limited to:

- Maintaining an investigation file with adequate documentation to allow an uninvolved party to understand how the decision to file or not file a SAR was reached.
- Performing sufficient due diligence on the customer or suspect. This would involve obtaining occupation or nature of business if not already contained in the financial institution's customer due diligence (CDD)/enhanced due diligence (EDD) documentation, gaining a basic

understanding of the purpose of the account or transactions in question, and performing research on adverse media/news information.

- Investigating not only the transaction(s) in question, but also conducting a historical review of the nature of the account activities and, where appropriate, related accounts over a reasonable period of time. Some common review periods include the previous six months or previous year, with some review periods starting from the date of account opening.
- Performing research on the entire customer relationship, including related accounts and related parties.

1856. What level of detail should a financial institution include in an investigation that may warrant the filing of a Suspicious Activity Report (SAR)?

An investigation warranting a SAR requires an explanation of the nature of the suspicious activity. The intent is to provide law enforcement agencies with as much information as possible to investigate the underlying activity further. It is important that financial institutions provide sufficient detail in their investigations to transfer their knowledge of the activity to law enforcement agencies.

The investigation should provide the facts of the activity, and the narrative should cover who, what, where, when and why, including, but not limited to, the date(s), amount(s), location(s), type(s) of transaction(s), name(s) of the party(ies) involved in the transaction(s) and the alert(s)/trigger(s) that initiated the investigation/SAR. All account numbers at the institution affected by the suspicious activity should be identified and, when possible, account numbers, names and locations at other institutions as well. Transactions should be listed chronologically, individually and by type (e.g., cash, wires or checks).

Financial institutions can submit a comma-separated values (CSV) file as an attachment that details the potentially suspicious transactions to supplement information provided in the investigation/SAR narrative.

If the subject of the filing is a customer of the institution, sufficient background information about the customer should be provided, including, but not limited to, additional Know Your Customer (KYC) information, known relationships and customer statements. If the subject is not a customer, information must be provided about the party(ies) involved to the extent possible.

If previous investigations have been conducted or previous SARs have been filed on the same party, it is important to provide references, such as the dates and details of these previous investigations and filings. The narrative should "tell the story" of why the financial institution believes the transaction activity is suspicious, and clearly state the final action taken (e.g., exit relationship, monitor the relationship) in the investigation.

For further guidance on SARs, please refer to the Suspicious Activity Reports section.

1857. What documentation should be maintained for investigations not warranting a SAR filing?

Financial institutions should maintain the same level of detailed investigative support for investigations not resulting in a SAR as they do for SAR filings. The financial institution should have enough support to justify its decision both to file a SAR and close an investigation without a SAR filing. This support should include a synopsis of both the customer and other suspects identified, a summary of the activity reviewed, and a clear determination as to why the situation did or did not warrant a SAR filing. The utilisation of a case management system that serves as a central repository for all investigations will assist financial institutions with the organisation and maintenance of the documentation.

1858. How can a financial institution evaluate the effectiveness of its suspicious transaction monitoring program?

When assessing overall effectiveness, the evaluation should not be limited to AML/CFT technology, but should also include the overall suspicious activity monitoring program, including systems, personnel, procedures and training. Some indicators and areas to assess include, but are not limited to, the following:

- **Alert-to-Investigation Ratio:** Financial institutions should review system rules that have low alert-to-investigation ratios to identify parameters that could be adjusted to reduce the volume of "false positives" (alerts cleared without escalation). Another indicator of ineffective monitoring is if a high percentage of recurring alerts were previously investigated and deemed not suspicious.
- **Investigation-to-SAR Filing Ratio:** Similar to alert-to-investigation ratios, analysing cases that lead to SAR filings may assist financial institutions in refining controls to better detect potentially suspicious activity by identifying high-risk products, services, customers or geographies that may require specific system rules or a separate manual monitoring process. In circumstances with low investigation-to-SAR filing ratios, the financial institution may need to revisit existing parameters, data feeds and staff training to reduce the number of false positives.
- **Non-System Sourced Investigations/SAR Filings:** Repeat investigations and SAR filings from non-system sources may provide insight into the development of new or enhanced monitoring rules (e.g., law enforcement inquiries, 314(a) and 314(b) information requests). However, if more SARs are filed on non-system sourced referrals than from automated alerts, existing monitoring rules need to be reviewed for effectiveness.
- **Lack of Alerts Generated for a Certain Product or Transaction Type:** This may indicate that a product or transaction type is not covered in the suspicious activity monitoring software, or that the existing rules and thresholds are ineffective in monitoring for potentially suspicious activity. In some instances, a manual monitoring process may need to be implemented to cover a particular product or transaction type (e.g., trade finance).

- **Few Alerts Generated for High-Risk Customers:** This may indicate an ineffective customer risk assessment methodology, ineffective incorporation of risk into suspicious activity monitoring software, or both.
- **Wide-Ranging Rates of Clearing Alerts by Investigative Personnel:** Developing a process in which more complex alerts and cases are assigned to seasoned personnel may improve the overall efficiency of the monitoring and investigation process. Additionally, to ensure alerts are properly reviewed, quality control reviews of cleared alerts by more experienced staff can be conducted.
- **Alert Assignment and Case Management:** Different system rules may generate alerts on the same activity; therefore, a comprehensive alert and case management system that assigns alerts based on customer and account relationships is critical to overcome any inefficiencies in reviewing the same transaction(s) flagged by multiple monitoring rules. A proper case management system should also incorporate non-system sourced cases (e.g., law enforcement inquiries, whistleblower hotline).
- **Productivity of Individual Rules/Scenarios:** Looking at how many alerts are generated from individual rules and the extent to which these alerts ultimately result in SARs being filed may yield results that can be used to modify or delete certain rules.
- **High Volume of Repeat SAR Filings on the Same Subject(s):** This may indicate an ineffective customer termination policy.
- **Backlogs or Late SAR Filings:** This may indicate ineffective use of monitoring software, lack of required personnel commensurate to the volume of alerts, inadequate knowledge and experience of monitoring and investigation personnel and/or a lack of appropriate management reporting to track and aid in understanding and promptly addressing any growing backlogs.
- **Auditors/Regulators Identify Suspicious Activity Unreported on SARs Filed by the Financial Institution or Question the Quality and Completeness of Investigation Files:** This may indicate that the monitoring and investigation team lacks: relevant industry/product knowledge; an understanding of applicable AML/CFT risks; fraud and forensic training/healthy dose of scepticism; the ability to work effectively with business lines to gather and document pertinent information; or an understanding of system functionality or detection logic.

Financial institutions should continuously review published typologies to identify emerging risks or controls to assist them in enhancing their suspicious activity monitoring program.

Overall, each component of a financial institution's suspicious activity monitoring program (including individual system rules and resulting alerts) should be analysed individually and collectively for overall effectiveness.

1859. What reports should be provided to senior management related to a suspicious activity monitoring and investigation program?

Management reporting is a process through which management (and the board of directors) are provided, routinely and on an as-needed escalation basis, the information they need to manage the

operations and risks of the organisation. Management reporting will vary depending on the type of financial institution, the nature of the products and services it offers, and the clients it serves. Examples of key risks and key performance indicators include, but are not limited to, the following:

- Number of SAR filings and associated volume of suspicious activity and deposit/lending balance of named subjects;
- Explanations for significant changes in volume of SAR filings;
- Volume of alerts and investigations;
- Aging of alerts and investigations;
- Alert-to-investigation ratio, investigation-to-SAR ratio;
- Summary of significant investigations (e.g., high volume of suspicious activity, uncovered weakness in monitoring program, investigations involving insiders, politically exposed persons [PEPs]);
- Major changes to the automated systems being used to support the company's AML/CFT Compliance Program and rationale for the changes; and
- Details of recently reported money laundering/terrorist financing schemes, to the extent that the company may because of its products/services and customers be subject to risks, and discussion of controls in place to mitigate such risks.

1860. What are some common gaps of suspicious activity monitoring and investigation programs?

Some common gaps of suspicious activity monitoring and investigation programs include, but are not limited to, the following:

- Incomplete monitoring of customer population or omission of transaction types;
- Inadequate development or communication of suspicious activity monitoring policies and procedures;
- Failure to incorporate risk assessments (e.g., customer risk assessment, line of business/legal entity risk assessment) into suspicious transaction monitoring program;
- Insufficient/inadequate resources dedicated to monitoring and investigation team(s);
- Lack of specific and customised training of employees (e.g., investigation training for compliance personnel, suspicious activity red flags training for business line personnel);
- Lack of internal referral network for potentially suspicious activity (e.g., whistleblower hotline);
- Failure to conduct monitoring on a customer level or consider relationships (e.g., entities owned or controlled by customer, beneficial owners);
- Inadequate use (or misuse) of suspicious activity monitoring technology (e.g., inadequate tuning/validation, poor alert management, inadequate case management);

- Poor documentation maintained for investigations, including those that did not lead to SAR filings;
- Poor follow-up on SAR actions (e.g., close, monitor); and
- Lack of reporting of key SAR information to senior management/board of directors.

For additional guidance on suspicious activity monitoring software, please refer to the AML/CFT Technology section.

Suspicious Activity Red Flags

1861. What are examples of suspicious activity?

The following is a sample list of red flags that may be applicable to different types of transaction activities and businesses. This is not an exhaustive list. It is essential that financial institutions consider these red flags as guidance and exercise judgment in identifying other transactions that may be unusual or indicate potential money laundering or terrorist financing.

Also, it is important to note that customers are not necessarily doing something illegal just because their activities mirror one or more of these red flags; however, such activities generally warrant further review and, if a satisfactory justification is not obtained, a more thorough investigation should be conducted to determine whether a SAR should be filed.

Further examples of potentially suspicious activity can be found in the SAR Activity Review: Trends, Tips & Issues issued periodically by FinCEN, the FATF's annual report on Money Laundering Typologies, the FFIEC BSA/AML Examination Manual and the Joint Money Laundering Steering Group (JMLSG).

Account Opening Red Flags

- Customer is unwilling to provide the required account opening information and/or documentation
- Customer uses unusual or suspicious identification documents that cannot be readily verified
- Customer exhibits unusual concern for secrecy, particularly with respect to identity, type of business, assets or dealings with other entities
- Customer has difficulty describing its business, the stated purpose of the account and the expected transactions in the account
- Customer lacks a general knowledge of its industry
- Customer's financial statements reflect concentrations of closely held companies or businesses that lack audited financial statements to support their value
- Customer is reluctant to provide information on controlling parties and underlying beneficiaries
- Customer questions reporting/recordkeeping requirements
- Customer requests that documentation standards be waived

- Customer provides forms of identification for CIP purposes with conflicting information
- Customer makes frequent or large transactions and has no record of past or present employment experience
- Customer has no apparent reason for using the institution's services (e.g., customer is not located in close proximity)
- Customer has multiple accounts under single or multiple names for no apparent business purpose
- Customer, or a person/entity publicly associated with the customer, has a questionable background, including prior criminal, civil or regulatory convictions
- Upon request, customer refuses to identify or fails to indicate a legitimate source of its funds and other assets
- Customer has a defensive stance to questions
- Customer uses same address(es) for multiple customers that have no apparent relationship
- Customer provides disconnected telephone number(s)
- Customer provides identification documents that are expired or appear false
- Customer provides inconsistent information when questioned

Account Activity and Transaction Execution Red Flags

- Transactions with no logical economic purpose
- Transaction not in line with customer's stated purpose of the account and/or nature of business
- Accumulation of large balances that are inconsistent with the customer's business, and the subsequent transfer of such balances to another jurisdiction
- Customer makes large deposits and maintains large balances with little or no apparent justification
- Transactions that involve higher-risk businesses
- Transactions involving senior political figures, both foreign and domestic
- Sudden high volume of unexplained activity
- High volume of transaction activity with low balances and/or account is frequently overdrawn
- Uncharacteristic nonpayment for services, which may indicate a loss of funds or access to funds
- Frequent transactions at daily maximums (e.g., cash withdrawals from an ATM)
- Frequent disbursements to/from apparently unrelated third parties
- Round-sum transactions (e.g., US$10,000.00, US$50,000.00, US$500,000.00)

- Layering (e.g., transfers between bank accounts of related entities or charities for no apparent reason)
- Customer opens a number of accounts under one or more names, and makes numerous cash deposits just under US$10,000, or deposits containing bank checks or traveller's checks
- Customer maintains multiple accounts at a bank or at different banks for no apparent legitimate reason; accounts may be in the same names or in different names with different signature authorities; inter-account transfers evidence common control
- Customer conducts multiple transactions several times in one day or over a short period of time (possibly using different tellers), indicating structuring
- Customer makes numerous deposits under US$10,000 in an account in short periods of time, thereby avoiding the requirement to file a Currency Transaction Report; this includes deposits made at an automated teller machine
- Deposit/withdrawal transactions just below reporting thresholds, indicating possible structuring or avoidance of tax reporting requirements (e.g., US$2,999, US$9,990)
- Lack of concern exhibited by the customer regarding risks, commissions or other transaction costs
- Transactions are frequently changed at the teller, particularly upon notification of identification and/or reporting requirements
- Customer attempts to bribe or threaten an employee in order to circumvent reporting requirements

Currency Red Flags

- Deposits of currency just below the reportable threshold conducted with multiple branches, tellers, ATMs, accounts and/or on different days
- Deposits of currency by multiple individuals into the same account
- Deposits of currency wrapped in currency straps that have been stamped by other financial institutions
- Frequent exchanges of small dollar denominations for large dollar denominations
- High volume of currency deposits and/or withdrawals inconsistent with the profile of the customer
- Multiple deposits occurring in various out-of-state locations
- Frequent cash deposits or withdrawals with no apparent/known business source
- Customer requests cash shipment or transfer to another account almost immediately after making numerous cash deposits
- Sudden increase in cash activity

- Lack of withdrawal of currency for businesses that generally require significant amounts of currency (e.g., retail, check cashers, owners of automated teller machines), possibly indicating another source of currency

For further guidance, please refer to the Currency Transactions section.

ATM Transactions and Owner/Operators of Privately Owned ATM Red Flags

- Automated teller machine (ATM) activity levels are high in comparison with other privately owned or bank-owned ATMs in comparable geographic and demographic locations
- Sources of currency for the ATM cannot be identified or confirmed through withdrawals from account, armoured car contracts, lending arrangements, or other appropriate documentation
- Frequent international ATM transactions, especially those preceded by cash deposits
- Frequent deposits and withdrawals from multiple ATMs, especially near daily maximums or near BSA reporting thresholds
- Activity from ATMs located in different states or countries

For further guidance, please refer to the Owner/Operators of Privately Owned ATMs section.

Bulk Shipments of Currency Red Flags

- An increase in the sale of large denomination U.S. bank notes to foreign financial institutions by U.S. banks
- Small denomination U.S. bank notes smuggled into Mexico being exchanged for large denomination U.S. bank notes possessed by Mexican financial institutions
- Large volumes of small denomination U.S. bank notes being sent from Mexican *casas de cambio* to their accounts in the United States via armoured transport, or sold directly to U.S. banks
- Multiple wire transfers initiated by *casas de cambio* that direct U.S. financial institutions to remit funds to jurisdictions outside of Mexico that bear no apparent business relationship with that *casa de cambio* (recipients include individuals, businesses, and other entities in free trade zones and other locations associated with Black Market Peso Exchange-type activities)
- The exchange of small denomination U.S. bank notes for large denomination U.S. bank notes that may be sent to jurisdictions outside of Mexico, including jurisdictions associated with Black Market Peso Exchange-type activities, such as Mexico, Guatemala, Argentina, Brazil, Paraguay, Uruguay and Venezuela
- Deposits by *casas de cambio* to their accounts at U.S. financial institutions that include third-party items (including sequentially numbered monetary instruments and checks)
- Deposits of currency and third-party items by Mexican *casas de cambio* to their accounts at Mexican financial institutions and thereafter, direct wire transfers to the *casas de cambio* accounts at U.S. financial institutions

- Frequent requests for cash letter instruments

For further guidance, please refer to the Bulk Shipments of Currency and Bulk Cash Smuggling section.

Branch and Vault Shipments Red Flags

- Significant exchanges of small denomination bills for large denomination bills
- Significant changes in currency shipment patterns between vaults, branches and/or correspondent banks
- Rapid increase in the size and frequency of cash deposits with no corresponding increase in noncash deposits
- Unusually large currency shipments to and from remote locations
- International cash shipments funded by multiple monetary instruments
- Frequent use of cash shipments of customers in non-cash intensive businesses
- Cash shipments with instructions inconsistent with normal cash shipment practices
- Branches whose large bill requirements are significantly greater than the average or branches that suddenly stop shipping large bills

Monetary Instrument Red Flags

- Purchase or deposit of structured monetary instruments, often in round dollar amounts, sequentially numbered, just below reporting threshold (e.g., US$2,999, US$9,990) for currency
- Purchase of multiple sequentially numbered monetary instruments for the same payee
- Use of one or more monetary instruments to purchase another monetary instrument(s)
- Purchase of cashier's checks, money orders, and so forth, with large amounts of cash
- Missing/illegible information (e.g., blank payee)
- Lack of signature
- Frequent payments to same payee(s)
- Deposit or use of multiple monetary instruments purchased on the same date from different banks or different issuers
- Numerous deposits of small monetary instruments, followed by a request for a large outgoing wire to another institution or country
- Customer purchases multiple money orders with no apparent reason

For further guidance, please refer to the Monetary Instruments section.

U.S. Dollar Draft Red Flags

- Significant variance in expected/historical activity versus actual activity in terms of volume of U.S. dollar draft activity
- Dollar amounts that appear to be designed to evade reporting requirements (i.e., under US$3,000 or US$10,000) or are purchased in round amounts
- Multiple sequentially numbered U.S. dollar drafts
- High volume of U.S. dollar drafts to the same payee or from the same remitter
- Drafts issued by *casas de cambio*
- Third-party endorsed drafts
- No payee named on the draft (typically from Mexico)
- Large volume of activity through correspondent master accounts opened by foreign banks

For further guidance, please refer to the U.S. Dollar Drafts section.

Wire Transfer Red Flags

- Apparently unnecessary and/or frequent changes to standard wire payment instructions
- Changes made to spelling of names and addresses of originators/beneficiaries (e.g., deliberate misspellings, reordering of names, incomplete addresses)
- Wire transfers to and from bank secrecy haven countries and countries known for or linked to terrorist activities, drug trafficking, illegal arms sales or other illegal activity
- Wires to other countries without changing the form of the currency (e.g., USD)
- Intentional circumvention of approval authorities or reporting limits by splitting transactions
- A large deposit followed by numerous, smaller wire transactions
- Numerous smaller wire transactions from an account that maintains a low balance
- Several deposits, particularly in currency or monetary instruments, followed by international wire transactions
- Unexplained or sudden, extensive wire activity, especially in accounts that had little or no previous activity
- Outgoing wire transactions requested by non-account holders, particularly for cash under US$10,000 designed to evade Currency Transaction Reporting
- Large number of wire transfers to/from unrelated third parties
- Large number of wire transfers for large round dollar amounts
- Indications of frequent overrides of established approval authority and other internal controls

- Wiring of funds without normal identifying information or in a manner that indicates an attempt to hide the identity of the sender or recipient
- Wire transactions designed to evade the US$3,000 identification/recordkeeping requirement
- Wire transactions sent or received from the same individual to or from different accounts
- Transactions sent by or to noncustomers, also known as "Payable Upon Proper Identification" (PUPID)

For further guidance, please refer to the Funds Transfer section.

Automated Clearinghouse Transactions Red Flags

- Unusually high level of transactions are initiated over the internet or by telephone
- Large value ACH transactions are frequently initiated through third party payment processors (TPPP) by originators that are not customers of the bank and for which the bank has no or insufficient due diligence
- Transactions involve multiple layers of unnecessary TPPPs
- Requests for information from the National Automated Clearinghouse Association (NACHA) may signal concerns.
- The TPPP involved has a history of violating ACH network rules and/or generating illegal or fraudulent transactions on behalf of their customers

Virtual Currency Red Flags

- Virtual currency exchanger/administrator is unlicensed or unregulated, where licensing/regulation is implemented
- Virtual currency exchanger/administrator is not affiliated or backed by a traditional financial institution
- Virtual currency exchanger/administrator is linked to nonbanking financial institutions (e.g., *casas de cambio*) in high-risk jurisdictions for criminal activity and financial crimes or lax AML/CFT systems
- Virtual currency exchanger/administrator has lax customer identification and monitoring policies and procedures and/or does not enforce AML/CFT policies, thus facilitating anonymous transactions
- Virtual currency exchanger/administrator is linked to advertisements of businesses involved in potentially illicit activities (e.g., illegal internet gambling, unregulated pharmaceutical companies, escort services)

For further guidance, please refer to the Virtual Currency Systems and Participants section.

Certificate of Deposit Red Flags

- Early redemption of certificates of deposit without regard to penalties
- Used as collateral for loans
- Disbursement of certificates of deposit by multiple bank checks or to unrelated third parties

Safe Deposit Box Red Flags

- Frequent visits to safe deposit boxes by one or more customers
- Visits to safe deposit boxes after withdrawals of large amounts of currency/purchases of monetary instruments
- Multiple safe deposit boxes rented by the same customer
- Safe deposit box opened by an individual who does not reside or work in the area
- Signatories have no apparent business or personal relationship

Lending Red Flags

- Early repayment of a loan in currency or monetary instruments (particularly for problem loans)
- Structured payments of loan in currency or monetary instruments
- Disbursement of loan proceeds via structured currency withdrawals or monetary instruments
- Disbursement of loan proceeds to a third party
- Third-party payment of a loan
- Unwillingness to provide information about the purpose of the loan and/or source of repayment and/or collateral
- Loan collateralised with a currency deposit, certificate of deposit, funds from an offshore account or in the name of a third party
- Loan proceeds are transferred offshore without apparent reason
- Attempts to sever any paper trail connecting a loan with the collateral for that loan
- Early pay-down or pay-off of a large loan, with no evidence of refinancing or other explanation

For further guidance, please refer to the Lending Activities section.

Mortgage and Real Estate Red Flags

- Borrower arrives at a real estate closing with a significant amount of cash
- Borrower purchases property in the name of a nominee, such as an associate or a relative

- Borrower negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table"
- Borrower sells property below market value with an additional "under the table" payment
- Borrower or agent of the borrower purchases property without much knowledge about the property inspection or does not appear sufficiently knowledgeable about the purpose or use of the real estate being purchased
- Borrower purchases multiple properties in a short period of time or appears to be buying and selling the same piece of real estate for no apparent legitimate purpose
- Seller requests that proceeds be sent to a high-risk jurisdiction or offshore bank
- Borrower makes payments with funds from a high-risk jurisdiction or offshore bank

For further guidance, please refer to the Mortgage Fraud section.

Money Transmitter Red Flags

Applicable to money transmitters (licensed or not) and/or informal value transfer systems (IVTS) as customers of a depository institution:

- Numerous deposits of third-party items, including sequentially numbered monetary instruments, into their accounts at U.S. banks
- Multiple remittances of funds transfers from their accounts at foreign financial institutions to accounts at U.S. banks
- Multiple remittances of funds to jurisdictions outside of their home country and there is no apparent business relationship between the MSB and the beneficiaries
- Large volumes of small denomination U.S. banknotes are sent from foreign MSBs via armoured transport for deposit into their U.S. accounts

For further guidance, please refer to the Money Services Businesses section.

Credit Card Red Flags

- Prepayment of credit card, particularly when refund checks will be issued to the customer
- Payment of credit card from high-risk jurisdiction or offshore bank
- Payment of credit card with cash or currency
- Payment of credit card by unrelated third parties
- Multiple payments within a billing cycle
- Prepayments followed by cash advances/purchases of convenience checks
- Payment of private label credit cards via gift card from the merchant
- Credit card refunds from merchants without offsetting transactions

Trade Finance Red Flags

- Items shipped that are inconsistent with the nature of the customer's stated line of business
- Obvious over- or under-pricing of goods and services
- Transactions involving high-risk goods (e.g., weapons, ammunition, chemicals, sensitive technical data, nuclear materials, precious gems, crude oil)
- Goods are transshipped through one or more jurisdictions for no apparent economic reason
- Missing trade documentation information (e.g., name and address of applicant/beneficiary, name and address of issuing/advising banks, specified or determinable amount and type of currency, sight or time draft to be drawn, expiry date, general description of merchandise, types and numbers of documents that must accompany the credit)
- Unwillingness to provide documents to prove the shipment of goods
- Transaction structure appears unnecessarily complex and designed to obscure the true nature of the transaction
- Documentation showing a higher or lower value or cost of merchandise than that which was declared to customs or paid by the importer
- Documentary fraud
- Changes in payment instructions
- Excessively amended letters of credit
- Presentations of letters of credit or documents where the financial institution has no record of the credit's existence
- Letter of credit that includes a condition for a "switch bill of lading"
- Bill of lading describing containerised cargo, but without container numbers or with sequential numbers
- Invoice showing miscellaneous charges (e.g., handling charges greater than 40 percent of total invoice value)
- Transaction(s) involving front/shell companies

For further guidance, please refer to the Trade Finance Activities section.

Capital Market Products Red Flags

- An account shows an unexplained high level of funds transfer activity with a very low level of securities transactions
- Client deposits or attempts to deposit cash at a financial institution that does not routinely accept cash

- Client takes both a short and a long position in a security or contract for similar amounts and similar expiration dates with no apparent business purpose
- Customer appears to be acting as an agent for an undisclosed third party, but declines or is reluctant to provide information relating to the third party
- Customer makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer the proceeds out of the account
- Customer funds an account with funding sources such as traveller's checks, third-party checks, checks made out to cash
- Transactions originating from/destined to high-risk jurisdictions that were not included as expected transactions in the account profile and/or are otherwise unexpected
- Transactions where the beneficiary name is not the account holder, or where the wire instruction is not the standard wire instruction provided at account opening
- Large trades/purchases performed in accounts with small balances
- Transactions/trades that consistently result in large losses

For further guidance, please refer to the Broker-Dealers in Securities section.

Insurance Products Red Flags

- Customer's lack of concern with the cost of the policy
- Customer's lack of concern with the performance of an insurance product
- Customer's lack of concern with the penalties/fees
- Purchase of a product that appears outside the customer's normal range of wealth or estate planning needs
- Large single-payment premiums for life and annuity policies
- Unusual methods of payment, particularly cash or cash equivalents
- Multiple currency equivalents from different banks and money services businesses used to make payments
- Beneficiaries that are unidentified or located in high-risk jurisdictions
- Policy repayments that are inconsistent with the customer's source of funds and/or income
- Premium payments that are made by apparently unrelated third parties
- Policy assigned to a third party soon after it is purchased
- Early policy cancellation (particularly during the free-look period of annuity contracts)
- Insurance policy loans or policy surrender values that are subject to a substantial surrender charge

For further guidance, please refer to the Insurance Products section.

Casino Red Flags

- Gaming transactions that do not correspond with the customer's profile (e.g., stated business, income/salary)
- Large transactions with minimal gaming activity
- Structuring of cash transactions in an attempt to evade currency transaction reporting requirements (e.g., US$9,900)
- An initial deposit of funds with the casino is either cashed out or transferred to a bank account with minimal or no gaming activity
- Customer betting with unusual characteristics (e.g., betting both sides of an even bet)
- Customer transfers chips to other individuals to cash out
- Customer redeems chips for casino checks that amount to significantly more than the amount of funds deposited with no apparent winnings to account for the additional amount
- Customer departs casino without cashing out chips, an activity referred to as "chip walking"

For further guidance, please refer to the Casinos and Card Clubs section.

Retail Red Flags

- Purchase of luxury items in cash or monetary instruments
- Return of high-value items paid for in cash or monetary instruments to obtain a check refund
- Purchase of prepaid access/gift cards with cash or monetary instruments
- Structuring of cash transactions in an attempt to evade Form 8300 reporting requirements by making purchases at different point-of-sale (POS) terminals or various branches
- Refusal to provide personal information for purposes of filing Form 8300 or other recordkeeping and reporting requirements
- Transactions on behalf of individuals/corporations located in jurisdictions with little or no AML/CFT regulation; countries with known drug, criminal or terrorist links; and offshore entities in tax havens
- Transactions made by high-risk customers, such as senior foreign political figures, if known
- Purchases that are inconsistent with past purchasing trends
- Third-party payments for luxury items
- Willingness to trade or exchange items for less than retail value

- Purchases of large quantities of precious metals and stones (e.g., gold, diamonds), fine art and other valuable items (e.g., stamps)
- Purchases of items in bulk that are small in size and high in value
- Purchases of items in bulk that are easy to resell online (e.g., baby formula, razors)

Consumer Products Red Flags

- Cross-border sales to transfer funds and/or goods across jurisdictions
- Profit margin on equipment/goods appears unrealistically high, indicating the possible sale of stolen equipment/goods
- Payment of proceeds to/by an unrelated third party

Terrorist Financing Red Flags

- An account for which several persons have signature authority, yet these persons appear to have no relation to each other
- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g., student, unemployed, self-employed)
- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g., countries designated by national authorities)
- Cross-border transfers of funds using prepaid cards
- Transactions to/from nonprofit or charitable organisation for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction
- Designee or close associate of designee under OFAC's Counter Terrorism Sanctions Program

Drug Trafficking and Marijuana-Related Businesses Red Flags

- Customer with an excessive number of individual accounts
- A common mobile number, address and/or employment references that are used to open multiple accounts under different names
- Cash deposits conducted by multiple unrelated third parties
- Cash deposits that smell like marijuana
- High volume of transactions with businesses or individuals located in different states or countries

- Excessive payments made to business owner, manager or employees
- Designee or close associate of designee under OFAC's Counter Narcotics Trafficking Sanctions Program
- To detect unlicensed marijuana-related business (MRB) activities of existing customers:
    - Business unable to provide state license;
    - Business unable or refuses to demonstrate legitimate source of funds of account activity or other investment(s);
    - Business deposits currency that smells like marijuana;
    - Excessive payments made to owners or employees;
    - Frequent inter-state transactions with third parties (e.g., customers, vendors, suppliers) in high-risk jurisdictions (e.g., located in or near states that have legalised marijuana-related activities, high intensity drug trafficking areas [HIDTAs]);
    - Business is located on federal property or in close proximity to a school in violation of federal and state laws;
    - Marijuana sold by the business was grown on federal property in violation of federal law; and
    - Searches of publicly available sources reveal business owners, employees or other related parties are involved in the illegal purchase of drugs, violence or other criminal activity or have been subject to sanctions for violations of state or local marijuana-related laws.

For further guidance, please refer to the sections: Counter Narcotics Trafficking Sanctions Program and Marijuana-Related Businesses.

Human Trafficking and Migrant Smuggling Red Flags

- Customer with an excessive number of individual accounts
- Customer who conducts transactions on behalf of customers whose accounts were recently closed due to suspicious activity
- Customer's telephone numbers linked to personal advertisements for potentially illicit activity (e.g., escort services) that have been verified through public sources
- Customer's address linked to residence and/or hotel with suspected ties to trafficking (e.g., named in previous investigations and busts, offer hourly rates)
- A common mobile number, address and/or employment references that are used to open multiple accounts under different names
- Households with an unusually high number of residents who also appear unrelated, but share accounts, addresses and mobile numbers

- Accounts opened in the name of unqualified minors, foreign workers or foreign students
- Accounts opened by an employer or recruitment agency on behalf of foreign workers and students (e.g., custodial arrangement)
- Accounts reported for identity theft
- Accounts opened with fraudulent or missing/incomplete documentation
- Accounts lacking commercial activity (e.g., payroll taxes) or activity inconsistent with the stated nature of business/expected activity
- Account activity beyond the living standard of the account holder
- Account activity conducted by a third party (e.g., employer) who always accompanies the account holder (may direct the transaction, possess the identification of the account holder and act as an interpreter)
- Account activity with beneficiaries/originators in high-risk countries known for human trafficking or with significant migrant populations (e.g., El Salvador, Guatemala, Honduras, Mexico) or along the southwest border of the United States
- High number of cash deposits structured to avoid reporting requirements
- Cash deposits into one account from multiple locations throughout all states, often followed by multiple wire transfers to high-risk countries (also known as funnel accounts)
- Frequent deposits and withdrawals from multiple branches and ATMs
- Frequent use of cash couriers
- Frequent exchanges of small dollar denominations for large dollar denominations by customers involved in noncash intensive business
- Frequent transfers to common recipients often in high-risk countries; often under the US$3,000 reporting threshold
- Frequent transfers or checks payable to casinos or money transmitters
- Frequent small dollar international funds transfers for “repayment of debt”
- Frequent deposits of payroll checks from multiple parties, seemingly unrelated
- Frequent payments for rent, hotels, rental cars, airline tickets or other travel-related accommodations
- Repeat payments to advertisers (e.g., websites, newspapers) that promote the sex industry (e.g., escort services)
- Frequent payments to unlicensed or noncompliant recruitment agencies (e.g., employment, students) with a history of labour violations
- Bill payments using money orders as opposed to paying with personal checks

- High volume of payments for multiple mobile phones
- High volume of payments for large food purchases
- High volume of deposits of government benefits for multiple beneficiaries followed immediately by cash withdrawals
- Purchases of luxury items or assets in high-risk countries

For further guidance, please refer to the Human Trafficking and Migrant Smuggling section.

Elder Financial Abuse Red Flags

- **Changes in transaction activity** – The elder's spending pattern may change, including:
  - Decreased spending on essential items (e.g., food, medication, utilities)
  - Increased spending and purchases of unnecessary items or items he/she can't use
  - Numerous withdrawals, including the maximum ATM withdrawal
  - Checks may be written out of sequence
  - Large wires to third-party beneficiaries with unclear relationships with the elder
- **Unexplained activity** – The activity may not make logical sense, given known details about the customer:
  - ATM withdrawals, when the elder is homebound
  - The sudden presence of overdrafts, when previously there had been limited to no insufficient funds activity
  - Numerous unpaid bills, when someone has been designated to pay them
  - An appearance of checks or signed documents, when the elder cannot write or lacks the capacity to understand what he/she is signing, or the signature on checks and documents may not resemble the elder's signature
- **Changes in account features** – The elder may request the addition of account features or changes to existing features, including:
  - A request for the issuance of a credit or debit card for the first time
  - Seeking to enrol in online banking
  - Changing the account beneficiary
  - Requesting that statements be sent to an address besides his/her own
- **Uncharacteristic requests** – The elder may seek to undertake a non-routine transaction, including:
  - Refinancing a mortgage
  - Closing a certificate of deposit without regard to penalties for early withdrawal

- Requesting to wire a large sum for no apparent purpose

For further guidance, please refer to the Elder Financial Abuse section.

Employee/Insider Abuse Red Flags

- Employee has lavish lifestyle inconsistent with his or her salary
- Employee continuously overrides internal controls
- Employee is reluctant to take long vacations
- Significant personal credit problems
- Behavioural changes indicating possible drug, alcohol, gambling addiction or fear of losing job
- High employee turnover, especially in areas vulnerable to fraud
- Refusal to take vacation or leave
- Lack of segregation of duties

For further guidance, please refer to the Know Your Employees section.

Business E-Mail Compromise (BEC) and E-Mail Account Compromise (EAC) Red Flags

- Email address used to send transaction instructions has been slightly altered (e.g., addition, deletion, changing of a letter so email address resembles authentic email address);
- Payment instructions include different language, beneficiary, account information, timing and amounts from previously verified and authentic transactions;
- Payment instructions include the same beneficiary as previous instructions, but different account information;
- Payment instructions include transfers to beneficiary with no payment history or documented relationship with the customer;
- Payment instructions include beneficiary/account information previously flagged for fraudulent activity;
- Payment instructions include language such as “Urgent”, “Secret” or “Confidential”;
- Payment instructions are delivered in a way to limit the time and opportunity for a financial institution to authenticate the transaction (e.g., close-of-business, end of the week);
- Payment instructions originate from a customer’s employee who is newly authorised to conduct transactions and/or has no history of conducting transactions;
- Customer’s employee or representative cannot verify payment instructions originating from emails from executives, attorneys or designees;
- Multiple payment instructions for additional payments shortly after a successful payment from an account not typically used in this manner (e.g., payments to vendors/suppliers); or

- Beneficiary in wire transfer instructions does not match the name of the account holder.

For further guidance on BEC/EAC, please refer to the Business E-Mail Compromise and E-Mail Account Compromise section.

AML/CFT TECHNOLOGY

Technology Basics

1862. What role does technology play in supporting a financial institution's AML/CFT Compliance Program?

Technology plays a significant, and expanding, role in supporting effective AML/CFT Compliance Programs and is used for a number of different components of a program, including, but not limited to:

- Risk Assessment Automation
- Know Your Customer (KYC) Process
- Customer and Transaction List Screening
- Monitoring, Investigating, Documenting and Filing of Suspicious Activity Reports (SARs)
- Large Currency Transaction Monitoring and Filing of Currency Transaction Reports (CTRs)
- Training Software
- Management Reporting

1863. Are financial institutions required to use technology in their AML/CFT Compliance Programs?

There are some jurisdictions (e.g., Switzerland, India) which require the institutions under their supervision to use automated transaction monitoring systems. Regulators in other jurisdictions have encouraged institutions to implement such software and, in some cases, have required the implementation of automated transaction monitoring software under the terms of enforcement actions. Likewise, regulators have increasingly encouraged the use of automated KYC repositories by making it clear that KYC information needs to be readily accessible to, among others, those responsible for monitoring and investigating potentially suspicious activity. Beyond any regulatory mandate, the reality is, however, that the volume of data that must be accessed and analysed to support various components of an AML/CFT compliance program makes it impossible for many institutions to defend their compliance programs as credible if they do not include strong technology support.

Certain regulators, notably the U.K. Financial Conduct Authority (FCA), are working closely with the financial services industry to explore the benefits of technology (i.e., regtech, technology that focuses solely on the application of a technology framework to automate various regulatory business processes) for improving the efficiency and effectiveness of AML/CFT compliance programs. For further guidance on regtech, please refer to The Future of AML/CFT Technology section.

1864. What is FATF's position on the use of technology to support AML/CFT Compliance Programs?

There is no FATF mandate that technology must be used. However, FATF has signalled its support of regtech initiatives, pointing to the potential of technological innovation to assist the public and private sectors in meeting the FATF's objectives of combating money laundering and terrorist financing.

1865. What key guidance have regulatory bodies issued on the use of AML/CFT technology?

Multiple U.S. regulatory bodies have issued guidance on the use of AML/CFT technology, including, but not limited to, the following:

- Supervisory Guidance on Model Risk Management (reflected in FRB's Supervisory Letter (SR) 11-07 and OCC Bulletin 2011-12) by the Federal Reserve Board (FRB) and the Office of the Comptroller of the Currency (OCC). For further guidance on models, please refer to Model Validation.
- The FFIEC's IT Handbook includes extensive guidance on the development, acquisition and maintenance of technology systems.
- Several U.S. regulators have published guidance on their expectations for the management of third-party risks which would apply to all vendor-supplied technologies. For further guidance on third-party risks, please refer to Know Your Third Parties.
- At the state level, the New York Department of Financial Services (DFS) adopted a first of its kind regulation that requires certain DFS-regulated institutions to certify annually to the effectiveness of their transaction monitoring and sanction filtering programs, including the enabling technologies. For further guidance on New York's AML/CFT regulation, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications.

1866. Can one provider handle multiple aspects of an AML/CFT Compliance Program and are there benefits to using a single vendor?

There are a number of providers that offer multiple AML/CFT and sanction-related products, including KYC, list screening, transaction monitoring and case management tools. Using one vendor may offer some efficiencies, may limit compatibility issues with core systems and may even provide potential cost savings from the bundling of offerings; however, before deciding to use only one provider, a company should assess the functionalities of the individual modules to ensure that they align with the company's needs. Conversely, there are companies who benefit by using "best of breed" solutions which belong to different vendors. The best strategy is one that aligns with the business needs of the organisation.

1867. What are the benefits of implementing AML/CFT technology solutions on an enterprise basis rather than a local basis?

An enterprise solution provides a holistic view that may be difficult to develop when solutions are implemented on a local (e.g., business line, countrywide) basis. Other potential benefits of an enterprise solution include that it:

- Affords more efficient/effective management of changes in software and processes
- Promotes data consolidation which can then be further leveraged for Big Data analytics
- Promotes data sharing among systems, e.g., sanctions screening and transaction monitoring systems can share the same database of customer information
- Effectively uses resources across the enterprise footprint
- Provides cost savings associated with training, maintenance, and operability across business and technology teams

However, there may be good reasons, such as the need for local customisation or privacy and data transmission restrictions, which may make an enterprise solution impractical.

1868. What are the potential challenges of implementing enterprise technology solutions?

The potential challenges of implementing enterprise technology solutions are listed below:

- A critical defect in the technology solution impacts the enterprise rather than just a local instance.
- Region-specific requirements related to data privacy and transmission cannot be incorporated into a single instance enterprise technology solution.
- A high level of customisation may be required to incorporate regional specific business processes (e.g., alert investigation process) into an enterprise solution.
- From a governance standpoint, an enterprise approach creates a team structure that is highly centralised, thus concentrating the knowledgebase centrally versus having a team structure that is decentralised as will be the case for local instance.
- Any changes to an enterprise solution may require a wider approval, which results in more time to implement changes due to considerations across the enterprise footprint.

1869. What steps should an institution consider when implementing a new technology solution?

Typically, there are software implementation guidelines that are defined by an institution's IT department. However, at a minimum, the following aspects of a typical software development life cycle (SDLC) need to be considered:

- Requirement definition and documentation also known as the Business Requirement Documentation (BRD)
- System design and functional requirements documentation

- System development
- Testing (system integration testing and user acceptance testing)
- Business readiness testing to plan for any increase in staffing needs due to a new technical solution, or additional support during Go-Live
- Training development
- Go-live planning
- Production support (BAU processes)

1870. What has the use of technology meant for the staffing of AML/CFT compliance departments?

The increasing use of technology to support AML/CFT compliance means that AML/CFT compliance officers and staff must be tech savvy. As the owners and/or end users of the various technologies used, AML/CFT compliance officers and their teams need to understand the functionality as well as the limitations of supporting technology.

1871. Does an AML/CFT compliance department need dedicated information technology (IT) resources to support the enabling technologies used for its AML/CFT compliance program?

As with any type of technology, a financial institution should ensure it has the appropriate personnel to support its AML/CFT technology needs. As the use of technology has expanded, so too have the skills required to ensure adequate support of these technologies. In addition to compliance, IT, and internal audit expertise, the other skill sets that are required include, but are not limited to:

- Data governance/lineage
- Privacy and information security
- Quantitative/statistical analysis
- Disaster recovery/business continuity

1872. Has the increasing use of technology in AML/CFT compliance programs resulted in the need for fewer people to staff AML/CFT compliance programs?

The answer to this question likely varies depending on the nature of the technology and the maturity of the organisation, e.g., risk assessment technology has helped to reduce the degree of manual effort required to conduct/update risk assessments; KYC utilities have likely lessened, to some extent, the number of people required to develop and maintain KYC information; and better calibrated transaction monitoring and filtering systems have improved the productivity of alerts, requiring fewer people to review and disposition alerts. However, despite these efficiencies, there has been little notable reduction in the overall size of AML/CFT compliance programs as regulatory pressure has continued and AML/CFT compliance staff are being asked to take on more and more responsibilities.

Many financial institutions have started exploring innovative solutions such as Robotic Process Automation (RPA), which eventually may allow them to re-evaluate their staffing models. For further guidance on RPA, please refer to The Future of AML/CFT Technology section.

1873. What information should an institution obtain and retain to support the selection and implementation of a technology solution?

At a minimum, the following information should be obtained and retained to support the selection of a technology solution:

- **Vendor Background Information**: number of years in business, relevant experience, reputation of the company and its principals, size and geographic reach, and financial stability.
- **Technology Functionality**: number of comparable installations, size of largest and smallest installations (in terms of users and transaction volumes), what businesses/products the technology is intended to cover, out-of-the-box scenarios available, ease of customisation, alert and case management features, reporting capabilities, scalability and ongoing availability of vendor support/training.
- **Implementation and Use**: ease of integrating the technology with the institution's platform/core systems, capacity to handle multiple environments (i.e., test and production), expected timeline for installation, frequency of upgrades and user-friendliness for end users.
- **User References**: experience of comparable users, developed through communications with, and/or ideally, site visits to, these institutions.

For additional information on the selection of various types of enabling technology, please refer to the sections below.

Risk Assessment Automation

1874. How can technology be used to support risk assessments?

Risk assessments generally consider multiple quantitative and qualitative factors as well as centralised and decentralised control assessments to determine residual risk. In many institutions, the AML/CFT or sanctions risk assessments begin as a "bottom up" exercise with numerous parties across the organisation providing input. An automated process facilitates the information gathering, making it easier to aggregate results across departments/groups and to develop a consolidated view of risk, and may make it easier to communicate risk assessment results to a broad audience. Automation also facilitates the risk assessment updating process and helps create a more repeatable and sustainable process.

Similarly, customer, product/service and geographic risk assessments, which are key inputs into an enterprisewide risk assessment, typically are based on multiple, risk-weighted factors that must be calculated to derive a risk score. For further guidance on risk assessments, please refer to the following sections:

- Enterprisewide Risk Assessment

- Horizontal Risk Assessment
- Line of Business/Legal Entity Risk Assessment
- Geographic Risk Assessment
- Product/Service Risk Assessment
- Customer Risk Assessment
- Office of Foreign Assets Control/Sanctions Risk Assessment

1875. Does an automated risk assessment process eliminate the need for human intervention?

An automated process may be helpful in removing subjectivity from the rating process, i.e., risk ratings may be systematically calculated based on information provided, rather than relying on individuals to determine risk ratings. However, it is still important to review and confirm the results based on the sound experience of compliance personnel and to afford compliance personnel the authority to adjust systematically-derived ratings, based on adequate written rationale. In addition, model performance should be tracked to facilitate calibration/enhancement over time: e.g., how many overrides were made by compliance reviewers? Was any backtesting performed to evaluate the accuracy of the risk assessment process?

1876. What are the benefits of using technology to support the customer risk rating process?

There are several benefits that result from automating the customer risk rating (CRR) process. For example:

- An automated customer risk scoring process that derives inputs from information collected for KYC purposes eliminates much of the subjectivity that can result from a manual scoring process.
- Automated systems, by their nature, facilitate more dynamic risk ratings, allowing for real time adjustments based on changing circumstances.
- Automated customer risk scores can more easily be incorporated into transaction monitoring systems to create more risk-aware rules and scenarios.

KYC Process

1877. How can technology support the KYC process?

Technology can be used as part of the customer onboarding process to verify customer information (e.g., customer identification program [CIP]); to streamline the collection and exchange of data through the use of KYC utilities; to collect and store customer due diligence (CDD), calculate the customer risk rating (CRR) of the customer, and perform and store enhanced due diligence (EDD) information. Collectively the customer profile of each customer (e.g., CRR, CIP, CDD EDD, associated documents) should be readily accessible to various institutional parties including account officers and

individuals responsible for monitoring and investigation; and to track and schedule the need for customer updates and visitations.

1878. How can technology support the customer verification and authentication processes?

Basic customer information (i.e., customer's name, address and tax ID number) can be digitally verified using positive verification systems that rely on data compiled by the large credit bureaus. For customers with no or limited credit experience, other third-party negative verification tools which incorporate alternative data sources (such as DMV records and criminal background checks and/or matching of a street address to a zip code) may be helpful.

For existing customers for which online identity authentication is necessary (e.g., in the instance where a customer may transact online), financial institutions are increasingly using "out-of-wallet" questions to confirm the customer's identity.

1879. What are out-of-wallet questions?

Out-of-wallet questions are questions to which only the customer knows the answer, i.e., if a customer's wallet is stolen, an identity thief will not know the answer to these questions by simply having a customer's ID or credit card.

Examples of out-of-wallet questions include:

- What was your favourite teacher's name?
- What is your favourite food?
- What was the name of your first pet?
- What street did you live on as a child?
- What is your favourite city?

Typically, a customer would be expected to answer several out-of-wallet questions before verification is confirmed.

1880. What are some of the important decisions that should go into the decision to purchase or subscribe to customer verification tools?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- What is the desired method of verification: positive, negative or logical?
- Does the tool support verification for individuals and businesses?
- Does the tool support verification for domestic and foreign customers?
- Is the verification process conducted in real time or in batch?
- Can the system be integrated with the customer information database?

1881. What is a KYC Utility?

A Know Your Customer (KYC) Utility is a central repository that stores the data and documents required to support a financial institution's KYC procedures. KYC Utilities may take different forms, including:

- Industry Collaborated/Supported Utility: a utility developed and maintained by a consortium of financial institutions
- Service Provider Utility: a utility or service provided by a third-party vendor
- Jurisdictional Utility: a utility designed to undertake core due diligence within a given jurisdiction

1882. What are the benefits of using a KYC Utility?

Leveraging a KYC Utility may offer multiple benefits, both to financial institutions and their customers. For financial institutions, the cost and time for onboarding may be reduced. For customers, the use of a KYC Utility may result in a more positive customer experience if the onboarding process is streamlined and they are not required to provide as much information.

1883. Can a financial institution rely on the integrity and completeness of information provided by a KYC utility?

Except in the instance of CIP where regulations explicitly allow for reliance on another financial institution, a U.S. financial institution is responsible for the integrity and completeness of the KYC information on which it relies. Financial institutions that decide to use a KYC Utility, therefore, should conduct thorough due diligence on the utility to understand what steps the utility takes or requires to ensure the KYC information provided is reliable.

1884. How do KYC Utilities manage customer privacy considerations?

Management of data privacy and data transmission requirements can be a significant challenge and may differ from utility to utility. It is important, therefore, that legal counsel be part of the due diligence team considering the use of a utility to ensure that a financial institution’s participation in a utility does not run afoul of any applicable data privacy or data transmission law or regulation.

1885. What role does customer list screening play in the KYC process?

Customer list screening plays an important part in the initial and ongoing KYC processes. It is used to confirm that a customer is not subject to sanctions, as required by the CIP rule. It is also used to identify customers that may pose higher or unacceptable levels of risk to the institution (e.g., PEPs or PEP-associated customers or individuals or businesses that are the subject of negative news). For additional information, please refer to the Customer and Transaction List Screening section.

1886. What role do internally-developed screening lists play in the KYC process?

Many financial institutions develop “bad guy” lists to capture the names of parties for which they do not want to open accounts or process transactions. These may include former customers on which the

institution has filed SARs and/or which the institution decided it was not interested in serving because of the perceived risk of the customer.

1887. What is a customer risk profile and what is its importance?

A customer profile is an outline or snapshot of customer information which includes demographic, geographic, and financial information as well as expected future behaviour. It provides the foundation for determining whether customer activity is reasonable. Many financial institutions have long-standing processes and procedures in place for developing and maintaining customer profiles. With the adoption by FinCEN in 2016 of its Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule), any financial institution that is subject to CIP requirements is also now obligated not only to develop customer risk profiles that include information developed at account opening, but to update this information throughout the customer relationship, on a risk-based periodic and/or event-driven basis.

For further guidance on the Beneficial Ownership Rule and customer risk profiles, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

1888. Why is it important to automate the collection and storage of CDD and EDD information?

Personnel responsible for reviewing and dispositioning transaction activity must have ready access to customer profiles and supporting documentation. For most institutions, paper-based files which were the norm in the past do not provide complete and timely access and do not facilitate the ongoing updating of customer information that is required.

In addition, certain regulations, such as CIP and USA PATRIOT Act Certifications, may require financial institutions to restrict transaction activity or close accounts with clients for which they do not have complete and current information. If information is maintained in hard copy form, tracking becomes more difficult and the chances of inadvertent non-compliance increase.

For further guidance on CIP, please refer to Section 326 – Verification of Identification. For further guidance on USA PATRIOT Act Certifications, please refer to the Foreign Bank Certifications section.

1889. How can technology support the updating of KYC information?

Simple tickler file software can be used to keep track of due dates for updating KYC information or scheduling customer visits as well as for tracking the expiration date of customer documents, such as identification documents or USA PATRIOT Act Certifications. Workflow features embedded in these systems allow financial institutions to assign follow-up responsibility and to track status.

Customer and Transaction List Screening

1890. What is interdiction software?

Interdiction software, also known as filtering or screening software, is a tool that facilitates the comparison of separate sets of data (e.g., a customer database with a list of individuals/businesses linked to illicit activity) for possible matches.

1891. How can interdiction software be used to support an AML/CFT and OFAC Sanctions Compliance Program?

Interdiction software is used to screen customers and transactions against OFAC Sanctions Listings (e.g., Specially Designated Nationals and Blocked Persons List [SDN List]) as part of an institution's AML/CFT and OFAC Sanctions Compliance Program. It is also used to screen for politically exposed persons (PEPs), 314(a), customised internal lists (e.g., terminated customers) and negative news.

1892. What are the different types of logic used by interdiction software to screen customers and transactions?

Interdiction software uses various algorithms to screen customer names. These algorithms are based on fuzzy logic that may, for example, match a name based on its phonetic pronunciation and not its spelling, or that recognise vowel and diacritic representations, nonstandard word splitting, concatenation, glottal stops, double letters, and consonants not present in Latin-based alphabets.

1893. What attributes should be screened?

In addition to the customer's name (which is a must), the following are additional attributes that may be leveraged to improve the efficacy of the screening process: address, date of birth (or incorporation, in the case of a business), social security number or equivalent, and country of citizenship. The use of additional attributes helps to refine the screening process and eliminate false positive matches.

1894. What are the different types of screening that may be deployed?

Generally, three types of screening are used by financial institutions:

- **Onboarding**: Screening performed when a new customer is onboarded. This is typically performed by querying the screening software. The matching results are analysed and upon clearance the customer is permitted to open an account and conduct transactions on the financial institution's platform.
- **Ongoing**: Screening performed whenever there is a change of either the watch list or customer information. This type of screening is typically of a "batch" nature which means that a systematic process is kicked off at a pre-determined time of the day.
- **Real Time**: Screening that is applicable to transaction activity which is time sensitive, e.g., wire transfer activity. In such an instance, the wire is watch list screened before it leaves the financial institution's payment platform. Since the wire can be originated by the financial institution at any time during the business day due to wire execution response time service level agreements

between customers and financial institutions, screening must be performed on an "as needed" basis within a quick response time (real time).

1895. What are some of the important considerations that should go into a decision to purchase interdiction software?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system include the source lists (e.g., OFAC Sanctions Listings, international sanctions programs [Her Majesty's Treasury [HMT] List], custom lists) in addition to the interdiction software?
- Does the system have the capability to update changes to source lists (changes occur frequently, as names get added or removed from these source lists) on a timely basis?
- Does the system handle screening of customers and all required transaction types (e.g., wires, ACHs)?
- What information is maintained by the vendor (e.g., names and addresses of entities/individuals, background information)?
- What is the matching algorithm (e.g., character by character, fuzzy logic, phonetic, Soundex) used by the system?
- Can end users customise the matching score (e.g., 100 percent match, 90 percent match)?
- Does the system have the ability/methodology to suppress repeat false positives?
- Does the system have match investigation capabilities?
- Is the system hosted by the institution or by the vendor?

1896. What are some common challenges that institutions experience with interdiction technology and its deployment?

There are a number of challenges that institutions may come across when managing interdiction software; some examples include:

- **Lack of Complete Screening Coverage of Customers**: Failure to identify and include all data feeds (e.g., customers from various lines of business) that should be scanned by the sanctions screening system can result in a gap in the sanctions screening program. This can result in incomplete screening of the customer population and breach regulatory requirements.
- **Use of Multiple Sanctions Screening Systems**: More often than not, institutions lacking a centralised sanctions screening strategy deploy multiple sanctions screening systems (e.g., different business segments implement their own sanctions screening systems). This can result in multiple versions of the same watch lists, disparate matching rules and varying threshold values, leading to potentially incomplete and unreliable sanctions screening and possible regulatory compliance issues.

- **Limited Functionality**: Limitations in screening algorithms that do not adequately account for misspellings, line breaks or foreign names or that cannot data match for non-Latin alphabets such as Arabic, Chinese, and Cyrillic.
- **Inadequate Matching Rules**: Out-of-the box or legacy configurations are often limited to simple matching rules such as matching entity names against the respective watch list names. The watch lists often contain additional attributes (e.g., date of birth, ID number, country of citizenship) that can be leveraged for identifying potential hits in a more effective manner (i.e., reduce the number of potential matches generated by applying the additional attributes against customer information, as part of the matching criteria). Utilising only simple matching rules can lead to incomplete monitoring of the bank's customer population and large volumes of "false positives" leading to significant effort spent reviewing system-generated alerts.
- **Data Quality and Completeness**: The quality and completeness of underlying data will significantly impact the volume of alerts generated and the amount of time it takes an individual to review these alerts. Any steps that can be taken to improve this data through the addition of items (e.g., data enrichment such as combining data from disparate systems, manual entry of information from paper files) should be considered as this will both potentially reduce the population that is to be remediated and increase the speed of making a decision on an individual alert.
- **Management Information (MI)**: MI has been used as feedback to the business to improve the data validation and control process to improve future data quality significantly. MI relating to alert generation can be used to establish a continuous improvement process for alert management and configuration (i.e., whether an alert's threshold should be adjusted or whether an alert should be demised as it is deemed obsolete) and for ongoing capacity and resource planning for the analytics and alert handling teams.

1897. What is a matching score and how is it derived?

A matching score is the sensitivity-based setting used to flag potential list screening "hits." Although there is no prescribed methodology for determining how a matching score is set, the following steps provide a high level outline of the steps that should be performed:

- Generate matches in a test environment using the vendor's suggested matching score.
- Select a statistically valid sample of matches and perform a match investigation to determine the quality of matches (i.e., false positives or true matches) that are generated.
- If the results indicate that the matching score value produces good quality alerts, or conversely that it produces poor quality matches, repeat the sampling process by decreasing or increasing the matching score and conducting additional investigations until an optimal (defined by the institution's risk tolerance) level of matches is achieved.

1898. Is there a "right" matching score that should be used for all interdiction systems?

No. The matching score is heavily dependent on the algorithms that are used by the individual interdiction system and, therefore, the matching score used by one system may produce a very different result in another system that uses different algorithms. Furthermore, even if two institutions use the same interdiction system, using the same matching score may not be appropriate because of differences in the customer base (and related nature of customer names) and each institution's risk tolerance.

1899. If a name appears on multiple watch lists, can "hits" be combined into one match to optimise the investigation work load?

Most, if not all, industry standard watch list providers assign a unique entity identifier to the same entity regardless of the number of watch lists on which the entity appears. This identifier can be used to consolidate all matches for the entity.

1900. What types of list providers are currently available?

Various vendors provide lists or databases that include sanctioned individuals and entities (e.g., Specially Designated Nationals and Blocked Persons List [SDN List]), politically exposed persons (PEPs) and subjects of negative media. Lists can be accessed through the internet by conducting ad hoc searches or ingested into an automated screening solution by batch processes.

1901. How does a financial institution determine which lists should be used when screening its customer base?

Financial institutions should discuss their needs and the vendor's sources with their legal departments, peers in the industry or other external advisers, as appropriate, to determine which are required and/or appropriate.

1902. For financial institutions that are headquartered in and only do business in the United States, is it enough just to use OFAC Sanctions Listings?

First, it is important to recognise that OFAC Sanctions Listings is actually comprised of many lists, all of which apply to U.S. financial institutions. Second, U.S. financial institutions must consider the extent to which they are at risk of violations of U.S. embargo programs (e.g., programs administered by the Department of Commerce's Bureau of Industry and Security), and decide whether they should also include these lists in their screening filters. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1903. Is there any advantage to deploying lists from other jurisdictions if they are made available by the list provider?

There are no benefits to deploying superfluous lists which may generate meaningless alerts that an institution will need to adjudicate. However, U.S. offices of a foreign banking organisation may have additional obligations beyond other U.S. domiciled institutions with respect to sanctions requirements of their home jurisdictions.

For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1904. Can a financial institution include/exclude other individuals or entities from vendor-supported screening?

Vendors often provide financial institutions with the ability to add individuals and entities they feel should be monitored beyond lists/names provided by the vendor. In addition, financial institutions may be able to exclude individuals or entities from screening by including these names on "white lists." The development of a white list can reduce the number of false positive alerts that institutions have to review for customers with which they are familiar and know are not subject to sanctions.

1905. What is a "white list"?

A "white list" is a compilation of names that a financial institution has decided to exclude from sanctions screening. The white list typically evolves from false hits that the financial institution has experienced – names that are exact or partial matches to names on a sanctions list, but which the financial institution, through its due diligence, has determined are not true matches.

1906. What are the pros and cons of using "white lists"?

The major benefit of using a "white list" is that it reduces the number of false positives that need to be reviewed and adjudicated. The potential disadvantage of white lists is that they can grow to be unwieldly over time and, if not subject to adequate white list management procedures, may expose a financial institution to avoidable sanctions violation risk.

1907. What are prudent practices for managing "white lists"?

Prudent practices for the management of white lists include, but are not limited, to:

- Limiting the number of people who can add names to the white list
- Screening the white list against applicable updated sanction lists
- Periodically purging the white list by reviewing how often white listed names trigger an alert and removing the names of non-productive white list entries

1908. What are some of the important considerations that should go into a decision to select a list provider?

There are many important considerations that should go into the decision to select a list provider, including, but not limited to, the following:

- Are the updates (e.g., additions, deletions, enhancements) to lists timely (i.e., real time, on demand)?
- Is notification of updates provided to end users?
- Is there an audit trail of when list updates are performed?

- Is supplemental information provided with the name of the individual/entity on the list (e.g., address, aliases, other public information)?
- Do lists include entity consolidation functionality? In other words, can the vendor de-duplicate customer names and watch list names to reduce the likelihood of generating multiple alerts for the same entities?
- Does the system include name dictionaries with variations for different alphabets, such as Chinese characters, Arabic or Cyrillic?
- Can inactive/dormant accounts be screened against list updates?
- Can "white lists" be screened against list updates?
- What different file formats (e.g., XML, CSV) are supported?

1909. How should a financial institution utilise its sanctions risk assessment to implement its sanctions screening program?

Financial institutions should be able to show a clear linkage between their sanctions risk assessments and their sanctions screening programs, i.e., they should be able to evidence how risk assessment results influence their decisions about matching scores as well as their decisions on what parties and transactions will be screened and when. For further guidance, please refer to the Office of Foreign Assets Control/Sanctions Risk Assessment section.

1910. How often should sanctions lists be refreshed?

Determining an acceptable time frame for refreshing the lists used by a financial institution should be a risk-based decision that is made with the knowledge that compliance is required immediately upon a name being added to a sanctions list, e.g., a large multinational financial institution will want to refresh its sanctions lists more quickly than may be necessary for a small institution that has no international activity. At a minimum, however, lists should be updated before the next customer screening cycle is executed.

For further guidance on general considerations for providers relating to technical factors, customer support, cost and disaster recovery, please refer to the Technology Basics section.

1911. Are compliance officers required to certify that sanctions screening programs are in compliance with AML/CFT and sanctions laws and regulations?

Federal AML/CFT and sanctions laws and regulations do not require "certifications." Due to identified serious shortcomings in AML/CFT programs, the New York State Department of Financial Services (DFS) enacted a rule in 2016 requiring annual certifications of transaction monitoring and filtering programs by the board of directors or senior official(s) responsible for the management, operations, compliance and/or risk management of a covered institution.

For more guidance, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications.

Monitoring, Investigating and Filing of Suspicious Activity Reports (SARs)

1912. What types of suspicious transaction monitoring software are currently available?

Several different types of suspicious transaction monitoring software are currently available. Some of the most commonly used AML/CFT technologies include rules-based software; profiling software; and artificial intelligence (AI) software or predictive analysis. Some of the more sophisticated or mature vendors in the industry have incorporated all three types of software into their solutions.

Rules-based software flags any transaction or activity that violates a business rule. These rules are typically modelled to detect known money laundering red flags as published by regulatory agencies and trade associations (e.g., Federal Financial Institutions Examination Council [FFIEC], Joint Money Laundering Steering Group [JMLSG], Wolfsberg Group of Banks, Financial Action Task Force [FATF]). Rules-based software can be customised over time through the addition and/or refinement of rules. Rules-based software is suitable for known patterns of suspicious activity (e.g., structuring, flow-through of funds).

Profiling software uses a combination of predictive profiles developed from a customer's identification and customer due diligence (CDD)/enhanced due diligence (EDD) information, as well as historical transactions. Profiling software is designed to flag transactions that are out of profile by utilising means, standard deviations and thresholds. Profiling software is suitable for both known and unknown patterns of suspicious activity.

In addition to leveraging the features of profiling software, artificial intelligence based systems take into account more upstream applications like KYC to make the process of data collection from multiple sources and systems "more intelligent." Additionally, these systems leverage prior knowledge and rules to link related entities, learn by remembering investigation results and applying them to the current dataset to determine whether an alert should be generated and if it does in fact need to be generated, determine the severity of the alert.

1913. What are the main factors that influence the cost associated with automated suspicious activity monitoring software?

Key cost drivers of automated suspicious activity monitoring software include, but are not limited to, the following:

- Complexity of current system environment (e.g., number of transactional systems, data center locations)
- Customisation requirements of suspicious activity monitoring software functionality and reports
- Customer and transactional data quality; amount of effort required to structure/transform the customer and transactional data so it can be processed by the system
- Resources allocated to maintain, update/optimise, and validate the system

1914. If cost is not a factor, should a financial institution select the most sophisticated transaction monitoring system available?

No. A financial institution should choose the transaction monitoring system that addresses its needs appropriately. Vendors offer a wide array of products and services; the most sophisticated solution may not be appropriate. Highly complex systems require significant implementation time and training. The investment may not be worth the return if the same objectives can be achieved with a different solution, or even a solution built in-house.

1915. What are the important considerations that should go into the decision to purchase a transaction monitoring tool?

Important considerations include, but are not limited to:

- Complexity of current system environment (e.g., number of transactional systems, data center locations)
- Customisation requirements of suspicious activity monitoring software functionality and reports
- Customer and transactional data quality; amount of effort required to structure/transform the customer and transactional data so it can be processed by the system
- Resources that will be required to maintain, update/optimise, and validate the system

1916. How should a financial institution utilise its AML/CFT risk assessments to implement its suspicious activity monitoring program?

Financial institutions should be able to show a clear linkage between their AML/CFT risk assessments and their suspicious activity monitoring programs, i.e., they should be able to evidence that all product/service and customer types, especially those considered high risk are being monitored, and they should be able to demonstrate that identified risk levels inform the suspicious activity monitoring program, e.g., how thresholds are adjusted depending on the level of risk.

1917. What can institutions expect when a transaction monitoring system is implemented?

If monitoring software is implemented poorly, the number of alerts generated can be overwhelming. This can occur when the criteria for generating alerts and setting thresholds has not been fully customised to the size and customer profile of the financial institution; when there is insufficient historical data within the system; when overly conservative variance parameters have been set; or a combination of these factors.

Institutions that follow a rigorous implementation methodology may still require some fine-tuning to optimise the use of the monitoring software, but generally they should expect to see more productive alerts than those generated by the system that was replaced or from manual monitoring.

1918. To what extent can financial institutions rely on suspicious transaction monitoring software?

Even though suspicious transaction monitoring software has become very sophisticated, software is only a tool and just one component of an effective suspicious activity monitoring program. Equally, if not more, important are both the ability of front line personnel to identify and report potentially suspicious activities and the experience levels and knowledge of personnel charged with reviewing and investigating alerts.

Additionally, a financial institution's suspicious transaction monitoring software may not be capable of or configured for monitoring all types of customers, products and/or transactions. For example, trade finance and select correspondent banking activity may require different detection models, the development of a home grown solution or manual monitoring procedures that cover these types of products.

1919. Should a financial institution deploy all of the available scenarios into production?

Not necessarily. The vendor will likely have developed scenarios for financial institutions with various geographic footprints, product and customer types (e.g., retail financial institutions, wholesale and institutional financial institutions, global financial institutions, institutions that provide clearing services). The decision on what scenarios to deploy should be based on the specific business profile and needs of a given institution. While deploying needless scenarios may not have an immediate impact on a financial institution, i.e., meaningless scenarios are not likely to result in significant volumes of alerts, but institutions that are unable to explain to regulators how and why they selected their scenarios may be subject to regulatory criticism. In addition, validating models with extraneous scenarios will unnecessarily drive up the costs of the validation.

1920. Should all customers regardless of type or risk level be monitored using the same thresholds?

No. The threshold values should be based on customer segments (e.g., business, individuals) and be customer risk-aware as this will enable the institution to provide a greater level of scrutiny to its high risk customers as compared to its medium or low risk customers.

1921. What inputs should a financial institution consider when determining what rules/scenarios to deploy in a transaction monitoring system?

At a minimum, the following inputs should be considered:

- Customer type
- Product type
- Services provided
- Geographic footprint
- Typologies published by various bodies (e.g., FFIEC, FATF)

1922. Should a financial institution rely on the recommendations of a vendor on the appropriate thresholds to use?

Apart from thresholds that may be rooted in regulation (e.g., US$10,000 for cash reporting) a financial institution should perform its own analytics to determine appropriate threshold values. This is because every institution's AML/CFT risk profile/risk appetite is different.

1923. What are some key points that a financial institution should consider to ensure effective scenario tuning?

The key points to consider to ensure effective scenario tuning are:

- **Data Analysis Time Period**: The tuning effort should take into account any seasonality factor in the transaction activity to determine the appropriate time period against which the analysis will be performed.
- **Sandbox Environment**: A dedicated environment should be created such that various "what-if" analyses can be performed.
- **Qualitative Testing of Alerts**: Based on the suggested threshold values, pseudo-alerts should be generated and provided to investigators for their feedback to ascertain the effectiveness of the newly suggested threshold values.
- **Metrics**: As part of the tuning exercise, metrics such as false positive rates and the case-to-SAR ratios should be closely tracked since these metrics will enable the tuning team to ascertain the impact of changes in the threshold values to the increase/decrease in alert "noise."

1924. What processes should be in place to ascertain that all data for in-scope customers and transactions are included in the transaction monitoring system?

In order to validate the integrity and completeness of customer and transaction data being ingested into the transaction monitoring system, the following processes should be in place:

- **Data Reconciliation Process:** This process focuses on ascertaining whether the number of customers/transactions in the application database reconciles with the respective source input files/staging tables. This process should also be designed to identify any anomalies – spikes or drop offs – in the number of customers/transactions being processed since this may be an indication of a potential problem, e.g., a core system may have been dropped, a coding change may have resulted in certain transactions being suppressed, an acquisition may have resulted in increased numbers of customers/transactions to the point where the change may call into question the efficacy of scenarios/thresholds currently deployed.
- **Data Integrity Verification Process:** Even though the transaction/customer volumes match with the source files/tables, the referential integrity of the transaction/customer may not be accurately reflected. Therefore, there needs to be a process that will verify the referential integrity of the supplied dataset. This is accomplished by, for example, mapping how the details of different transaction types are captured by the transaction monitoring system.

- **Batch Process Monitoring:** Typically, the data verification processes run in a "batch" (automated) mode. There should be processes in place to notify the respective production support team in the event of a failure of the automated batch run. This will enable the support team to research the problem and prevent the downstream processes (e.g., the alert generation cycle) from commencing before the upstream issues have been resolved.

1925. Are compliance officers required to certify that transaction monitoring programs are in compliance with AML/CFT laws and regulations?

Federal AML/CFT laws and regulations do not require "certifications." Due to identified serious shortcomings in AML/CFT programs, the New York State Department of Financial Services (DFS) enacted a rule in 2016 requiring annual certifications of transaction monitoring and filtering programs by the board of directors or senior official(s) responsible for the management, operations, compliance and/or risk management of a covered institution.

For more guidance, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications.

1926. What circumstances other than automated alerts and employee referrals might prompt the need to identify or monitor customer or transaction activity for potential suspicious activity?

Other potential "triggers" may include 314(a) requests, subpoenas, law enforcement or regulatory inquiries or media reports. For example, the names of individuals and/or companies involved in or potentially involved in money laundering schemes may be disclosed in the press and a financial institution may want to perform an ad hoc search to determine whether it has conducted business for any of the named parties.

1927. What types of case management systems are currently available?

Vendors have developed a variety of case management systems that cover the majority of tasks handled by the AML/CFT compliance department. At a high level, case management systems can be used not only to facilitate the handling of alert and case adjudication, but also to facilitate the Currency Transaction Report (CTR) filing and exemption process, the follow-up on customer documentation exceptions, and the review and regular update of customer risk ratings and profiles.

1928. What are some of the important considerations that should go into a decision to purchase a case management tool for alert and case adjudication?

In many instances, institutions acquire a case management module as part of a transaction monitoring system. Nonetheless, institutions should still evaluate the functionality of the case management module to ensure it meets the institution's needs. There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system have the ability to import data from multiple sources (e.g., transaction monitoring alerts, internal referrals, external sources)?

- Does the system have the functionality to allow for clear and complete explanation of alert and case disposition?
- Does the system have workflow management capabilities (e.g., assignment of cases, multi-user-level hierarchy)?
- Does the system allow for grouping and cross-referencing of alerts?
- Does the system have the ability to upload attachments (e.g., internal email; research, such as internet; correspondence with customer; customer identification information)?
- Does the system have the ability to export summaries of investigations out of the system?
- Does the system have record retention abilities to retain cases for future investigations, examinations and audits?
- Does the system have pre-built reporting templates that allow for automatically populating and filing SARs? If not, can these features be easily customised and incorporated?
- Does the system allow for different ways (e.g., date, customer name) of searching for past alerts and/or cases?

1929. What is a case workflow and how does it help with investigations?

Case workflow is a technical implementation of the alert investigation process from an alert/case lifecycle point of view. Essentially, case workflow captures each and every "stage" the alert/case goes through before it is closed. Automating the alert investigation process (by creating and maintaining the case workflow) significantly improves the alert investigation process as it eliminates the need for the manual movement of alerts/cases from one individual to another. Additionally, it promotes efficient tracking of alerts (e.g., alert aging, investigator throughput).

1930. How does AML/CFT technology support the preparation and filing of SARs?

Existing vendor technologies support the collection of data from various sources and the auto-population and e-filing of SAR forms. These technologies can improve the accuracy and speed of the SAR process. For further guidance on SARs, please refer to the Suspicious Activity Report section.

1931. Can investigation and SAR filing activity be linked to a customer's profile?

Yes, all industry standard case management software allows the association of investigation and SAR filing activity to the customer's profile. This capability significantly enables future investigation of alerts/cases for the same customer.

Large Currency Transaction Monitoring and Filing of Currency Transaction Reports (CTRs)

1932. What types of currency transaction monitoring and CTR filing solutions are currently available?

Available CTR filing solutions range from stand-alone systems that function in the back office only and therefore are nightly batch driven to fully integrated solutions that provide real-time aggregation to the front office. Additionally, some systems include functionality to monitor for suspicious currency activity and manage the financial institution's Currency Transaction Report (CTR) exemption process.

1933. What are some of the important considerations that should go into a decision to purchase a currency transaction monitoring and CTR filing solution?

There are many important considerations that should go into this decision, including, but not limited to, the following:

- Does the system have real-time aggregation?
- Does the system handle aggregation for foreign customers and/or foreign currencies?
- Does the system link related customers?
- Are noncustomer transactions captured?
- Does the system include all currency transactions (e.g., ATMs)?
- Can the system integrate with a customer information platform (i.e., automatically upload from a customer information platform or manually entered information)?
- Does the system have an intrinsic case management feature (e.g., assign cases to multiple users, document reason for not filing a CTR)?
- Does the system facilitate the electronic filing of CTRs, the CTR amendment process and/or the CTR exemption process?
- Does the system include a reporting/trending capability for historical CTR filings?
- Does the system have record retention capabilities to comply with recordkeeping requirements for CTRs?
- Can the system link up with transaction monitoring systems to trigger SARs for instances of structuring?

Training Software

1934. How can technology support AML/CFT training?

Technology can provide an efficient and effective way of deploying training to a large audience. Numerous vendors, for example, offer basic AML/CFT and sanctions training which companies require all of their employees to complete. Other companies use technology to deploy in-house developed

customised training programs to select audiences within their organisations. Technology can also be used to assign training courses, track completion, and document results of comprehension testing.

1935. What are some of the important considerations that should go into a decision to purchase third party-developed training?

The most important consideration that should go into a decision to purchase any third-party training program should be the applicability to the needs of the organisation (e.g., an AML training program developed for a domestic retail banking market will have little applicability to a wholesale foreign bank branch or a broker-dealer). Other important considerations include understanding the frequency at which the vendor updates training modules to deal with regulatory changes and the user-friendliness of deploying the training.

Management Reporting

1936. What is management reporting?

Management reporting is a process through which management (and the board of directors) are provided, routinely and on an as-needed escalation basis, the information they need to manage the operations and risks of the organisation. Management reporting will vary depending on the type of financial institution, the nature of the products and services it offers, and the clients it serves. The following are non-exhaustive examples of key risks and key performance indicators and other information related to the AML/CFT Compliance Program that may be considered:

- **Suspicious Activity Reports (SARs) and significant investigations**
  - Number of SAR filings and associated volume of suspicious activity and deposit/lending balance of named subjects
  - Explanations for significant changes in volume of SAR filings
  - Volume of alerts, investigations
  - Aging of alerts and investigations
  - Alert-to-investigation ratio, investigation-to-SAR ratio
  - Summary of significant investigations (e.g., high volume of suspicious activity, uncovered weakness in monitoring program, investigations involving insiders, politically exposed persons [PEPs])
- **Currency Transaction Reports (CTRs)**
  - Overall volume of cash activity
  - Number of CTR filings and associated volume of cash activity
  - Explanations for significant changes in volume of cash activity/CTR filings
- **Office of Foreign Assets Control (OFAC) and other sanctions reporting**

  - Number of OFAC blocked/rejected report filings and associated volume of blocked/rejected activity and deposit/lending balance of named subjects
  - Aging of "hits"
  - Results of OFAC/sanctions risk assessment

- **Information sharing**
  - Number of confirmed 314(a) matches and associated deposit/lending balance of named subjects
  - Number of incoming/outgoing 314(b) requests and associated deposit/lending balance of named subjects
  - Number of National Security Letters (NSLs)
  - Number of subpoenas and other information requests

- **Training**
  - Number of exceptions (e.g., employees who have not completed or who have failed training)
  - Summary of significant updates to the training program

- **Staffing**
  - Significant staff changes, turnover trends, approved and unfilled positions

- **Technology**
  - Major changes to the automated systems being used to support the company's AML/CFT Compliance Program and rationale for the changes
  - Status of any major technology implementations, upgrades or changes affecting the AML/CFT Compliance Program
  - Results of independent validations of supporting technology models

- **Third-party reliance**
  - Periodic discussion of any third parties on which the company relies for any part of its AML/CFT or sanctions compliance programs and actions taken by the company to satisfy itself with third parties' compliance efforts

- **Risk assessments**
  - Results of executed AML/CFT risk assessments (e.g., enterprisewide risk assessment, horizontal risk assessment, line of business/legal entity risk assessment, geographic risk assessment, product/services risk assessment, customer risk assessment, OFAC/sanctions risk assessment), including inherent risk, ratings of controls/control environment and residual risk

  - Changes in the institution's risk profile and explanations for what is driving the change
  - Summary of significant changes to risk assessment methodologies
  - Number of high-risk customers and associated deposit/lending balances
  - New products/services/transaction types and associated risks
  - New target markets (e.g., customer type, geography) and associated risks
- **Examination/independent testing/self-testing findings**
  - Summary of findings and status of corrective actions
- **Changes in laws, regulations or regulatory expectations**
  - Summary of new requirements and their impact on the company
- **Current events**
  - Details of recently reported money laundering/terrorist financing schemes, to the extent that the company may, because of its products/services and customers, be subject to risk and discussion of controls in place to mitigate such risks
  - Summary of recent AML enforcement actions and relevance of the issues cited to the financial institution

The content, level of detail and frequency of reports should be tailored to the audience (e.g., business line management, compliance, risk management, senior management, or board of directors).

1937. How can technology help with management reporting?

There are numerous business intelligence (BI) tools (e.g. Cognos, Microstrategy, Tableau) available in the market that enable the AML/CFT Compliance team to connect their compliance "datamart" to the system to generate reports that provide meaningful insights to a variety of AML/CFT stakeholders. A typical BI implementation enables the AML/CFT compliance team to track various metrics related to its suspicious activity monitoring program (e.g., number of SARs filed, aging alerts, number of alerts pending requests for information [RFIs]) and other aspects of its AML/CFT Compliance Program (e.g., OFAC alerts, 314(a)/(b) information requests, CTRs).

Model Validation

1938. What is a model?

The term model refers to a quantitative method, system, or approach that applies statistical, economic, financial, or mathematical theories, techniques, and assumptions to process input data into quantitative estimates. Models meeting this definition might be used for analysing business strategies, informing business decisions, identifying and measuring risks, valuing exposures, instruments or positions, conducting stress testing, assessing adequacy of capital, managing client assets, measuring compliance with internal limits, maintaining the formal control apparatus of the bank, or meeting

financial or regulatory reporting requirements and issuing public disclosures. The definition of model also covers quantitative approaches whose inputs are partially or wholly qualitative or based on expert judgment, provided that the output is quantitative in nature.

1939. Based on the definition of "model," are all AML/CFT systems models?

Typically, although there can be exceptions, transaction monitoring, sanctions screening and customer risk scoring systems are considered models whereas systems, such as a CTR system that relies on simple addition and not advanced mathematical theory, are not considered models. A CTR system may be considered an end-user calculation system, which also requires validation, but in a far more streamlined fashion than a full quantitative model.

1940. What is model governance?

Model governance refers to the processes and frameworks by which an entity manages its models. These processes and frameworks include, but are not necessarily limited to: the roles and responsibilities of the board, management, and business units across the model life cycle; independent model validation; maintenance of a model inventory; standards for model documentation; change control management; access controls; ongoing monitoring programs; and model risk control requirements.

1941. What guidance have the regulators provided on model governance?

In April 2011, the OCC and FRB jointly issued guidance on model risk management, which is reflected, respectively, in the following:

- **OCC Bulletin 2011-12** – Supervisory Guidance on Model Risk Management
- **FRB SR 11-7** – Guidance on Model Risk Management

In July 2016, the DFS finalised its **Part 504 – Transaction Monitoring and Filtering Program Requirements and Certifications.** While the DFS guidance is specific to certain DFS-regulated financial institutions, the basic principles included in these documents have become the standard for financial institutions in the U.S., regardless of the responsible regulator.

1942. Who are the key players in an effective Model Governance Program and what are their roles?

While the key players may vary somewhat from institution to institution, they typically include the following:

- The **Model Owner**, who is often the BSA/AML Officer or the Head of Transaction Monitoring, who is responsible for:
  - Ensuring robust model development, implementation, use and maintenance for each of the in-scope models.

  - Ensuring that periodic independent validations occur and that ongoing tuning is performed on the in-scope models, which may include recommending scenarios for development, decommission or modification.
  - Performing, in concert with other responsible parties, initial and ongoing due diligence of third-party vendors who supply or service models, or provide model inputs for the institution's use.
  - Ensuring that in-scope models are appropriately considered in the institution's disaster recovery program.
  - Maintaining documentation for all areas of AML/CFT model risk management, including but not limited to, the model inventory, model user procedures, model validation results, tuning and optimisation testing results, and disaster recovery testing results.

- **Information Technology**, often a dedicated Compliance or AML/CFT Technology Group, or an individual within the Chief Data Officer's (CDO) group, which would be responsible for:
  - Ensuring the completeness and the integrity of the data that is ingested into the in-scope models.
  - Advising AML/CFT compliance, in advance, of any technology changes that may impact the use or performance of the in-scope models.
  - Working collaboratively with AML/CFT compliance to support the installation or upgrade of AML/CFT and sanctions-related models.
- **Independent Model Validation**, which may be a qualified, independent internal group (such as an independent model validation team—generally in the risk group, or second line of defence) or an independent third-party provider which is responsible for the periodic independent validation of the models, including:
  - Documenting the scope, approach and results of data integrity testing to ensure the accurate and sound nature of data imported from source systems.
  - Documenting the scope, approach, test cases and results of logic validation testing to ensure the ongoing appropriateness and effectiveness of scenarios and thresholds, to ensure the models operate as intended.
  - Presenting findings from the periodic model validations to the AML/CFT Compliance Officer and other responsible parties, such as the Model Risk Management Office or Committee, senior management, responsible AML/CFT Committees, and the board of directors.
- **Internal Audit**, which is responsible for testing adherence to the institution's model governance policy, including:

- Evaluating whether the institution adheres to policy, procedures and regulatory expectations for the selection, installation, testing, and ongoing maintenance of any models used to support the AML/CFT Compliance Program.
- Determining whether the model validation of in-scope models meets with U.S. regulatory expectations and that conclusions reached are adequately supported by analysis performed/work papers.
- Evaluating the accuracy and completeness of the model inventory and the processes for establishing and monitoring limits on model usage.
- Evaluating procedures for updating models to ensure that they are clearly documented and tested to determine whether the procedures are being followed.
- Evaluating whether the model owner is complying with documentation standards, including risk reporting.
- Periodically performing audits of the integrity and completeness of data used in the models.
- Tracking and reporting any outstanding issues identified in model validation and/or internal audit reports that affect the use and reliability of models.

1943. What is model validation?

Model validation is an exercise conducted by an independent team (i.e., a team that does not directly own the model in question) to ascertain whether the subject model is working as intended. The effort involves execution of a battery of tests against data (e.g., transactions, customers, accounts), logic (e.g., scenario logic, risk rating calculation) and outputs (e.g., alerts, assigned risk scores) to ascertain whether the respective test results are in accordance with the expected test results.

1944. Who should perform a model validation?

It is a regulatory expectation that the model validation should be performed by a party independent of the model owner and approver, and with the requisite technical and subject matter expertise to be able to perform the necessary tasks. In our experience, model validation is typically performed by an internal model validation team or an outsourced provider.

1945. What are the main steps in the validation of a transaction monitoring model?

The following steps need to be executed to validate a transaction monitoring model:

- **Model Governance Review**: This step involves evaluating the framework the financial institution has in place to manage the selection and maintenance of all models used in the support of its AML/CFT compliance program
- **Data Quality Review**: This step involves determining the quality and completeness of the key data elements. Since a transaction monitoring system is heavily dependent on the availability of good data, it is imperative to confirm that the transaction monitoring system is supplied with a complete and reliable dataset that meets the data quality standards of the financial institution.

- **Logic Validation**: This step involves determining whether the in-scope scenarios are functionally executing as defined in written specifications.
- **Threshold Values Validation**: This step involves determining whether the threshold values of the in-scope scenarios are calibrated correctly.

1946. What support should a financial institution have for decommissioning a rule or scenario?

Although there is no documented benchmark around what the financial institution should do before decommissioning a scenario, the institution should maintain a detailed log that evidences that the scenario that is a candidate for decommissioning has not:

- Been deemed as a productive scenario;
- Resulted in a productive alert for some prescribed (e.g., 12 months, 18 months) period of time; or
- Resulted in cases (indicating a more detailed review of the alert was required).

1947. What are the main steps in the validation of a list screening model?

The following steps need to be executed to validate a list screening model:

- **Model Governance Review:** The objective of this step is to evaluate the policies, procedures and practices an institution has in place to manage the selection and use of a list screening model, including, but not limited to, its access controls, change management processes, and disaster recovery back-up.
- **Source Data Review:** During this step, the completeness and quality of the data being fed to the interdiction software is evaluated. Data feeds should be reconciled to ensure that all the appropriate sources of data are being captured and tests should be performed to ensure that data details are being sourced completely and to the correct fields.
- **Sanctions and Watch Lists Selection:** Similar to the red flag review that is performed to ensure alignment between an institution's AML/CFT risk assessment and the scenarios deployed for transaction monitoring, an institution should also ensure that its list selection is guided by the risks of its customers, products/services and geographic footprint as captured in its OFAC/Sanctions Risk Assessment.
- **Alignment of Matching Score with Risk Appetite:** An institution should also consider its own risk profile and risk appetite. Generally, if an institution's overall sanctions risk assessment is "high," the institution will choose a lower matching coefficient, while an institution with a lower risk assessment may prefer a higher matching coefficient (as this would result in fewer potential matches). Institutions will need to test a sample of alerts to determine if the output is in line with its risk appetite.
- **Identification of Matching Rules:** A financial institution should also determine what matching criteria (beyond name) is provided by the solution, and whether this criteria is being used effectively to minimise unproductive alerts.

- **Testing of Matching Capabilities:** This is one of the more complex tests, as it can be difficult to replicate independently the algorithms used by vendor firms. Rather than replication, the matching algorithms can be tested by taking the following two approaches:
  - Sample Testing: Institutions can create a "good sample" (entities that are not on the watch lists) and a "bad sample" (entities known to be on the watch lists), and then run these names through the system to determine whether or not they generated an alert.
  - Name Masking: Institutions can create multiple variations of the "bad sample" in order to test how effective the matching algorithm is. This is done to test the capability of the system to apply "fuzzy logic" to match the altered names against the names on the watch lists.

1948. What are some common name-masking techniques that can be applied to test the fuzzy logic?

Some common name-masking techniques include:

- **Soundex:** Soundex is a phonetic algorithm for indexing names by sound, as these sounds are pronounced in English, such that names that are pronounced similarly are encoded to the same representation so they can be matched despite differences in spelling. For example, Mary can be matched to Marie, and Carmen can be matched to Carman.
- **Containment:** The objective of the containment algorithm is to use only a portion of the name to determine whether the system will produce a match. For instance, Matthew may be truncated to Matt, and Robert to Rob. The purpose of this algorithm is to ensure that systems can match an entity based on an abbreviation of the name.
- **Extraneous characters:** The purpose of this algorithm is to introduce stray characters into the name and test whether the system is able to bypass these extraneous characters and match the name against entries in the watch list. For example, the system should be able to match "ODonnell" and "O'Donnel."
- **Permutations:** Permutations are achieved using various combinations of first, middle and last name. For example, switching the last and first name while leaving the middle (if applicable) name is one possible variation. Another example is taking the first initial of the first name and leaving the rest of the name unchanged.

1949. Why would an institution consider adjusting the sensitivity settings for its sanctions screening system?

Generally, sensitivity settings/fuzzy logic will be calibrated as part of a model validation. However, the model owner/users may identify the need to make adjustments outside of the model validation process. This may happen if there is empirical evidence that the current settings are not optimal (e.g., there is an unwieldy volume of false positives) or it becomes clear that there is an error in the way the settings were configured versus what was intended. In the latter case, it is important first to identify the root cause of the error before any change is made to the system.

1950. What are the main steps in the validation of a customer risk rating model?

The following are the steps that need to be executed to validate a customer risk rating model.

- **Model Governance Review:** This step involves evaluating the program the financial institution has in place to ensure an adequate framework for the selection and maintenance of all models used in the support of its AML/CFT compliance program.
- **Data Quality Review:** This step involves determining whether the quality of the key data elements is in line with the expectation. As a customer risk rating model is heavily dependent on the availability of good data, it is imperative to ensure that the customer risk rating model is supplied with a dataset that meets the data quality standards of the financial institution.
- **Risk Scoring Logic Validation:** This step involves determining whether the risk scoring logic employed by the system is able to:
  - Assign appropriate scores for each of the identified risk factors;
  - Consolidate the individual scores into a single overall score; and
  - Assign the appropriate risk level based on the overall risk score.

1951. When and at what frequency should a model be validated?

Although there is no specific guideline around the frequency at which a model should be validated, existing regulatory guidance requires that an institution assess the need for a model validation on at least an annual basis. Determinants of need would include factors such as changes in an institution's business (in its customer and/or product/service mix) or previously identified gaps which may have been remediated, but have not been validated.

1952. What support should a financial institution have for decommissioning a rule or scenario?

Although there is no documented benchmark around what the financial institution should do before decommissioning a scenario, the institution should maintain a detailed log that evidences that the scenario that is a candidate for decommissioning has not:

- Been deemed as a productive scenario;
- Resulted in a productive alert for at least 18 months; or
- Resulted in cases (indicating a more detailed review of the alert was required).

Data Analytics

1953. How can data analytics enhance an AML/CFT compliance program?

Data analytics allows organisations to enhance the full lifecycle of their AML/CFT compliance program through a range of capabilities from descriptive (what happened/is happening?), to predictive (what may happen next?), to prescriptive (what should we do next?). Through analysis of KYC parameters, past transactional behaviour, as well as incorporation of government- and third-party-published

information, an organisation can not only better understand what types of customers and activity are presenting AML/CFT risk but also predict what customers and activity may present heightened risk to the institution in the future. Data analytics can support the breadth of AML/CFT activities from identification of optimal models; detection of suspicious parties or activity amongst millions of data points; alert and case management including routing, prioritisation, and even dispositioning; and, finally, providing a critical feedback loop to ensure that an AML/CFT compliance program adapts over time to emerging threats.

1954. What is customer segmentation?

Customer segmentation is a technique by which the customers are sorted into different groups. The segmentation is done by leveraging KYC attributes of customers, their transactional activity or combining the two datasets. Examples of customer segments are: High Transaction Activity customers (determined by leveraging transactional data), and Non-Resident Aliens (NRA) customers (determined by leveraging KYC data).

1955. Can customer segmentation be leveraged to enhance transaction monitoring?

Yes, leveraging customer segmentation enables the institution to deploy highly targeted threshold values for suspicious activity monitoring scenarios. Furthermore, customer segmentation promotes the decoupling of a customer's AML/CFT risk with transaction activity thus further enabling the institution to deploy threshold values which are not only at the customer risk level but at a combination of risk level and customer segment which is one level finer than just determining the thresholds at the customer risk level.

1956. What is transactional activity based segmentation?

Transactional activity based segmentation is an approach of segmenting customers based on their past transaction activity. In this approach, the customers that have similar transaction activity are grouped into the same segment which enables the threshold setting/tuning team to determine/tune threshold values that are specifically targeted for the respective segment.

1957. How can transactional activity segmentation be leveraged in a customer risk scoring model?

Transactional activity based segmentation can be leveraged in customer risk scoring models by identifying natural cuts in the transaction activity exhibited by the institution's customer base. Subsequently appropriate "points" can be assigned to each natural cut of transaction activity which can then be aggregated with other risk factors (e.g., customer's occupation, PEP status) to determine the overall customer risk score and therefore the customer risk rating.

By leveraging transactional activity based segmentation, the customer risk rating model can be made more dynamic versus merely using customer attributes like occupation or PEP status, as they generally will not change over time.

1958. What is Extract Transform and Load (ETL) processing and how can it support an AML/CFT compliance program?

Extract Transform and Load (ETL) processing is one of the most often used data constructs as part of typical system implementation and maintenance. In a typical ETL process, data is fetched from the data repository/ies (extract). After extraction, the data is formatted in a manner such that it is acceptable to the target system (transform) and finally persisted on the target system (load).

As all AML/CFT systems are heavily data dependent the ETL construct can be leveraged to systematically load the required data sets into the target systems. Tools such Informatica and Ab Initio are some of the industry standard tools that offer out of the box ETL capabilities.

1959. What are examples of some of the tools that can be used for data analytics?

The common software products that are used for AML/CFT data analytics are SAS, R and Tableau. The common techniques leveraged are focused around distribution analysis, clustering analysis and correlation analysis.

The Future of AML/CFT Technology

1960. What is fintech?

Financial Technology (fintech), describes a business that aims to provide financial services by making use of software and modern technology. It is an application of technology based solutions to the financial services industry with a key objective of improving the efficiency of the underlying business processes. Examples of fintech include, but are not limited to, payment processors, money transmitters, lending firms, and automated stock portfolio recommenders/balancers.

Banks and other financial institutions are also trying to innovate from within their organisations. They achieve this by either partnering with fintech companies, creating their own innovation hub, where they invite fintech firms to innovate within the bank's technology infrastructure or by purchasing the fintech firm outright.

1961. What is regtech?

Regulatory Technology, or simply regtech, is a specific branch of fintech that focuses solely on the application of a technology framework to automate various regulatory business processes. Like fintech, regtech applies the same nimble, scalable, mobile-friendly solutions and rapid, low-cost deployment to improve risk management, transaction monitoring, regulatory compliance, reporting, data storage and analytics. It offers new ways of solving old problems by offering speed, security, and agility in complying with regulatory requirements. As such, financial institutions have good reasons to look forward to implementing the technology.

Although regtech is still in its infancy and the market is very fragmented, it has the potential to replace many of the traditional manual and paper-based solutions which also tend to be resource-intensive, tying up both capital and IT capacity.

Applied to AML/CFT compliance, a regtech real-time transaction monitoring solution can bridge communication gaps by consolidating and analysing data from disparate systems. Applied to KYC processes, regtech can be used to create a secure central data repository with reference data utilities to protect personally identifiable information. The technology also can monitor financial services regulations in every country and region within an institution's footprint and report back to internal audit. Risk Reporting (Management Reporting) is also a feature that many financial institutions and regtech firms are improving by providing on-demand and visual renditions of various static reports.

1962. Have regulators taken a position on the use of regtech solutions?

U.S. regulators (notably the OCC and CFPB) have expressed an openness to exploring the capabilities of fintech and regtech.

The OCC has defined Responsible Innovation as the use of new or improved financial products, services and processes to meet the evolving needs of consumers, businesses, and communities in a manner that is consistent with sound risk management and is aligned with the bank's overall business strategy. The OCC has established an Office of Innovation and has implemented a framework supporting responsible innovation. The office serves as the central point of contact and clearinghouse for requests and information related to innovation.

The CFPB's Project Catalyst initiative is designed to encourage consumer-friendly innovation. In October 2016, the CFPB released the first Project Catalyst report. The CFPB wants to engage closely with companies, entrepreneurs, and other stakeholders who are at the front lines of innovation.

The U.K.'s Financial Conduct Authority (FCA) has also been a proponent of fintech. It has developed a regulatory sandbox that allows businesses to test innovative products, services, business models and delivery mechanisms in a live environment.

1963. How is regtech different from traditional technology solutions?

While the confluence of regulations and technology is not new, regtech firms are bringing new solutions to existing (old) problems. The focus of such firms is to bring about innovative solutions whose hallmarks are agility, flexibility and ease of implementation.

Regtech firms are bringing about process efficiencies within existing functions, such as Robotic Process Automation to clear simple transaction monitoring alerts. They also focus on simplification, such as visual reporting and dynamic on-demand reporting vs. creating static reports.

1964. How might regtech change the landscape for AML/CFT technology?

Regtech provides the means to automate more routine compliance tasks and harness and use data in a way that improves decision-making, provides additional insights, and most importantly, saves costs. Some trends in the AML/CFT space are listed below, and some are actually in the process of being implemented at various financial institutions:

- Regtech firms could partner with existing transaction monitoring vendors to determine better ways of rendering alerts and tying them to KYC data that allows investigators to have all the information they need to clear the alert(s)

- Predictive analytics and artificial intelligence built within transaction monitoring systems to eliminate or reduce false positives or false negatives
- Case management tools can be created with robotic capabilities to bring about process efficiencies to eliminate most of the manual tasks
- KYC systems will be able to make regular and automated calls to screening tools to determine customer risks associated with indicators such as OFAC sanctions listings, PEPs and negative news
- Leveraging blockchain technology to enhance the KYC functions within and across banks
- Visual analytics and reporting at the push of a button

The above are just a few examples of where regtech firms and banks are innovating to bring about significant change in the coming years.

1965. What is a blockchain, and how can it be used to support AML/CFT compliance?

Blockchain technology, also known as distributed ledger technology (DLT), is generally defined as the secure distributed ledger of digital events that uses consensus and cryptography to validate each transaction while also protecting the identities of all participating parties. Bitcoin and similar cryptocurrencies first used blockchain technology, but there are many applications of this technology that can be used to support AML/CFT compliance. By design, blockchains are intended to be immutable once information is recorded. Blockchain could play a significant role in streamlining the KYC process if used for KYC repositories where information could be used by eligible, participating financial institutions, thereby eliminating the need for customer outreach. The KYC data is unique, and it is impossible to create two conflicting entries into this system.

1966. What is robotic process automation (RPA) and how can it be used to support AML/CFT compliance?

Robotic process automation is the ability of the system to capture relevant information, analyse that information and take appropriate action to move the task at hand to the next step in the respective business process. A practical application of robotic process automation is the ability to capture the publicly available information for a given alerted customer, populate it in the alert investigation form and discern whether the alert can be closed as false positive or needs to be moved to a human being for a detailed investigation.

1967. What is artificial intelligence and how can it be used to support AML/CFT compliance?

Artificial Intelligence (AI) is a branch of software engineering that focuses on automatically making decisions for the problem at hand based on the decisions made in the past for the same problem. AI can be used in AML/CFT compliance in following areas:

- Automatically closing alerts that are false positives
- Automatically changing the risk rating of the customer based on the changes in the publicly available information

- Automatically performing CDD for low- and medium-risk customers

1968. Are there any added risks to these new technologies?

The opportunities for such technologies in compliance automation, AML/CFT and management reporting are many and exciting. Financial institutions historically have struggled to comply with new regulations, in part because the compliance processes were rigid and not easily changed. As this field matures, risk and compliance functions are likely to see increased operational excellence. Underlying data will become more reliable, enabling better decisions; adoption of new controls and compliance procedures will get faster and easier; and senior management will be able to manage risk more effectively.

The same thing that makes regtech attractive to the market – its agility and flexibility – may also be what presents risks in that the technologies may not undergo the same rigorous development processes as traditional technology. That said, all technologies are only tools and not in and of themselves the keys to a successful compliance program.

While financial institutions may rely on regtech vendors, this does not mean that these vendors assume the risk of the institution. While the IT burden of implementation and maintenance of the new technology may be reduced, there is a new and growing responsibility for institutions to vet and monitor vendors to ensure that the providers' policies, values and procedures align with those of the organisation — especially when it comes to privacy and cybersecurity.

Also, while automation can improve processes, it is critical for financial institutions to review all risk and compliance procedures during project planning to avoid accelerating bad or obsolete processes, and to verify data integrity to ensure that reports are accurate and reliable.

NONBANK FINANCIAL INSTITUTIONS AND NONFINANCIAL BUSINESSES

NBFI Basics

1969. What is meant by the term "nonbank financial institution" (NBFI)?

For purposes of our discussion, NBFIs include all entities, excluding depository institutions, considered to be financial institutions under the Bank Secrecy Act (BSA). These include, but are not limited to, the following:

- Money services businesses (MSBs) (e.g., licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally; currency exchanges; issuer or seller of traveller's checks, money orders or similar instruments; sellers or providers of prepaid access)
- Broker-dealers in securities
- Futures commission merchants (FCMs) and introducing brokers (IBs)
- Commodity trading advisers (CTAs)
- Commodity pool operators (CPOs)
- Mutual funds
- Insurance companies
- Casinos and card clubs
- Operators of credit card systems
- Dealers in precious metals, precious stones or jewels
- Persons involved in real estate settlements and closings
- Investment advisers
- Unregistered investment companies
- Loan or finance companies (e.g., nonbank residential mortgage lenders and originators [RMLOs])
- Housing government-sponsored enterprises (GSEs)
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Travel agencies
- Pawnbrokers
- Telegraph companies

For additional guidance on how requirements apply to the types of companies listed above, please refer to the respective questions below.

1970. Some of the companies identified as NBFIs are not "financial institutions" in the traditional sense (e.g., pawnbrokers, travel agencies, telegraph companies). Why are they included as "financial institutions"?

Just as is the case with traditional financial institutions, the companies included under the definition of "financial institution" may provide opportunities to money launderers and terrorist financiers (e.g., because they are cash-intensive and/or because they facilitate the conversion of funds into goods that can be used or resold).

1971. Do NBFIs have to comply with all the same provisions of the BSA and USA PATRIOT Act as traditional financial institutions?

Not all provisions of the BSA and USA PATRIOT Act apply to all NBFIs. Currently, the following NBFIs are exempt from the requirement to maintain an AML Program under Section 352 of the USA PATRIOT Act:

- Pawnbrokers
- Travel agencies
- Telegraph companies
- Sellers of vehicles, including automobiles, airplanes and boats
- Persons involved in real estate closings and settlements
- Private bankers
- Commodity pool operators (CPOs)
- Commodity trading advisers (CTAs)
- Investment companies

Additionally, NBFIs that are subsidiaries of bank holding companies (BHCs) are typically included in the enterprisewide AML/CFT Compliance Program and subject to organisational requirements to establish an AML Program. Some of the differences in application are highlighted in the questions below.

For additional guidance on the various AML/CFT requirements common to many NBFIs, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections.

1972. With which provisions of the BSA and USA PATRIOT Act should an institution that is in multiple businesses (e.g., banking, broker-dealer, insurance) comply?

At a minimum, individual financial institutions that are subject to issued AML/CFT regulations must comply with the specific requirements applicable to their industry. In addition, many diversified organisations with subsidiaries that are subject to AML/CFT regulations issued by multiple agencies

have chosen to implement enterprisewide AML/CFT standards that apply to all entities within the organisation. Of course, some or all of the entities within the organisation may need to implement more detailed policies and/or procedures to implement requirements specific to their industries.

It is also worth noting that federal banking regulators have indicated that nonbank subsidiaries and affiliates of insured banks should have effective Customer Identification Programs (CIPs) in place, even though CIP requirements may not apply to these entities by regulation.

It is important to note that some NBFIs are subject to state AML/CFT laws and regulations that may impose more stringent requirements on the NBFI (e.g., recordkeeping and suspicious activity reporting requirements for lower transaction thresholds than the federal requirement, record retention periods that are longer than the federal requirement).

1973. Are NBFIs required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

1974. What are the heightened money laundering and terrorist financing risks of NBFIs?

The following characteristics, which may apply in varying degrees, may heighten the money laundering and terrorist financing risks of NBFIs:

- Cash-intensiveness
- High volume of transactions
- High-risk nature of customer base (e.g., high net worth; geographically dispersed; financially sophisticated; increased use of corporate structures, such as offshore private investment companies; lack of ongoing relationships with customers, such as money services businesses [MSBs] and casinos)
- High-risk product offerings (e.g., ability to transfer funds domestically and internationally, particularly to jurisdictions with weak AML/CFT requirements; stored-value cards; transportability of merchandise; high-value merchandise; merchandise that is difficult to trace, such as precious stones)
- Ability to transfer value (e.g., conversion to precious gems, immediate or deferred income through insurance and other investment products, real estate)
- Access to funds held in foreign financial institutions or access by foreigners to funds held in domestic financial institutions
- Historically less regulated or less stringently regulated than traditional financial institutions, such as depository institutions

- Potentially weaker controls than traditional financial institutions due to fewer regulatory pressures and/or the private ownership structures
- Difficulty in monitoring for suspicious activity due to the complex nature of transactions (e.g., involvement of multiple third parties, therefore decreasing transparency of transaction details)
- Possibility of operating without proper registration or licensing (e.g., MSBs)
- History of abuse by money launderers and terrorists

1975. How does the NBFI list in the BSA compare to that outlined by the Financial Action Task Force (FATF)?

The BSA definition largely parallels the FATF guidance except that it does not include professional service providers such as lawyers, notaries and other independent legal professionals and accountants. As noted above, the United States has not issued AML/CFT regulations for a number of NBFIs, even though they are defined as financial institutions under the USA PATRIOT Act.

For further guidance on international standards for AML/CFT laws, please refer to the Financial Action Task Force section.

1976. Are there specific AML/CFT requirements for professional service providers?

Although not required to maintain an AML Program under Section 352 of the USA PATRIOT Act, professional service providers are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments [CMIR], Report of Foreign Bank and Financial Accounts [FBAR]). Additionally, assuming they are U.S. persons, professional service providers are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

Trade associations and FATF have highlighted the need for professional service providers to establish AML/CFT controls due to their positions as gatekeepers and intermediaries to the financial system. In order to establish accounts at financial institutions, professional service providers already may be required by their banks to implement basic AML/CFT controls to mitigate the risks associated with their professions. The risks of professional service providers were emphasised in the most recent Mutual Evaluation Report (MER) (2016) of the United States.

For additional guidance on professional service providers, please refer to the Professional Service Providers section. For further details on the U.S. MER, please refer to the Mutual Evaluations: Methodology and Reports section.

Money Services Businesses

Definitions

1977. What is a money services business (MSB)?

The BSA defines an MSB as "a person wherever located doing business, whether or not on a regular basis or as an organised or licensed concern, wholly or in substantial part within the United States, in one or more capacities" listed below:

- Issuer or seller of traveller's checks or money orders
- Check casher
- Dealer in foreign exchange
- Provider or seller of prepaid access
- Money transmitter

The U.S. Post Office also falls within the regulatory definition of MSBs but is exempt from some of the AML/CFT requirements (e.g., registration).

Definitions, including minimum activity thresholds, exemptions and AML/CFT requirements of each of the aforementioned covered MSB activities, are provided below. Specific AML/CFT laws and regulations for an MSB vary based on the activities that it is involved in, as well as whether it is performing as the agent or as the principal MSB (e.g., an MSB not acting on behalf of another MSB).

1978. Are TPPPs included in the definition of money services businesses?

Generally, no. A money services business (MSB) is defined as any organisation offering one or more of the following services:

- Issuer and seller of money orders and traveller's checks
- Check casher
- Dealer in foreign exchange
- Provider or seller of prepaid access
- Money transmitter

According to FinCEN, a merchant payment processor, also known as a TPPP, processes payments from consumers as an agent of the merchant to which the consumers owe money, rather than on behalf of the consumers themselves; therefore, it does not meet the regulatory definition of a money transmitter. The role of the merchant payment processor in these transactions is to provide merchants with a portal to a financial institution that has access to the payment system (e.g., ACH); it is not to transmit funds on behalf of third parties. If the TPPP provides other services beyond processing payments (e.g., check cashing), it may qualify as an MSB (or an agent of an MSB) and be subject to AML/CFT requirements for MSBs. Some banks have required or urged TPPPs to register as a condition to providing them with

services; other TPPPs have voluntarily done so to provide additional assurance that they are mitigating ML/TF risks by establishing an AML Program.

1979. Are all types of MSBs required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

No. Only MSBs that conduct more than US$1,000 in covered MSB activity with the same person (in an aggregate amount in one type of covered MSB activity) on the same day or provide money transmission services of any amount must maintain an AML Program.

For example, an entity that cashes checks, in aggregate, of more than US$1,000 for any person in a single day in one or more transactions is covered and must establish an AML Program.

The AML/CFT requirements for MSBs are implemented under regulation 31 C.F.R. 1022.100 et seq. – Rules for Money Services Businesses.

1980. Are virtual currency exchangers included within the definition of MSBs that are required to establish AML Programs?

In FinCEN Ruling FIN 2014-R007, unless a limitation or exemption applies, administrators or exchangers of "convertible virtual currencies" that conduct the following activities fall under the definition of money transmitter:

- Accepts and transmits a convertible currency
- Buys or sells convertible virtual currency in exchange for the following:
  - Currency of legal tender; or
  - Another convertible virtual currency

FinCEN defines an "exchanger" or "administrator" as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."

For further guidance, please refer to the Virtual Currency Systems and Participants section.

1981. Do common carriers of currency (e.g., armoured car services) fall under the definition of MSBs that are required to establish AML Programs?

Unless they provide financial services that would fall under the definition of money transmission services, the BSA specifically exempts common carriers of currency from the definition of money transmitters. For further guidance, please refer to the Common Carriers of Currency and Armored Car Services section.

1982. How is the term "agent" defined for MSBs?

The term "agent" is a separate business entity from the MSB that the MSB authorises, through written agreement or otherwise, to sell its MSB services (e.g., monetary instruments, funds transfers). MSB agents engaging in covered activities are MSBs, too, and are subject to the AML/CFT requirements.

Agents may include businesses such as grocery stores, convenience stores, travel agencies and gas stations.

For further guidance, please refer to the Agents of MSBs section.

1983. Are foreign-located entities engaged in covered MSB activities within the United States required to establish AML Programs?

Yes. FinCEN clarified that all entities engaged in covered MSB activities within the United States, regardless of the physical location of their agents, agencies, branches or offices, are required to establish AML Programs and comply with other AML/CFT laws and regulations. Examples include foreign entities with U.S. customers and foreign entities transmitting funds to or from U.S. recipients via the internet.

Foreign-located entities engaged in MSB activities are also required to designate a person who resides in the United States to function as an agent to accept service of legal process.

1984. Are there exemptions to the definition of an MSB?

Yes. The following are exempt from the regulatory definition of an MSB:

- A bank or foreign bank;
- A person registered with and functionally regulated or examined by the U.S. Securities and Exchange Commission (SEC) or the Commodity Futures Trading Commission (CFTC);
- A foreign financial agency that engages in financial activities that, if conducted in the United States, would require the foreign financial agency to be registered with the SEC or CFTC; and
- A natural person who engages in covered MSB activities on an infrequent basis and not for gain or profit.

For further guidance on the application of these exemptions and the regulatory definition of MSBs, please refer to the Guidance on the Applicability of the Definition of Money Services Businesses section.

1985. Does licensing affect whether an MSB is required to establish an AML Program?

A business that engages in covered MSB activity in the United States is required to establish an AML Program and comply with other AML/CFT requirements whether or not it is licensed or required to be licensed.

Although the likelihood of compliance is low, unlicensed MSBs (both those which are ignorant of the licensing requirement or wilfully avoid licensing) are obligated to comply with AML/CFT requirements and are subject to penalties for the criminal act of running an unlicensed money transmitter business pursuant to Section 373 - Illegal Money Transmitting Businesses of the USA PATRIOT Act.

For further guidance, please refer to the Informal Value Transfer Systems section.

1986. Is registration the same as licensing?

No. Registration is administered by FinCEN. Licensing is administered by each state and imposes separate requirements on MSBs. Operating an unlicensed MSB where licensing is required is illegal. For further guidance on registration requirements, please refer to the Registration for Money Services Businesses section.

1987. What is an informal value transfer system (IVTS)?

An informal value transfer system (IVTS) refers to any system, mechanism or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, regardless of whether it is in the same form. They are networks that facilitate the transfer of value (e.g., cash, commodities) domestically or internationally outside the conventional financial systems. IVTS activities often do not involve traditional banking transactions or services, such as deposit or lending products, although they may sometimes use banking systems.

IVTSs are also known as informal money transfer systems (IMTSs), underground banking systems and alternative remittance systems. Examples include hawalas and the Black Market Peso Exchange (BMPE).

For further guidance, please refer to the Informal Value Transfer Systems section.

1988. How does the Financial Action Task Force (FATF) define MSBs?

The Financial Action Task Force (FATF) uses the term "money or value transfer services" (MVTS) to describe MSB activity. MVTS are defined as "financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, a message, a transfer or through a clearing network to which the MVTS provider belongs."

The term "hawalas and other similar service providers" (HOSSPs) is used to describe informal value transfer systems (IVTSs).

1989. How do the U.S. AML/CFT requirements for MSBs correspond to the FATF Recommendations?

MSBs fall under FATF's definition of financial institution. As with covered financial institutions, FATF suggests MSBs implement preventive measures (e.g., customer due diligence, reporting of suspicious activities to the financial intelligence unit [FIU]) in multiple Recommendations, including, but not limited to, the following:

- Recommendation 10 – Customer Due Diligence
- Recommendation 11 – Recordkeeping
- Recommendation 14 – Money or Value Transfer Services

- Recommendation 15 – New Technologies (e.g., new products/services, such as prepaid access, mobile payments, electronic money, digital currencies; new delivery mechanisms for existing/new products/services)
- Recommendation 16 – Wire Transfers
- Recommendation 17 – Reliance on Third Parties
- Recommendation 18 – Internal Controls and Foreign Branches and Subsidiaries
- Recommendation 20 – Reporting of Suspicious Transactions

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

Issuers and Sellers of Money Orders and Traveller's Checks

1990. How is the term "issuer and seller of money orders and traveller's checks" defined for MSBs?

An issuer is defined as "a person that issues money orders or traveller's checks that are sold in an amount greater than US$1,000 to any person on any day in one or more transactions."

A seller is defined as "a person that sells money orders or traveller's checks in an amount greater than US$1,000 to any person on any day in one or more transactions."

1991. What is the difference between an issuer and a redeemer of money orders and traveller's checks?

An issuer of a money order or traveller's check is the business ultimately responsible for the payment of the money order or traveller's check.

A redeemer, or seller, is a business that exchanges money orders and traveller's checks for currency, monetary or other negotiable instruments. The acceptance of a money order or traveller's check as payment for goods and services is not considered redemption.

Check Cashers

1992. What is a check casher?

A check casher is defined as an entity that provides a customer with money orders, or a combination of currency and money orders, in exchange for a check, in an amount greater than US$1,000 on any day in one or more transactions. An entity providing check-cashing services for less than US$1,000 is not required to maintain an AML Program pursuant to Section 352 of the USA PATRIOT Act.

1993. Are there exemptions to the definition of a check casher?

Yes. The following entities are not included in the definition of a check casher:

- A person who sells prepaid access in exchange for a check, monetary instrument or other instrument;

- A person who solely accepts monetary instruments as payment for goods or services other than check cashing services;
- A person who engages in check cashing for the verified maker of the check who is a customer otherwise buying goods and services;
- A person who redeems his/her own checks; or
- A person who only holds a customer's check as collateral for repayment by the customer of a loan.

Dealers in Foreign Exchange

1994. What is a dealer in foreign exchange?

A "dealer in foreign exchange" is defined as "a person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds or other instruments denominated in the currency, of one or more countries in an amount greater than US$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery."

1995. What is a "*casa de cambio*"?

A "*casa de cambio*," the Spanish term for currency exchange, money exchange, or bureau de change, is a business whose customers exchange one currency for another.

Providers and Sellers of Prepaid Access

1996. How is the term "prepaid access" defined?

"Prepaid access" is defined as "access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Prepaid access applies to a very broad range of prepaid services, including but not limited to open-loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, and many prefunded employee programs such as a Health Savings Account."

1997. How is the term "provider and seller of prepaid access" defined?

The terms "provider" and "seller" of prepaid access are defined as the following:

- **Provider of prepaid access** – The participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access (provider). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program.
- **Seller of prepaid access** – Any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if:

- That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or
- That person sells prepaid access (including closed-loop prepaid access) to funds that exceed US$10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales.

1998. Why was "stored value" renamed as "prepaid access"?

"Stored value" was renamed as "prepaid access" because the technology used in the stored-value industry has changed. The updated terminology provides flexibility so it will not become obsolete as the industry advances to encompass all emerging payment methods, including but not limited to personal identification numbers, electronic serial numbers, cards, tokens, key fobs and mobile phones.

FinCEN stated that prepaid access is not itself a device or vehicle, but that devices and vehicles are the means through which prepaid funds are accessed. The two main elements of prepaid access are:

- Funds that have been paid in advance; and
- Those funds that can be retrieved or transferred at some point in the future. FinCEN also clarified that it intended its definition to include the necessary regulatory elasticity to survive future technological advancements.

1999. What guidance has been issued on prepaid access?

The following are examples of information and guidance that have been issued on prepaid access:

- **Prepaid Cards/Stored-Value Cards" subsection within Electronic Cash – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **"E-Banking" and "Emerging Retail Payment Technologies"** within the "Retail Payment Systems" sections within the FFIEC Information Technology Examination Handbook by the FFIEC
- **Application of the Prepaid Access Rule to Closed Loop Prepaid Access Sold or Exchanged in a Secondary Market** (2013) by FinCEN
- **Application of the Prepaid Access Rule to Bank-Controlled Programs** (2012) by FinCEN
- **Outreach to the Prepaid Access Industry** (2012) by FinCEN
- **Frequently Asked Questions Related to Prepaid Access Final Rule** (2011) by FinCEN
- **Notice of Proposed Rulemaking: Bank Secrecy Act Regulations: Definition of "Monetary Instrument"** (2011) by FinCEN (related to Prepaid Access devices)
- **Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS)** (2014) by the Wolfsberg Group of Banks (Wolfsberg Group)

- **Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions** (2011) by the World Bank (WB) Report on Money Laundering Using New Payment Methods (2012) by the Financial Action Task Force (FATF)
- **Payroll Cards: An Innovative Product for Reaching the Unbanked and Underbanked** (2005) by the Office of the Comptroller of Currency (OCC)
- **The 2008 Survey of Consumer Payment Choice** by the Federal Reserve Bank of Boston
- **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by FATF
- **Consumer Payment Choice: A Central Bank Perspective** by the Consumer Payments Research Center at the Federal Reserve Bank of Boston
- **Prepaid Cards: Vulnerable to Money Laundering?** (2007) by the Federal Reserve Bank of Philadelphia
- **The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards** (2008) by the Federal Reserve Bank of Philadelphia
- **Emerging Risk Forum "Cash, Check, or Cell Phone?" Protecting Consumers in a Mobile Finance World** (2010) by the Federal Reserve Bank of Boston
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** (2010) by the World Bank (WB)
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** (2004) by the Bank of International Settlements (BIS)
- **Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs** (2008) by the Network Branded Prepaid Card Association (NBPCA)
- **Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues** (2010) by the Federal Reserve Bank of Boston
- **Understanding Risk Management in Emerging Retail Payments** (2008) by the Federal Reserve Bank of New York

Additional organisations providing guidance on stored-value products include, but are not limited to, the following:

- **Federal Reserve Bank of Boston Risk and Policy Analysis Unit**
- **Federal Reserve Bank of Boston Consumer Payments Research Center (CPRC)**
- **Federal Reserve Bank of Philadelphia Payment Cards Center**
- **Network Branded Prepaid Card Association (NBPCA)**

For additional guidance, please refer to the Providers and Sellers of Prepaid Access section.

Money Transmitters

2000. What is a money transmitter?

A money transmitter is defined as the following:

- Any person engaged in the transfer of funds
- A person who provides money transmission services

"Money transmission services" is defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."

"By any means" includes money transmission through the following:

- A financial agency or institution;
- A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both;
- An electronic funds transfer network; or
- An informal value transfer system (IVTS).

2001. Are there exemptions to the definition of a money transmitter?

Yes. The term "money transmitter" does not include a person who only:

- Provides the delivery, communication or network access services used by a money transmitter to support money transmission services;
- Acts as a payment processor to facilitate the purchase of, or payment of, a bill for a good or service through a clearance and settlement system by agreement with the creditor or seller;
- Operates a clearance and settlement system or otherwise acts as an intermediary solely between BSA-regulated institutions, including but not limited to, the following:
  - Fedwire system
  - Electronic funds transfer networks
  - Certain registered clearing agencies regulated by the SEC and derivatives clearing organisations
  - Other clearinghouse arrangements established by a financial agency or institution
- Physically transports currency, other monetary instruments, other commercial paper or other value that substitutes for currency as a person primarily engaged in such business (e.g., armoured car service) from one person to the same person at another location or to an account belonging to the same person at a financial institution, provided that the person engaged in physical transportation has no more than a custodial interest in the currency, other monetary instruments, other commercial paper or other value at any point during the transportation;

- Provides prepaid access;
- Accepts and transmits funds only integral to the sale of goods or provision of services, by the person who is accepting and transmitting the funds.

Guidance on the Applicability of the Definition of Money Services Businesses

FinCEN has issued considerable guidance on the applicability of the definition of money services businesses to various business types that can be found at www.fincen.gov/statutes_regs/guidance. Several of these sets of guidelines are summarised below.

2002. Is a business that cashes payroll checks for its employees included in the definition of a check casher?

No. According to FinCEN Ruling FIN-2006-G005, a business that cashes payroll checks for its employees does not meet the regulatory definition of a check casher.

2003. Is a payday lender included in the definition of a check casher?

Yes. A payday loan is a short-term loan that is intended to cover a borrower's expenses until his or her next payday. According to FinCEN Ruling 2002-2, a business that provides "payday loans" by providing cash to customers in return for a postdated personal check meets the regulatory definition of a check casher.

2004. Is a "merchant payment processor" included in the definition of a money transmitter?

No. According to FinCEN Ruling 2003-8, merchant payment processors, also known as third-party payment processors (TPPPs), process payments from consumers as an agent of the merchant to which the consumers owe money, rather than on behalf of the consumers themselves; they therefore do not meet the regulatory definition of a money transmitter. The role of the merchant payment processor in these transactions is to provide merchants with a portal to a financial institution that has access to the payment system (e.g., ACH); it is not to transmit funds on behalf of third parties.

2005. Is a "company acting as an Independent Sales Organisation (ISO) and payment processor" included in the definition of a money transmitter?

No. According to FinCEN Ruling FIN-2014-R009, a company acting as an ISO and payment processor would not be included in the definition of a money transmitter, to the extent that the company complies with the requirements of the TPPP exemption, similar to the FinCEN ruling for merchant payment processors.

2006. Is a "member-sponsored merchant and/or retail operator of automated teller machines (ATMs) that participates in a third-party prepaid card reload program" included in the definition of an issuer of prepaid access or money transmitter?

No. According to FinCEN Ruling FIN-2008-R005, member-sponsored merchants and retail operators of ATMs that participate in a third-party prepaid card reload program serve only as (1) the physical

point in the reload process where a card is presented to transmit data to a member of the prepaid card reload program and (2) the point where the customer presents funds for collection. The merchant and retail operator of ATMs do not control nor conduct the actual transaction that results in the adding of value to the reloadable card and therefore do not meet the regulatory definition of an issuer of prepaid access.

Additionally, regulations also provide that "the acceptance and transmission of funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself will not cause [the merchant and/or ATM retail operator] to be a money transmitter" either. In other words, the act of collecting funds from the customer that is then forwarded to the member for eventual credit to a prepaid card is not considered a funds transfer; therefore the merchant or ATM retail operator is not a money transmitter.

2007. Is a "company that offers a loan acceleration product for consumer financing" included in the definition of a money transmitter?

No. A loan acceleration product is a service that assists borrowers in paying off consumer loans faster, utilising various methods (e.g., biweekly payments). According to FinCEN Ruling FIN-2008-R009, a company that offers a loan acceleration product for consumer financing does not meet the regulatory definition of a money transmitter. Generally, the acceptance and transmission of funds as an integral part of a transaction other than the funds transmission itself (e.g., in connection with a sale of securities or service [loan acceleration]) will not cause a person to be a money transmitter.

2008. Is a "foreign exchange dealer" included in the definition of a dealer in foreign exchange or money transmitter?

Yes. According to FinCEN's Ruling FIN-2008-R002, a foreign exchange dealer is included in the definition of a dealer in foreign exchange as currency from one country is exchanged for currency from another country.

A foreign exchange dealer may also be a money transmitter if it does not limit its business activity to accepting and transmitting funds for the purpose of executing and settling foreign exchange transactions with its unaffiliated business customers, but also settles transactions by moving funds between its customers and their third-party foreign counterparts through its own accounts.

2009. Is a "foreign exchange broker or consultant" included in the definition of a dealer in foreign exchange or money transmitter?

No. According to FinCEN's Ruling FIN-2008-R004, an "intermediate foreign exchange broker and consultant" is engaged in obtaining interbank prices for the foreign currency transactions of its clients. Because the foreign exchange consultant does not exchange foreign currency in the course of providing its services to its clients, it does not meet the regulatory definition of currency dealer or exchanger.

Additionally, regulations also provide that "the acceptance and transmission of funds as an integral part of the execution and settlement of a transaction other than the funds transmission itself will not cause [the foreign exchange consultant] to be a money transmitter" either. In other words, the forwarding of client funds to another financial institution by the foreign exchange consultant for

subsequent exchange by the third-party financial institution is not considered a funds transfer; therefore, the foreign exchange consultant is not a money transmitter.

2010. Is a "person who is engaged in the business of foreign exchange risk management" included in the definition of a dealer in foreign exchange and/or a money transmitter?

Yes. According to FinCEN's Ruling FIN-2008-R003, a person who is engaged in the business of foreign exchange risk management is included in both the definitions of a dealer in foreign exchange and a money transmitter, and thereby is subject to applicable AML/CFT requirements.

A foreign exchange risk management company "manages exchange rate risk for internet seller clients operating in currency A who (1) offer products for purchase by customers who operate in currency B (sale transactions), and (2) purchase supplies offered by suppliers who operate in currency C (supply transactions) by conducting foreign exchange or 'hedging' transactions in the relevant currency for the client." Additionally, the foreign exchange management company settles sale and supply transactions by the following methods:

- Settling Sale Transactions: "Submitting the bank card information of a client's customer, which it has received from the client, to the card processor for authorisation and payment. This payment is made into the company's own account, and the company ultimately remits those funds to the client."
- Settling Supply Transactions: "Moving funds from its clients to its clients' suppliers through their own accounts."

The method of managing exchange rate risk falls under the definition of currency dealing and exchanging, as currency from one country is exchanged for currency from another country.

The method of settling supply transactions (moving funds from its clients to its clients' suppliers through their own accounts) is considered a funds transfer; therefore a person who is engaged in the business of foreign exchange risk management, as defined above, falls under the definition of money transmitter.

2011. Are users who create or "mine" virtual currencies included in the definition of a money transmitter?

In FinCEN Ruling FIN-2013-G001, users who create or "mine" convertible virtual currencies solely for personal use do not fall within the definition of a money transmitter. If users mine for other than personal use (e.g., facilitate the transfer of funds between third parties), they may be money transmitters and be subject to the AML/CFT requirements of MSBs. For further guidance, please refer to the Virtual Currency Systems and Participants section.

2012. Are "virtual currency exchangers" included in the definition of a money transmitter?

In FinCEN Ruling FIN 2014-R007, unless a limitation or exemption applies, administrators or exchangers of "convertible virtual currencies" that conduct the following activities fall under the definition of money transmitter:

- Accepts and transmits a convertible currency
- Buys or sells convertible virtual currency in exchange for the following:
  - Currency of legal tender; or
  - Another convertible virtual currency.

FinCEN defines an "exchanger" or "administrator" as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."

For further guidance, please refer to the Virtual Currency Systems and Participants section.

2013. Are "businesses that develop and distribute virtual currency software" included in the definition of a money transmitter?

No. In FinCEN Ruling FIN-2014-R002, businesses that develop and distribute virtual currency software do not fall under the definition of money transmitter as these activities on their own do not constitute acceptance and transmission of value. The exemption is still applicable if the purpose of the software is to facilitate the sale of virtual currency.

2014. Are "investors in virtual currency businesses" included in the definition of a money transmitter?

No. In FinCEN Ruling FIN-2014-R002, investors in virtual currency businesses do not fall under the definition of money transmitter, as the act of investing does not constitute accepting and transmitting of value.

2015. Are companies that distribute and sell products from "bank-controlled prepaid access programs" included in the definition of prepaid access provider?

No. In FinCEN Ruling FIN-2012-R003, businesses that distribute and sell bank-controlled prepaid access programs do not fall under the definition of prepaid access provider. In this situation, the bank would be the provider of prepaid access. Banks are excluded from the definition of MSBs and are subject to separate AML/CFT requirements.

Depending on the details of the program, the business, however, may fall under the definition of seller of prepaid access and thus be subject to specific AML/CFT requirements.

For further guidance, please refer to the Providers and Sellers of Prepaid Access section.

2016. Does the selling of "closed loop prepaid access in a secondary market" nullify its exemption from the prepaid access rule?

No. In FinCEN Ruling FIN-2013-R003, the sale or exchange of closed loop prepaid access in a secondary market does not nullify its exemption from the prepaid access rule.

Key AML/CFT and Sanctions Requirements

2017. With which key AML/CFT and sanctions requirements are MSBs required to comply?

MSBs must comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML Program and ongoing monitoring and updates; the AML Program should cover agents of the principal MSB, both domestic and foreign (Section 352)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Suspicious Activity Reports (SARs) (except check cashers)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Recordkeeping Rule and Travel Rule, Purchase and Sale of Monetary Instruments) (Additional recordkeeping requirements for dealers in foreign currency)
- Information-sharing (e.g., Section 314(a) [in some cases mandatory]; Section 314(b) [optional])
- Registration with FinCEN (exemption for agents of other MSBs that are MSBs solely because they offer products or services of other MSBs)
- OFAC and other sanctions requirements
- Designation of a person who resides in the United States as an agent to accept service of legal process (for foreign-located MSBs)

The AML/CFT requirements for MSBs are implemented under 31 C.F.R. 1022 – Rules for Money Services Businesses.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to MSBs is provided below.

2018. Since MSBs do not have "customers with accounts" in the traditional sense, do they have CIP obligations under Section 326 of the USA PATRIOT Act?

MSBs are not subject to the CIP requirement. However, if an MSB establishes a relationship with a party (e.g., through the issuance of ID cards, stored-value cards, web-based transfer services), additional verification procedures, including the adoption of a Know Your Customer (KYC) program, would be appropriate. Gathering information up front will assist the MSB with its monitoring and, as necessary, reporting of CTRs and SARs.

For guidance on CIP requirements, please refer to Section 326 – Verification of Identification.

2019. Are MSBs subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners under the Beneficial Ownership Rule. MSBs are not subject to the CIP requirement and therefore are not required to identify beneficial owners on legal entity customers; however, as a practical matter, MSBs that have established KYC programs for online and/or recurring customers should consider including beneficial ownership information if they do business with legal entities.

In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance, please refer to the sections Beneficial Owners and Section 352 – AML Program.

2020. Are MSBs required to file CTRs?

Yes, MSBs are required to file CTRs. For a listing of financial institutions required to file CTRs at the time of this publication, please refer to the Currency Transaction Reports section.

2021. Can MSBs grant CTR exemptions?

No. Only depository institutions (e.g., banks, savings associations, thrift institutions, credit unions) can grant exemptions, and then only for their U.S. customers. For further guidance, please refer to the CTR Exemptions and the Designation of Exempt Persons Form section.

2022. Should an MSB with multiple agents aggregate cash transactions across agents for CTR filing purposes?

FinCEN has indicated that multiple currency transactions occurring across multiple agents must be aggregated for CTR reporting when the MSB has knowledge that they are by or on behalf of the same person and meet the CTR reporting threshold.

For example, an MSB has two agents, Agent A and Agent B. A customer goes to Agent A and sends US$7,000 to an individual and, on the same day, goes to Agent B and sends an additional US$7,000 to the same (or another) individual. Both transactions are conducted in cash, and neither agent is aware of the other transaction. In this case, the MSB must file a CTR if it knows that multiple currency transactions aggregating to more than US$10,000 have been conducted by the same person on the same day. Financial institutions need to take care to understand whether they will be deemed to have such knowledge, as some financial institutions that have failed to aggregate appropriately have been fined.

2023. Do MSBs have their own, unique SAR form?

No. Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms (e.g., Suspicious Activity Report by Money Services Businesses [SAR-MSB]) with a single form that must be submitted electronically. The filing criteria for MSBs, however, differs from other types of financial institutions (e.g., banks, broker-dealers) as detailed below.

As of April 1, 2013, MSBs must submit the new SAR (and other FinCEN Reports) electronically through the BSA E-Filing System.

2024. What types of activities require a SAR to be filed for MSBs?

MSBs should file a SAR upon detection of the following activities:

- **Transactions aggregating to US$2,000 (except where detailed below) or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA)** – Any transaction(s) totalling or aggregating to at least US$2,000 (except where detailed below) conducted by a suspect through the MSB, where the MSB knows, suspects or has reason to suspect that the transaction either: involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
- **Transactions relating to clearance records aggregating to US$5,000 or more that involve potential money laundering or violations of the BSA** – An MSB should file a SAR whenever it detects any known or suspected federal criminal violations or pattern of violations have been committed or attempted through it or against it involving clearance records or other similar records of money orders or traveller's checks that have been sold or processed.
- **Evasion** – A SAR should be filed in any instance where the MSB detects that the transaction was designed to evade any BSA regulations, whether through structuring or other means.
- **No business or apparent lawful purpose** – The transaction has no business or apparent lawful purpose, and there is no known reasonable explanation for the transaction after examination of available facts, including the background and possible purpose of the transaction.
- **Facilitate criminal activity** – The transaction involves the use of the MSB to facilitate criminal activity.

For red flags that assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

2025. What are some of the statistics and trends in SAR filings for MSBs?

According to FinCEN, out of 1.98 million SAR filings from January 1, 2016 through December 31, 2016, MSBs filed over 870,000 SARs or 44 percent of all filings:

- Fifty-one percent of SARs were filed on activity taking place in California, New York, Texas, Florida, North Carolina, Virginia, Colorado and Georgia; approximately 8 percent of SARs came from an unknown/blank state;
- Thirty-nine percent of SARs were filed on customers, 27 percent on "other" relationship types, 24 percent on unknown/blank relationship types and 11 percent on individuals with no relationship with the MSB;

- Forty-eight percent of SARs involved funds transfers, 23 percent involved U.S. currency, 22 percent involved money orders and 11 percent involved prepaid access;
- Top suspicious activity categories of SARs filed by MSBs included:
  - Structuring: 31 percent
  - Other Suspicious Activities: 40 percent (included nearly 198,000 cases related to "suspicious use of multiple locations," over 21,000 cases related to identity theft, nearly 30,000 cases related to elder financial exploitation, 459 cases related to unauthorised electronic intrusion and 154 cases related to suspected corruption [foreign and domestic])
  - Money Laundering: 8 percent
  - Fraud: 15 percent (separate from Mortgage Fraud which accounted for less than 0.01 percent)
  - Terrorism/Terrorist Financing: 0.06 percent (1,074 cases)

2026. Are there exemptions to the suspicious activity reporting requirement of MSBs?

The SAR requirement currently does not apply to MSBs engaged solely in check cashing.

Therefore, if an MSB provides, for example, wire transfers and check cashing, its SAR filing requirements would apply only to its wire transfer activities. MSBs can, however, voluntarily file SARs on check cashing.

2027. Should MSBs file SARs on behalf of their agents?

Yes. An MSB must file SARs on any covered suspicious activity that is transferred or transacted through it, or is attempted, including suspicious activities at its agent locations.

2028. Are there red flags for detecting potentially suspicious activity for MSBs?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments) has been provided in this publication. Common red flags include, but are not limited to, the following:

- For monetary instruments:
  - Monetary instruments purchased on the same or consecutive days at different locations, and/or are numbered consecutively in amounts designed to evade reporting requirements (i.e., under US$3,000 or US$10,000), or are purchased in round amounts
  - Blank payee lines
  - Instruments which contain the same stamp symbol or initials
- For funds transfers:

- Frequent, large, round dollar wire transactions
- Wire transfers to and from bank secrecy haven countries and countries known for or linked to terrorist activities, drug trafficking, illegal arms sales or other illegal activity

For further guidance on red flags, please refer to the sections: Suspicious Activity Red Flags, Currency Red Flags, Monetary Instrument Red Flags and Informal Value Transfer System (IVTS) Red Flags.

2029. Must an MSB maintain its AML Program in English?

There is no prohibition against an MSB maintaining its AML Program in a language other than English. In fact, where English is not the first language of the business's owners, employees or customers, maintaining an AML Program in the language(s) most commonly used may be particularly helpful. However, FinCEN requires that, upon request, an English language translation be available within a reasonable period of time. Businesses, therefore, would be well-advised to maintain English translations of key documents, such as policies and procedures, to ensure that they can meet the "reasonable" time frame required by FinCEN.

In addition to English, FinCEN does provide guidance for MSBs in the following languages:

- Arabic
- Chinese
- Farsi
- Korean
- Somali
- Spanish
- Russian
- Vietnamese

2030. Are MSBs required to hire a third party to perform the independent review of the AML Program?

No. In implementing the independent testing requirement, FinCEN stated that MSBs are not required to hire a third party firm to conduct a review of their programs. The review may be conducted by an officer, employee or group of employees so long as the reviewer is not the designated compliance officer of the MSB and does not report directly to the compliance officer, nor have other responsibilities for AML/CFT compliance. For additional guidance on independent testing, please refer to the Independent Testing section.

2031. What type of information should an MSB be prepared to provide to a financial institution when establishing an account relationship?

MSBs should be prepared to provide the following information to a financial institution when establishing an account relationship:

- Basic identifying information about the MSB, its owners and principal officers, and a history of its operations
- Products and services offered
- List of branches and agents, including the jurisdictions in which they operate
- FinCEN registration, if required
- Proof of compliance with state or local licensing requirements, if applicable
- Anticipated account activity (e.g., volume and type of transaction activity, seasonal fluctuations)
- Purpose of the account(s) (e.g., domestic remittances, remittances to foreign-based agents)
- Results of the independent testing of the AML Program (unless subject to attorney-client or work product privilege or other confidentiality obligation)
- Written AML policy
- Written agent management, termination and employment screening practices

Financial institutions may choose to require additional information from an MSB either at account opening or at a later date.

2032. What are the key recordkeeping requirements of the BSA for MSBs?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs, RMSBs). Additionally, other required documentation must be retained by dealers in foreign exchange, such as the following:

- When required, a taxpayer identification number (TIN) (or passport number or description of a government-issued identification for non-resident aliens) of each person for whom a transaction account is opened or a line of credit is extended and for each person who has a financial interest in the account
- List of names, addresses and account or credit line numbers of those persons from whom the dealer in foreign exchange was unable to obtain the above information
- Statements of accounts from banks, including paid checks, deposit slips, charges or other debit and credit entry memoranda, representing the entries reflected on such statements
- Records of each exchange of currency involving transactions in excess of US$1,000, including the name, address, TIN or passport number; date and amount of transaction; currency name; and total amount for each foreign currency
- Signature cards or other documents evidencing signature authority over each deposit or security account containing the name of the depositor, address, TIN or passport number, and signature of the depositor or authorised signer
- Each item, including checks, drafts or transfers of credit, of more than US$10,000 remitted or transferred to a person, account or place outside of the United States

- A record of each receipt of currency, other monetary instruments, investment securities and checks, and of each transfer of funds or credit of more than US$10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside of the United States
- Records prepared or received by a dealer in the ordinary course of business, which would be needed to reconstruct an account and trace a check in excess of US$100 deposited in such account through its internal recordkeeping system to its depository institution or to supply a description of a deposited check in excess of US$100
- A record maintaining the name, address, TIN or passport number of any person presenting a certificate of deposit for payment, as well as a description of the instrument and date of transaction
- A system of books and records that will enable the dealer in foreign exchange to prepare an accurate balance sheet and income statement

The above applies to dealers in foreign exchange. The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, broker-dealers, casinos and card clubs) as well. For further guidance, please refer to the sections: BSA Recordkeeping Requirements, Broker-Dealers in Securities and Casinos and Card Clubs.

2033. Are dealers in foreign exchange limited to passports as a form of documentation used to verify the identification of non-resident aliens?

No. In FinCEN Ruling FIN-2014-R003, an exception was granted allowing dealers in foreign exchange to accept other forms of government-issued documentation (e.g., Border Crossing Card bearing a B1/B2 visitor visa), beyond the passport, to verify the identity of non-resident aliens seeking to exchange currency.

2034. Are check cashers subject to additional recordkeeping requirements of the BSA for MSBs?

No. Check cashers are not required to maintain additional records under the recordkeeping requirements of the BSA for MSBs specific to their check cashing activity as with money transmitters, issuers of monetary instruments, and dealers in foreign exchange (e.g., Funds Transfer Recordkeeping Requirement and Travel Rule, Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments). However, if they provide money services other than check cashing, they are required to maintain records as detailed above.

For additional guidance on recordkeeping requirements, please refer to the sections: Funds Transfer Recordkeeping Requirement and Travel Rule and Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments.

2035. Are MSBs required to conduct AML/CFT and OFAC risk assessments?

MSBs are expected to develop and maintain risk-based compliance programs. This requires that they conduct AML/CFT risk assessments. The AML/CFT risk assessments developed by MSBs should

address such factors as geographic risk, product risk (e.g., limits, in-person or internet services) and risks associated with the agents and other business partners of an MSB. The same reasoning applies to conducting OFAC/Sanctions risk assessments. For additional guidance on AML/CFT and OFAC/Sanctions risk assessments, please refer to the Risk Assessments section.

2036. Are MSBs required to conduct customer risk assessments?

As previously indicated, MSBs often do not have "customers" per se. However, in instances where MSBs do have "customers" or collect sufficient information on parties involved in transactions to be able to profile these parties, they should conduct customer risk assessments and tailor their AML/CFT Compliance Programs, particularly monitoring, to the risk.

2037. As customers, should all MSBs unilaterally be considered high risk?

No. The risks of each MSB should be assessed based on a variety of factors (e.g., product/service offerings, nature and geography of customer base, size and geography of operations, and nature of services). Evaluating the risks of MSBs in this manner will result in different risk ratings (e.g., low, moderate, high). However, as a practical matter given the nature of the business, most MSBs are likely to have high or moderate (not low) inherent risk.

2038. Are MSBs required to maintain separate checking accounts for their check cashing and money transmission lines of business?

No. According to FinCEN Ruling FIN-2008-R012, MSBs are not required to maintain separate checking accounts for their check cashing and money transmission lines of business. In some instances, however, as a requirement to establish an account at a bank, MSBs may be required to establish separate accounts for their various lines of business in accordance with the bank's internal policy.

2039. Are MSBs required to comply with OFAC and sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2040. Do MSBs have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. MSBs can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyberattacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2041. Who is responsible for examining MSBs for compliance with AML/CFT requirements?

The responsibility for examining MSBs is delegated to the IRS by FinCEN. Many states also examine MSBs and their agents for compliance with AML/CFT and other federal and state requirements.

2042. What were some common deficiencies identified in recent enforcement actions involving MSBs?

The following areas are some of the common deficiencies in AML/CFT compliance programs that have been identified in recent enforcement actions involving MSBs:

- Inadequate suspicious activity monitoring program and suspicious activity report (SAR) filing program, including, but not limited to, the following deficiencies:
    - Lack of alignment with the AML/CFT risks of the MSB
    - Lack of or inadequate escalation procedures to senior management for significant investigations
    - Failure to file timely SARs
- Inadequate due diligence of agents
    - Failure to terminate relationships with agents responsible for significant suspicious activity (e.g., elder financial exploitation)
- Inadequate structuring, resources and training of AML/CFT compliance officer and staff
    - Poor communication or wilful miscommunication between compliance personnel and senior management on significant matters

For further details on recent enforcement actions involving MSBs, please refer to the Key U.S. Enforcement Actions and Settlements section. For further guidance on enforcement actions, please refer to the Enforcement Actions section.

2043. What was the "Haider Settlement"?

To date, the largest public civil AML enforcement action against an individual was a US$250,000 fine and a three-year injunction barring compliance employment with any money transmitter against the former chief compliance officer (CCO) of MoneyGram International Inc. (MoneyGram), Thomas E. Haider, commonly referred to as the "Haider Settlement" (May 2017).

In December 2012, MoneyGram entered into a Deferred Prosecution Agreement (DPA) with the DOJ with a forfeiture of US$100 million for aiding and abetting wire fraud and failing to maintain an effective AML Program. Initially, Haider faced a personal fine up to US$5 million for his "wilful inaction." According to FinCEN's press release, Haider ultimately settled for a lower amount after admitting, acknowledging and accepting responsibility for the following:

- "[F]ailing to terminate specific MoneyGram outlets after being presented with information that strongly indicated that the outlets were complicit in consumer fraud schemes;
- [F]ailing to implement a policy for terminating outlets that posed a high risk of fraud; and
- [S]tructuring MoneyGram's anti-money laundering (AML) program such that information that MoneyGram's Fraud Department had aggregated about outlets, including the number of reports of consumer fraud that particular outlets had accumulated over specific time periods, was not generally provided to the MoneyGram analysts who were responsible for filing suspicious activity reports with FinCEN."

For further details on MoneyGram's enforcement action, please refer to the Key U.S. Enforcement Actions and Settlements section.

Registration Requirements of MSBs

2044. What is a Registration of Money Services Business (RMSB) form?

Completion and submission of FinCEN 107 form, Registration of Money Services Business (RMSB), satisfies the covered MSB requirement to register with FinCEN. The RMSB must be filed within 180 calendar days after the date the business is established. MSBs must reregister every two years on or before December 31 using the same RMSB form.

The RMSB requirement is implemented under regulation 31 C.F.R. 1022.380 – Registration of Money Services Businesses.

2045. What is the purpose of the registration requirement for MSBs?

The purpose of the registration requirement is to identify MSBs that are operating so they may be monitored for compliance with AML/CFT laws and regulations.

2046. Is registration the same as licensing?

No. Registration is administered by FinCEN. Licensing is administered by each state and imposes separate requirements on MSBs. Operating an unlicensed MSB where licensing is required is illegal. For additional details on unlicensed MSBs, please refer to the Informal Value Transfer Systems section.

2047. Are all MSBs required to register with FinCEN?

All MSBs must register with FinCEN, except the following:

- MSBs that solely serve as an agent of another MSB
- U.S. Postal Service

For further guidance on RMSBs, please refer to the Registration of Money Services Businesses section.

2048. How do the U.S. licensing and registration requirements for MSBs correspond to FATF Recommendations?

U.S. licensing and registration requirements for MSBs parallel FATF Recommendations. In **Recommendation 14 – Money or Value Transfer Services**, FATF recommends measures to license and register businesses that provide money or value transfer services (MVTS). Measures should be applied to agents as well, independently or as part of the AML/CFT Compliance Program of the principal business.

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

Agents of MSBs

2049. How is the term "agent" defined for MSBs?

The term "agent" is a separate business entity from the principal MSB that the principal MSB authorises, through written agreement or otherwise, to sell its MSB services (e.g., monetary instruments, funds transfers). MSB agents engaging in covered activities are MSBs, too, and are subject to the AML/CFT requirements. Agents may include businesses such as grocery stores, convenience stores, travel agencies and gas stations.

2050. Is an employee of an MSB considered an agent?

No. A person who is solely an employee of the MSB is not an agent of that MSB.

2051. What are the heightened money laundering and terrorist financing risks of agents?

Agents pose similar if not more heightened risks than do principal MSBs, due to the same factors that heighten the risks of MSBs relative to other types of financial institutions (e.g., banks, broker-dealers). These factors include, but are not limited to, the lack of traditional relationships with "customers," the lack of compliance-related experience of owners/management, the lack of sophisticated internal controls and high employee turnover. Further, for many though not all agents, their MSB business is secondary to their primary business and may not, therefore, be subject to the same focus on compliance that principal MSBs exhibit.

2052. Is the principal MSB liable for an agent's deficient AML/CFT Compliance Program?

According to FinCEN Guidance FIN-2016-G001, both the principal MSB and the agent are liable, regardless of contractual assignments of responsibility. Principal MSBs should have written procedures for handling non-compliant agents including agent contract termination.

2053. What information is an MSB required to maintain about its agents?

Each MSB that is required to register must prepare and maintain a list of its agents. The agent list is not filed with the RMSB but must be maintained at a location in the United States. The list must include the following specific information:

- Agent name
- Agent address
- Agent telephone number
- The type of service(s) provided by each agent on behalf of the MSB
- Identification of the months in the immediately preceding 12 months in which the gross transaction amount of each agent with respect to financial products/services issued by the MSB exceeds US$100,000
- The name and address of any depository institution at which an agent maintains a transaction account for part or all of the funds conducted by the agent on behalf of the MSB

- The year in which each agent first became an agent of the MSB
- The number of branches or subagents that each agent has

The list should be updated annually and retained for a period of five years. Upon request, the MSB should make the agent list available to FinCEN, the IRS and appropriate law enforcement agencies. Requests for such information should be coordinated through FinCEN. An MSB's regulators and auditors also may request such information.

2054. What due diligence should MSBs conduct when acquiring and maintaining agents?

Based upon risk, MSBs should conduct due diligence and enhanced due diligence (EDD) when acquiring and maintaining agents, including, but not limited to, the following:

- Performing adequate due diligence to ensure that the business is in good standing
- Performing background checks and credit checks on the primary owners of the agent
- Performing ongoing due diligence necessary to understand the agent's operations, customer base and services (e.g., periodic onsite visits, maintaining and updating agent due diligence on a regular basis)
- Obtaining letters of reference
- Ensuring that the agent has an effective AML Program in place or that the agent agrees to adopt the MSB's AML Program
- Requiring that the agent agrees to share relevant information upon request of the MSB

2055. What is "mystery shopping" and are MSBs required to mystery shop their agent locations?

"Mystery shopping" is a process that involves mystery shoppers visiting an MSB and posing as customers and providing detailed evaluations of their experience (both good and bad) using written reports or questionnaires. Mystery shopping may have multiple objectives (e.g., ensuring employees are adhering to applicable laws and regulations and following the company's internal policies and procedures, evaluating customer service, and/or assessing how well employees are meeting company sales goals).

Agent mystery shopping is not a regulatory requirement. However, mystery shopping has become a growing industry practice used to identify and mitigate risks associated with agent relationships.

2056. What is a foreign agent or foreign counterpart of an MSB, and what are the heightened money laundering and terrorist financing risks of foreign agents?

A foreign agent or counterpart of an MSB is a business outside of the United States that the MSB authorises, through written agreement or otherwise, to sell its instruments or, in the case of funds transmission, to receive or pay its funds transfers or facilitate other flow of funds into and out of the United States. MSBs utilise relationships with foreign agents and counterparties to facilitate the movement of funds into or out of the United States, similar to correspondent banking relationships.

The movement of money through wire transfers to or from foreign establishments may place MSBs at higher risk of facilitating the flow of illicit funds or legitimate funds used for illicit purposes.

2057. Has any guidance been issued relating to an MSB's obligations with respect to foreign agents and foreign counterparts?

FinCEN issued interpretive guidance requiring that an MSB's AML Program be capable of detecting the abuse of products and services offered through foreign agents or counterparties by establishing procedures for:

- Conducting due diligence on foreign agents and counterparties, including, but not limited to, identification of the owners and evaluation of their operations and policies, procedures and controls to determine whether they are reasonably designed to help ensure they are not subject to abuse
- Performing risk-based monitoring on foreign agents and foreign counterparts
- Taking corrective action or terminating relationships, as appropriate

Providers and Sellers of Prepaid Access

Definitions

2058. What are the key features of FinCEN's final rule, "Definitions and Other Regulations Relating to Prepaid Access"?

The final rule, which was issued July 29, 2011, "Definitions and Other Regulations Relating to Prepaid Access" (Prepaid Access rule), imposes regulatory requirements under the BSA to entities involved in the provision or sale of prepaid access of virtually all types (open- or closed-loop) through nearly any means (card, code, fob, smartphone).

Certain providers and sellers of prepaid access are subject to numerous AML/CFT, information capture and retention requirements. Non-bank financial institutions (NBFIs), retailers, merchants and others who offer or sell such products are subject to portions of the Prepaid Access rule.

There are two separate prongs of the rule:

- Whether a prepaid access arrangement requires a "provider" as defined in the Prepaid Access rule; and
- Whether an entity or person that sells prepaid access qualifies as a "seller of prepaid access" under the rule. An entity that is involved in any way with prepaid access should carefully evaluate whether its activities are covered in either prong.

Key features of the final rule include:

- Defining key terms including:
  - **Prepaid access** – Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an

electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Prepaid access applies to a very broad range of prepaid services, including, but not limited to, open-loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, and many prefunded employee programs such as a Health Savings Account.

  - **Prepaid program** – An arrangement under which one or more persons acting together provide(s) prepaid access. The functionality of the specific prepaid access offered may determine regulatory obligations. Certain exemptions apply.
  - **Providers of prepaid access** – The participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access (provider). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program.
  - **Sellers of prepaid access** – Any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if:
    - That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or
    - That person sells prepaid access (including closed-loop prepaid access) to funds that exceeds US$10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales.

- Renaming "stored value" as "prepaid access";
- Replacing the terms "issuer" and "redeemer" of prepaid access with the terms "provider" and "seller";
- Expanding AML/CFT requirements to include providers and sellers of prepaid access (e.g., registration requirements for "providers"; and for any entity that is a provider or seller of prepaid access, filing of suspicious activity reports (SARs) and currency transaction reports (CTRs), customer information recordkeeping, policies and procedures, internal controls, training, new transactional recordkeeping and independent audits);
- Guidelines to assist participants in determining who would serve as the provider for the particular prepaid program; in the event the participants do not determine who will serve as the provider, then it will be determined by FinCEN (although there is no grace period or safe harbour extended where the provider was not identified by the participants). If there is only one party in the prepaid

program, and its prepaid access does not qualify for an exemption, then it must be the prepaid access provider (unless it is a bank);

- Exemptions for lower-risk prepaid access arrangements with qualifying exclusions;
- Exemptions for bank centric programs for the provider of prepaid access requirements; and
- Limited exemptions for sellers of prepaid access.

2059. Why did the rule rename "stored value" as "prepaid access"?

The final rule renamed "stored value" as "prepaid access" because the technology used in the stored-value industry has changed. The updated definition provides flexibility so it will not become obsolete as the industry advances to encompass all emerging payment methods, including but not limited to personal identification numbers, electronic serial numbers, cards, tokens, key fobs and mobile phones.

FinCEN stated that prepaid access is not itself a device or vehicle but that devices and vehicles are the means through which prepaid funds are accessed. The two main elements of prepaid access are:

- Funds that have been paid in advance; and
- Those funds that can be retrieved or transferred at some point in the future. FinCEN also clarified that it intended its definition to include the necessary regulatory elasticity to survive future technological advancements.

2060. What are the heightened money laundering and terrorist financing risks of prepaid access?

Transactions may involve funds that have been transferred to or from an unknown party or from a party that wants to engage in illicit transactions or money laundering. Law enforcement has voiced concerns in part due to the ease with which prepaid access can be obtained, the high velocity of money that potentially can be moved with prepaid access and the anonymous use of some prepaid access. However, unlike cash, there are records available for all of the transactions performed for a particular prepaid access device.

Following are examples of types of factors that may increase the risk associated with a prepaid access product:

- Reloadability
- High value/unlimited load amount
- Lack of account relationship with issuer and/or seller of the products
- Lack of identification of purchaser
- Source used to fund product is cash, credit card or another stored-value product
- Ability to conduct cross-border transactions
- Ability to make cash withdrawals

2061. Is the definition of prepaid access limited to cards?

No. The regulatory definition of prepaid access was designed to be applicable to emerging and developing technologies, which may include but are not limited to the following:

- Near field communications (NFC) (set of short-range wireless technologies that establish electromagnetic radio fields that enable devices to communicate with each other when touching or in close proximity)
- Chip technology
- Magnetic strips
- Cellular phones
- Prepaid access through the internet using PINs/codes
- Prepaid access through fobs, tokens, chips or other technology
- E-cards
- Virtual currency

Prepaid access products encompass a large number of current and emerging growth products, such as open-loop general purpose reloadable (GPR) cards, certain closed-loop cards, mobile phone access, and fob or barcode access.

2062. Do all types of prepaid access products pose the same degree of risk?

No. FinCEN has issued guidance that the following types of prepaid access products pose lower risk:

- Closed-loop prepaid access – Prepaid access to funds or the value of funds with a maximum dollar threshold of US$2,000 that can be used only for goods or services involving a defined merchant or location (or set of locations), such as a specific retailer or retail chain, a college campus, or a subway system;
- Devices that do not permit international use (e.g., use at foreign merchants via the internet or face to face); and
- Non-reloadable devices.

2063. What is the difference between a closed-loop and open-loop prepaid access product?

Closed-loop prepaid access products are usable only at a specific merchant, or a group of merchants using the same branding, such as a Starbucks card. They may be in a fixed amount or reloadable. Open-loop prepaid access products may be used at multiple merchants, such as a prepaid card that contains a Visa logo and can be used at any merchant that accepts Visa debit cards. Open-loop cards may also come in fixed or reloadable amounts.

2064. If multiple merchants participate as the "defined merchant" that accepts the prepaid access product, is it still considered a closed-loop system?

According to FinCEN's Frequently Asked Questions regarding Prepaid Access published in March 2016, a "defined merchant" is not limited to a single merchant but extends to multiple unaffiliated partner merchants joined for the limited purpose of providing a closed-loop prepaid access program.

2065. Can a closed-loop prepaid access product be used to launder illicit funds?

As with any type of payment product or service, it is possible for a closed-loop prepaid access product to be misused. Law enforcement has identified instances where drug dealers used illicit funds to purchase closed-loop gift cards, and the cards were then used to purchase retail items. However, there have been few reported incidents of misuse of either closed- or open-loop prepaid cards in the United States to date, especially for cards issued by a U.S.-based issuer.

2066. Which prepaid access arrangements are excluded from the definition of prepaid access program?

The rule has identified five arrangements that are excluded from the definition of a prepaid access program with three high-risk factors that would negate some exclusions. Two of the five excluded arrangements can be summarised as follows:

- Prepaid access to funds with the following criteria:
  - Load limit less than or equal to US$1,000 at the point of initial load;
  - Total maximum value less than or equal to US$1,000 can be accessed at any point in the lifecycle of the prepaid access; and
  - Less than or equal to US$1,000 can be withdrawn with the use of the prepaid access on any given day.
- Payroll and Benefit Cards - The payment of benefits, incentives, wages or salaries through payroll cards or other such electronic devices for similar purposes.

If the aforementioned excluded arrangements display any one of the following three high-risk factors, they would no longer be exempt from prepaid access regulations:

- International use (e.g., can be used to withdraw cash or purchase goods and services from foreign ATMs or foreign merchants via the internet or in person);
- Person-to-person transfers; and
- Reloads from a non-depository source (e.g., retail stores, MSBs).

The three remaining excluded arrangements can be summarised as follows:

- Closed-loop products with a maximum value less than or equal to US$2,000 on any day that cannot be redeemed for cash;

- Government Funded Prepaid Access – Payment of government benefits such as salaries, tax refunds, and benefits, including unemployment, child support, disability, social security, and disaster assistance, through electronic devices; and
- Flexible Spending and Dependent Care Funded Prepaid Access – Reimbursement of funds for defined, qualifying expenses related to pre-tax flexible spending accounts for healthcare and dependent care expenses or Health Reimbursement Arrangements (as defined in 26 U.S.C. §§105(b) and 125) for healthcare expenses.

Exclusions have nuances that need to be carefully reviewed before relying on them.

2067. Does the US$2,000 threshold for closed-loop products apply to a single device or per individual?

The US$2,000 threshold is applied to the device or vehicle and does not require aggregation of all purchases of distinct closed-loop prepaid access devices bought by an individual in a single day. However, as discussed further below, an entity that sells more than US$10,000 in almost any combination of prepaid access is subject to the portion of the Prepaid Access rule applicable to "sellers of prepaid access."

2068. Must a prepaid access product display its maximum value on the product itself?

No. The final rule did not include the requirement that the maximum value of a prepaid access product be clearly visible on the product itself.

2069. Why is the "provider" assigned the primary responsibility for ensuring a prepaid access program is in compliance with AML/CFT laws and regulations?

The final rule centralises the primary regulatory obligations with the provider of a prepaid access program since it is often the party with the greatest access and/or ability to gain access to relevant information to comply with BSA reporting requirements. The provider is generally the participant with principal oversight and control over one or more prepaid programs.

FinCEN believes the provider is the entity in the best position to file CTRs and SARs, maintain or have access to transaction records, and establish and maintain AML Programs because it is likely to have business relationships with most or all of the other participants in the transaction chain.

2070. How is the "provider" of a prepaid access program determined?

The final rule provides two methods for determining the provider of a prepaid access program:

- **Agreement Approach** – A contractual determination among the participants in a prepaid access program as to who would serve as the provider. The determination is communicated to FinCEN when the provider registers as a money services business utilising the Registration of Money Services Businesses (RMSB).
- **Provider Criteria** – In the event participants in a prepaid access program fail to come to an agreement or the provider has failed to register, the following five factors, each of which is not

dispositive on its own, will be used by FinCEN to determine a provider of a prepaid access program:

- Organiser of the prepaid program (e.g., initiated or established the program);
- Sets the terms and conditions and determines that the terms have not been exceeded;
- Determines the other businesses that will participate in the prepaid program, which may include the issuing bank, the payment processor or the distributor;
- Controls or directs the appropriate party to initiate, freeze or terminate prepaid access;
- Engages in activity that demonstrates control and oversight of transactions.

2071. Are there exemptions to the definition of a "provider" of prepaid access?

Yes. Banks and financial institutions regulated by the SEC and the CFTC are exempt from the definition of "provider" by the final rule. While not subject to prepaid access regulations, financial institutions that offer prepaid access products should take risk management steps to reduce the ML/TF risks of these products and third-party payment processors (TPPP) that offer these products. For further guidance, please refer to the Prepaid Access and Stored Value and Third-Party Payment Processor sections.

2072. Why are sellers of prepaid access subject to prepaid access regulations?

FinCEN has determined that because sellers of prepaid access generally have face-to-face contact with consumers at the point-of-sale, they are in one of the best positions to collect customer identifying information and detect potentially suspicious activity.

2073. Are any persons who accept payments for an initial or subsequent loading of prepaid access not considered "sellers" for the purpose of regulatory requirements for prepaid access?

Yes. Persons who accept payments for an initial or subsequent loading of prepaid access are not considered "sellers" if they:

- Do not sell prepaid access under a prepaid program that can be used before the purchaser's identification can be obtained and verified; and
- Have implemented policies and procedures to reasonably prevent the sale of prepaid access (including closed-loop prepaid access) to funds that exceed US$10,000 to any person during any one day.

2074. How does the prepaid access final rule amend the regulatory requirements for MSBs?

In addition to updating the definition of "stored value" to "prepaid access," MSBs that qualify as providers and sellers of prepaid access may be required to file suspicious activity reports, register with FinCEN and take a number of other actions. Remaining regulations for MSBs remain unaffected by the

Prepaid Access rule. For further guidance on the AML/CFT requirements of MSBs, please refer to the Money Services Businesses section.

2075. Have additional regulations been proposed for prepaid access?

Yes. In 2011 FinCEN issued a proposed rule amending the definition of monetary instrument to include select tangible prepaid access devices for purposes of Report of International Transportation of Currency or Monetary Instruments (CMIR) requirements. In 2017 the U.S. Senate introduced a bill that would amend the definition of monetary instrument to include funds stored in a digital format (e.g., prepaid access devices, virtual currency).

Pursuant to the Dodd-Frank Wall Street Reform and Consumer Protect Act, the Consumer Financial Protection Bureau (CFPB) held a hearing in May 2012 regarding prepaid access, particularly general purpose reloadable (GPR) cards Pursuant to DFA, in 2016, the CFPB finalised the rule "Prepaid Accounts Under the Electronic Fund Transfer Act (Regulation E) and the Truth in Lending Act (Regulation Z)." However, this rule, which was scheduled to become effective on October 1, 2017, but has been put on hold under the Trump administration, focuses on prepaid consumer protection issues, not AML/CFT.

Additionally, the CFPB and other domestic and international organisations (e.g., OCC, FATF) are focused on "financial inclusion," the availability of financial services at affordable costs to disadvantaged and lower income segments of the economy, as it relates to prepaid access, mobile banking and other methods of payments.

2076. How do the FATF Recommendations address prepaid access?

FATF Recommendation 15 – New Technologies advises that countries and financial institutions conduct risk assessments to identify and evaluate the ML/TF risks and vulnerabilities of new technologies. FATF uses the term "new payment products and services" (NPPS) to describe some of the new product offerings (e.g., prepaid cards, mobile payments, electronic money, digital currencies).

FATF also published "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Systems" in 2013. For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

2077. What guidance has been issued on prepaid access?

The following are examples of information and guidance that have been issued on prepaid access:

- **"Prepaid Cards/Stored-Value Cards" subsection within Electronic Cash – Overview** within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **"E-Banking" and "Emerging Retail Payment Technologies"** within the "Retail Payment Systems" sections within the FFIEC Information Technology Examination Handbook by the FFIEC

- **Application of the Prepaid Access Rule to Closed Loop Prepaid Access Sold or Exchanged in a Secondary Market** (2013) by FinCEN
- **Application of the Prepaid Access Rule to Bank-Controlled Programs** (2012) by FinCEN
- **Outreach to the Prepaid Access Industry** (2012) by FinCEN
- **Frequently Asked Questions Related to Prepaid Access Final Rule** (2011) by FinCEN
- **Notice of Proposed Rulemaking: Bank Secrecy Act Regulations: Definition of "Monetary Instrument"** (2011) by FinCEN (related to Prepaid Access devices)
- **Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS)** (2014) by the Wolfsberg Group of Banks (Wolfsberg Group)
- **Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions** (2011) by the World Bank (WB) Report on Money Laundering Using New Payment Methods (2012) by the Financial Action Task Force (FATF)
- **Payroll Cards: An Innovative Product for Reaching the Unbanked and Underbanked** (2005) by the Office of the Comptroller of Currency (OCC)
- **The 2008 Survey of Consumer Payment Choice** by the Federal Reserve Bank of Boston
- **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by FATF
- **Consumer Payment Choice: A Central Bank Perspective by the Consumer Payments Research Center** at the Federal Reserve Bank of Boston
- **Prepaid Cards: Vulnerable to Money Laundering?** (2007) by the Federal Reserve Bank of Philadelphia
- **The Laws, Regulations, Guidelines, and Industry Practices That Protect Consumers Who Use Gift Cards** (2008) by the Federal Reserve Bank of Philadelphia
- **Emerging Risk Forum "Cash, Check, or Cell Phone?" Protecting Consumers in a Mobile Finance World** (2010) by the Federal Reserve Bank of Boston
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** (2010) by the World Bank (WB)
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** (2004) by the Bank of International Settlements (BIS)
- **Recommended Practices for Anti-Money Laundering Compliance for U.S.-Based Prepaid Card Programs** (2008) by the Network Branded Prepaid Card Association (NBPCA)
- **Person-to-Person Electronic Funds Transfers: Recent Developments and Policy Issues** (2010) by the Federal Reserve Bank of Boston

- **Understanding Risk Management in Emerging Retail Payments** (2008) by the Federal Reserve Bank of New York

Additional organisations providing guidance on stored-value products include, but are not limited to, the following:

- **Federal Reserve Bank of Boston Risk and Policy Analysis Unit**
- **Federal Reserve Bank of Boston Consumer Payments Research Center (CPRC)**
- **Federal Reserve Bank of Philadelphia Payment Cards Center**
- **Network Branded Prepaid Card Association (NBPCA)**

Key AML/CFT and Sanctions Requirements

2078. With which key AML/CFT and sanctions requirements are "providers of prepaid access" required to comply?

Prepaid access providers must comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML Program and ongoing monitoring and updates. The AML Program must be sufficiently detailed with standards and criteria specified for how the information is to be accessed, collected, verified and retained, and must have provisions addressing communication to employees and for the training of any individuals or entities acting as their agent. (Section 352)
- Retaining access to customer information that was collected, which must, at a minimum, include:
  - Name
  - Date of birth
  - Address
  - Identification number

Additionally, a provider must establish and maintain procedures to verify the identity of a person who obtains prepaid access under a prepaid program (similar in scope to Customer Identification Program [CIP] verification procedures of Section 326 of the USA PATRIOT Act).

- Retaining transaction records generated in the ordinary course of business that would be needed to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers, or other prepaid-related transactions. Such information must be retained for a period of five years after the last use of the prepaid access. Such information may include, but is not limited to:
  - Type of transaction (e.g., ATM withdrawals, POS purchase)
  - Amount and location of transaction
  - Date and time of transaction

  - Any other unique identifiers related to transactions

- Filing of Currency Transaction Reports (CTRs)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (i.e., Section 314(a) [in some cases mandatory]; Section 314(b) [optional])
- Registration with FinCEN
- OFAC and other sanctions program requirements

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to providers and sellers of prepaid access is provided below.

2079. With which key AML/CFT requirements are sellers of prepaid access required to comply?

Sellers of prepaid access are required to comply with the same AML/CFT requirements as providers. Among other things, "sellers of prepaid access" have an obligation to collect and retain customer information on the purchaser. FinCEN indicated there are two situations under which a seller of prepaid access must collect customer information. Sellers that sell prepaid access that allows access to funds under a "prepaid access program" without the verification of customer information are responsible for collecting customer information, or sellers that sell any type of prepaid access in a combined amount greater than US$10,000 in a day to a person or an entity (excluding the bulk sale exception noted above) must also obtain customer information.

2080. Are providers and sellers of prepaid access required to register with FinCEN as required for money services businesses?

Providers of prepaid access are required to register with FinCEN. Sellers of prepaid access are required to register with FinCEN, unless they are acting as an agent of an MSB.

2081. What information must a provider of prepaid access provide when registering with FinCEN?

In addition to a complete and accurate Registration for Money Services Businesses (RMSB) form, a prepaid access provider is, among other things, required to provide a complete list of the prepaid programs for which it serves as a provider (e.g., sellers of prepaid access that meet the regulatory definition of the Prepaid Access Rule).

For further guidance on RMSBs, please refer to the Registration section within the Money Services Businesses section.

2082. What guidance has FinCEN provided for expected efforts to prevent sales of US$10,000 of collective prepaid access?

According to FinCEN's Frequently Asked Questions regarding Prepaid Access published in March 2016, providers and sellers of prepaid access should, at a minimum, implement the following:

- Develop an internal policy regarding sales of prepaid access in excess of US$10,000 to a single individual in a day;
- Articulate the aforementioned internal policy with appropriate personnel in the organisation; and
- Monitor activity to avoid sales in excess of US$10,000 to a single individual in a day.

2083. Do providers and sellers of prepaid access have CIP obligations?

Providers and sellers of prepaid access are not subject to the CIP requirement (unless they are otherwise required to do so under the Bank Secrecy Act [BSA]/USA PATRIOT Act); however, they are subject to their own customer information recordkeeping requirement that mirrors the CIP requirement of Section 326 of the USA PATRIOT Act. As described above, entities that qualify as "providers of prepaid access" or "sellers of prepaid access" must obtain, verify and retain the following information on the customer involved in the initial purchase of the prepaid product:

- Name
- Date of birth
- Address
- Identification number

There may be situations in which both are responsible for collecting customer information. In these instances, providers and sellers must agree as to who will collect the information (although the provider will remain liable in any event). Where an entity qualifies as a "seller of prepaid access" for selling more than US$10,000 in prepaid access in a day to a person or an entity, there may be situations under which only the seller, but not the provider, is obligated to collect the customer information. For further guidance on CIP, please refer to Section 326 – Verification of Identification.

2084. Are providers and sellers of prepaid access subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No, unless the provider and seller of prepaid access is a bank subject to CIP requirements. Only institutions subject to the CIP requirement are required to identify beneficial owners under the Beneficial Ownership Rule. Providers and sellers of prepaid access who are not subject to the CIP requirement therefore are not required to identify beneficial owners. However, the Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future.

For further guidance, please refer to the sections Beneficial Owners and Section 352 – AML Program.

2085. Is there any circumstance in which a holder (e.g., consumer) of a prepaid access product may be subject to CIP requirements?

According to FinCEN's Frequently Asked Questions regarding Prepaid Access published in March 2016, if the provider or seller of prepaid access is a bank or other financial institution currently subject to the CIP requirement under Section 326 of the USA PATRIOT Act, a holder (e.g., consumer) of a general purpose prepaid card with the ability to reload creates a formal banking relationship equivalent to an account and therefore would be required to provide identifying information to satisfy CIP requirements. CIP is also applicable under arrangements where the bank contracts with third-party prepaid access program managers.

Under certain circumstances (e.g., payroll cards, government benefit cards, health benefit cards) where only the employer/provider can make deposits into the account or subaccount, the "customer" may be the employer/provider and not the underlying users.

2086. What other records must be retained by providers of prepaid access?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, "providers of prepaid access" must retain transactional records generated in the ordinary course of business that would be necessary to reconstruct prepaid access activation, loads, reloads, purchases, withdrawals, transfers or other prepaid-related transactions.

The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, broker-dealers, casinos) as well. For further guidance, please refer to the sections: BSA Recordkeeping Requirements and Nonbank Financial Institutions and Nonfinancial Institutions.

2087. How long are providers and sellers of prepaid access required to retain records?

Under federal law, both providers and sellers of prepaid access are required to retain records for five years. Providers of prepaid access must retain access to records for five years after the last use of the prepaid access. Sellers must retain access to records for five years from the date of the sale of the prepaid access. Some states may require longer retention periods.

2088. Are providers and sellers of prepaid access required to file CTRs?

Yes, providers and sellers of prepaid access are required to file CTRs. For a listing of financial institutions required to file CTRs at the time of this publication, please refer to the Currency Transaction Reports section.

2089. Can providers and sellers of prepaid access grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions, credit unions) can grant exemptions, and then only for their U.S. customers.

2090. Do providers and sellers of prepaid access have their own, unique SAR form?

No. Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms (e.g., Suspicious Activity Report by Money Services Businesses [SAR-MSB]) with a single form that must be submitted

electronically. The filing criteria for providers and sellers of prepaid access, however, differs from other types of financial institutions (e.g., banks, broker-dealers) as detailed below.

As of April 1, 2013, providers and sellers of prepaid access must submit the new SAR (and other FinCEN Reports) electronically through the BSA E-Filing System.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2091. What types of activities require a SAR to be filed for prepaid access providers and sellers?

Prepaid access providers and sellers should file a SAR upon detection of the following activities:

- Any transactions conducted or attempted by, at, or through a "provider" or "seller of prepaid access" involving or aggregating funds or other assets of at least US$2,000 when the "provider" or "seller of prepaid access" knows, suspects or has reason to suspect that:
  - The transaction involves funds derived from illegal activity or is intended or conducted in order to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
  - The transaction is designed, whether through structuring or other means, to evade any regulations promulgated under the BSA.
  - The transaction has no business or apparent lawful purpose and the "provider" or "seller of prepaid access" knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.
  - The transaction involves the use of the "provider" or "seller of prepaid access" to facilitate criminal activity.

There are other SAR reporting requirements additionally applicable to issuers of money orders or traveller's checks in connection with their review of clearance records that involves or aggregates funds or other assets of at least US$5,000. For red flags that assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

2092. How many of the SARs filed in a calendar year involve prepaid access?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports involving prepaid access totalled nearly 41,000 (2 percent) and were distributed across financial institution types as follows:

- Depository institutions: 25,000 cases (62 percent)
- Money services businesses (MSBs): 13,000 cases (32 percent)

- Other types of financial institutions (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily): 2,700 cases (7 percent)
- Securities and futures firms: 59 cases (0.1 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 3 cases (less than 0.1 percent)
- Insurance companies: 1 case (less than 0.1 percent)
- Housing GSEs: 0 cases (0 percent)
- Casinos and card clubs: 0 cases (0 percent)

2093. Are persons transporting or shipping prepaid access products across the U.S. border in an aggregate amount of more than US$10,000 required to file a Report of International Transportation of Currency or Monetary Instrument (CMIR)?

Not currently. However, in October 2011, FinCEN proposed amending the definition of "monetary instruments" to include tangible prepaid access devices that would be subject to reporting on CMIRs; the proposed rule was withdrawn in 2014 due to industry pushback. FinCEN may issue a reworked rule in 2017.

Initially the proposed rule defined the term "tangible prepaid access device" as the following:

- Any physical item that can be transported, mailed, or shipped into or out of the United States and the use of which is dedicated to obtaining access to prepaid funds or the value of funds by the possessor in any manner without regard to whom the prepaid access is issued.

This definition would include devices such as general-use prepaid cards, gift cards, store cards, payroll cards, government benefit cards, and any tangible device to the extent that they can provide access to prepaid funds or the value of funds by being readable by a device employed for that purpose by merchants (e.g., cell phones, key fobs). The definition does not extend to credit and debit cards.

Similar to the exclusion for a traveller's check issuer or its agent, a business or its agent offering prepaid devices prior to their delivery to a seller for sale to the public would not be subject to the CMIR filing requirement.

For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

2094. Are providers and sellers of prepaid access required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2095. Do providers and sellers of prepaid access have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Providers and sellers of prepaid access can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyberattacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations;
- Fulfilment of regulatory reporting obligations;
- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);

- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2096. Should providers and sellers of prepaid access address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber incident or through fines levied by regulatory authorities), providers and sellers of prepaid access can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2097. Do providers and sellers of prepaid access have additional obligations as they relate to their agents?

The AML Program of "providers" and "sellers of prepaid access" should address communication and training of any individuals or entities acting as their agents. For further guidance, please refer to the Agents of MSBs section.

2098. Who is responsible for examining providers and sellers of prepaid access for compliance with AML/CFT laws and regulations?

The responsibility for examining providers and sellers of prepaid access is delegated to the IRS by FinCEN, unless the provider or seller is a bank or financial institution regulated by the SEC or CFTC. Many states also examine providers and sellers of prepaid access and their agents for compliance with AML/CFT and other regulations if they come within the scope of licensure within the state.

Broker-Dealers in Securities

Definitions

2099. How are the terms "broker" and "dealer" defined?

The Securities Exchange Act of 1934 (Exchange Act) defines these terms broadly:

- A "broker" is "any person engaged in the business of effecting transactions in securities for the account of others."
- A "dealer" is "any person engaged in the business of buying and selling securities for his/her own account, through a broker or otherwise."

2100. Are "traders" included in the definition of "dealers"?

No. "Traders" are persons who buy and sell securities for their own personal account, not as a part of a business.

2101. What are the heightened money laundering and terrorist financing risks of the securities industry?

As with banks, broker-dealers can be vulnerable to the laundering of illicit proceeds through their financial system. However, vulnerabilities also exist, not just from customers, but insiders. Although not specific to broker-dealers, the threats within the industry are difficult to monitor and mitigate due to the complex nature of the products and services offered by broker-dealers.

2102. Which types of broker-dealers in securities are required to maintain an AML Program under Section 352 of the USA PATRIOT Act?

Virtually all broker-dealers in securities registered or required to be registered with the U.S. Securities and Exchange Commission (SEC) under the Exchange Act are required to maintain an AML Program and comply with other AML/CFT laws and regulations.

Registered broker-dealers are also referred to as "members."

2103. Are "associated persons" (e.g., employees) of broker-dealers required to register with the SEC?

The Exchange Act defines "associated persons" as "any partner, officer, director, branch manager, or employee of the broker-dealer, any person performing similar functions, or any person controlling, controlled by or under common control with, the broker-dealer."

Associated persons who "effect transactions in securities" solely for their broker-dealer are not required to register separately with the SEC but must meet licensing requirements (e.g., passing a securities qualification examination such as the Series 7). These licensed persons are referred to as "registered representatives."

Registered representatives who wish to engage in an independent securities business outside of the "associated persons" relationship must register with the SEC.

Associated persons actively engaged in the management of the broker-dealer (e.g., sole proprietors, officers, partners, managing directors) are required to register as principals.

2104. Who is responsible for examining broker-dealers for compliance with AML/CFT laws and regulations?

The SEC is responsible for examining registered broker-dealers for compliance with AML/CFT laws and regulations.

In addition, oversight and examinations may be conducted by the other self-regulatory organisations (SROs). The responsible SRO is based upon where the broker-dealer is registered and/or listed.

2105. What is a self-regulatory organisation (SRO)?

A self-regulatory organisation (SRO) is a nongovernment organisation that has the power to create and enforce industry regulations and standards under the supervision of a federal agency.

Examples include, but are not limited to, the following:

- Financial Industry Regulatory Authority (FINRA) (formerly known as the National Association of Securities Dealers [NASD])
- New York Stock Exchange (NYSE)
- American Stock Exchange (Amex)
- Municipal Securities Rulemaking Board (MSRB)

2106. When broker-dealers are members of more than one SRO, which one is responsible for oversight and examinations?

The SEC designates a responsible SRO as the "designated examining authority" where multiple SROs are involved.

2107. What key AML/CFT guidance has been issued on broker-dealers?

The following key AML/CFT guidance and resources have been issued on broker-dealers:

- Anti-Money Laundering (AML) Source Tool for Broker-Dealers by the U.S. Securities and Exchange Commission (SEC)
- Anti-Money Laundering Template for Small Firms by Financial Industry Regulatory Authority (FINRA)
- OFAC Search Tool by FINRA
- AML E-Learning Courses (2012) by FINRA
- Money Laundering and Terrorist Financing in the Securities Sector (2009) by Financial Action Task Force (FATF)

- Wolfsberg Frequently Asked Questions on Selected Anti-Money Laundering Issues in the Context of Investment and Commercial Banking (2006) by the Wolfsberg Group of Banks (Wolfsberg Group)
- Principles on Client Identification and Beneficial Ownership for the Securities Industry (2004) by International Organisation of Securities Commissions (IOSCO)
- Guidance on Sharing of Suspicious Activity Reports by Securities Broker-Dealers, Futures Commission Merchants, and Introducing Brokers in Commodities (2006) by FinCEN
- Question and Answer Regarding the Broker-Dealer Customer Identification Program Rule (2003) by Securities and Exchange Commission (SEC)
- Frequently Asked Questions – Customer Identification Program Responsibilities under the Agency Lending Disclosure Initiative (2006) by FinCEN
- Customer Identification Program Rule No-Action Position Respecting Broker-Dealers Operating Under Fully Disclosed Clearing Agreements According to Certain Functional Allocations (2008) by FinCEN
- Bank Secrecy Act Obligations of a U.S. Clearing Broker-Dealer Establishing a Fully Disclosed Clearing Relationship with a Foreign Financial Institution (2008) by FinCEN
- Application of the Regulations Requiring Special Due Diligence Programs for Certain Foreign Accounts to the Securities and Futures Industries (2006) by FinCEN
- Foreign Asset Control Regulations for the Securities Industry (2004) by OFAC
- Opening Securities and Futures Accounts from an OFAC Perspective (2008) by OFAC
- Risk Factors for OFAC Compliance in the Securities Industry (2008) by OFAC

Key AML/CFT and Sanctions Requirements

2108. With which key AML/CFT and sanctions requirements are broker-dealers required to comply?

Broker-dealers must comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program, approved in writing by senior management, that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an annual independent review of the AML Program and ongoing monitoring and updates (Section 352)
- Establishment of a Customer Identification Program (CIP) (Section 326)
- Establishment of a customer due diligence program that identifies beneficial owners under select circumstances (Section 312, Beneficial Ownership Rule)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- Complying with Special Measures (Section 311)
- Obtaining Foreign Bank Certifications (Section 319(b))
- Establishing an enhanced due diligence (EDD) program for foreign correspondent account relationships, private banking relationships and politically exposed persons (PEPs)
- OFAC and other sanctions requirements
- The AML/CFT requirements for broker-dealers are implemented under 31 C.F.R. 1023 – Rules for Brokers or Dealers in Securities.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to broker-dealers is provided below.

2109. Are broker-dealers required to conduct a risk assessment?

Broker-dealers are required to develop and maintain risk-based AML Programs. This means that they are expected to understand their risks and document their rationale for implementing controls for their AML Programs. There has to date not been the same degree of regulatory emphasis for broker-dealers on preparing formal AML/CFT and sanctions risk assessments as there has been for banking organisations; however, as a leading practice, many of the same risk assessment approaches used by banking organisations could apply to broker-dealers.

Additionally, any NBFI that is affiliated with a bank holding company will, by necessity, need to perform a risk assessment in order for the bank holding company to meet regulatory expectations for performing an enterprisewide risk assessment.

For further guidance, please refer to the Risk Assessments section.

2110. Which securities rules parallel the AML Program requirement of Section 352?

FINRA Rule 3310 (consolidated NASD Rule 3011 and NYSE Rule 445) parallels the AML Program requirements of Section 352 of the USA PATRIOT Act. SROs often issue parallel rules consistent with both FINRA and the BSA (e.g., MSRB Rule G-41 applies to municipal securities dealers).

The following Exchange Act rules address the other BSA reporting and recordkeeping requirements (e.g., SARs) for broker-dealers:

- 17 C.F.R. 240.17a-8 – Financial Recordkeeping and Reporting of Currency and Foreign Transactions; and
- 17 C.F.R. 405.4 – Financial Recordkeeping and Reporting of Currency and Foreign Transactions by Registered Government Securities Brokers and Dealers.

For further guidance on AML/CFT rules for broker-dealers, please visit the SEC's website "AML Source Tool for Broker-Dealers" at http://www.sec.gov/about/offices/ocie/amlsourcetool.htm#3.

2111. Did the consolidated FINRA Rule 3310 have any significant changes to the AML/CFT requirements for broker-dealers?

No. The consolidated FINRA Rule 3310 did not make any significant changes to the existing AML/CFT requirements for broker-dealers.

2112. Are there special requirements for the AML compliance officer of a broker-dealer?

Neither the USA PATRIOT Act nor FINRA Rule 3310 (formerly NASD rule 3011) requires AML compliance officers to register either as representatives or as principals. However, FINRA's general registration requirements state that persons who engage in the supervision, solicitation or conduct of investment banking or securities business for member firms need to register. Thus, being the AML compliance officer of a member firm would not necessarily trigger registration requirements, but instructing registered persons on particular securities product could.

Generally, the individual responsible for overseeing the entire AML Program should be an officer of the broker-dealer.

Broker-dealers are, however, not only required to designate an AML compliance officer, but also to provide the following information to FINRA through the FINRA Contact System (FCS):

- Name
- Title
- Mailing address
- Email address
- Telephone number
- Facsimile number

2113. Is there a comparable broker-dealer rule for the Customer Identification Program (CIP) requirement under Section 326 of the USA PATRIOT Act?

Multiple broker-dealer rules related to customer records, recordkeeping requirements and other related matters already exist that are consistent with the CIP requirement and other customer due diligence requirements of the USA PATRIOT Act. These include, but are not limited to, the following:

- Exchange Act Rule 17 C.F.R. 240.17a-3: Records to be Made by Certain Exchange Members, Brokers and Dealers

- Exchange Act Rule 17 C.F.R. 240.17a-4: Records to be Preserved by Certain Exchange Members, Brokers and Dealers
- FINRA Rule 2090 – Know Your Customer
- FINRA Rule 2111 – Suitability

These rules are generally referred to as "books and records" requirements.

2114. What is the "suitability" rule and how does it compare to the CIP requirement?

The suitability rule differs in purpose, requirements and timing from the CIP requirement. The purpose of the rule is to assess the suitability of investments for potential clients, not per se to verify their identities. The suitability rule requires the following information in addition to that required for CIP:

- Telephone number
- Employment status (including occupation and whether the customer is an associated person of a broker-dealer)
- Annual income
- Net worth (excluding value of primary residence)
- Investment objectives
- Signatures and/or approvals by appropriate personnel (dated in some instances)

Unlike the CIP requirement, broker-dealers are not prohibited from opening an account if the required information is not obtained. Information can be obtained during the account opening process.

2115. Are broker-dealers required to obtain the source of funds from their customers under the BSA?

Broker-dealers are specifically required to obtain the source of funds for their private banking customers pursuant to Section 312 of the USA PATRIOT Act. However, leading practice suggests broker-dealers also include a source of funds requirement as part of their CDD or EDD program.

2116. How is the term "account" defined for a broker-dealer?

The term "account" is defined as "a formal relationship with a broker-dealer established to effect transactions in securities, including, but not limited to, the purchase or sale of securities, securities loaned and borrowed activity and the holding of securities or other assets for safekeeping or as collateral." Examples include, but are not limited to, the following:

- Cash accounts
- Margin accounts
- Prime brokerage accounts
- Accounts established to engage in securities repurchase transactions

It does not include an account the broker-dealer acquires through an acquisition, merger or purchase of assets or assumption of liabilities or that is opened to participate in an employee benefit plan established under the Employee Retirement Income Security Act (ERISA).

For additional guidance on the types of accounts and customers subject to the Customer Identification Program (CIP) requirement, please refer to Section 326 – Verification of Identification.

2117. Who "owns" the account/customer when both introducing and clearing brokers are involved?

Both the introducing broker and clearing broker "own" the account and therefore are obligated to comply with applicable AML/CFT requirements (e.g., performing CIP, monitoring and reporting suspicious activity). However, under certain circumstances, introducing and clearing brokers are able to rely on each other for parts of their CIP. For example, an introducing broker would be in a better position to perform CIP since it established the relationship with the customer. The clearing broker would likely be in a better position to monitor for suspicious activity since it processes the transactions and has visibility into the customer's transaction activity.

2118. What are the risks of the relationships between introducing brokers and clearing brokers?

Both the introducing broker and clearing broker face third-party risk because the information which the other financial institution relied upon to support the AML/CFT Compliance Program (e.g., CIP, sanctions screening, monitoring for potentially suspicious activity) may not adequately execute its AML/CFT responsibilities consistent with regulatory and/or internal standards.

For further guidance on third-party risk, please refer to the Know Your Third Parties section.

2119. Is someone with trading authority over an account considered a "customer" under the CIP requirement?

A person with trading authority prior to the effective date of the CIP regulation is not a "customer." However, any person granted trading authority after the effective date of the CIP regulation is a customer and is subject to the requirements of CIP.

2120. How is the term "private banking account" defined for broker-dealers?

The term "private banking account" is defined as an account that:

- Requires a minimum deposit of assets of at least US$1 million;
- Is established or maintained on behalf of one or more non-U.S. persons who are direct or beneficial owners of the account; and
- Has an employee assigned to the account who is a liaison between the broker-dealer and the non-U.S. person.

For additional guidance on private banking and related EDD requirements, please refer to the Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts section.

2121. How is the term "correspondent account" defined for broker-dealers?

The term "correspondent account" is defined as "any formal relationship established for a foreign financial institution to provide regular services to effect transactions in securities." According to the U.S. Department of the Treasury, correspondent accounts for broker-dealers include:

- Accounts to purchase, sell or lend securities (e.g., securities repurchase agreements)
- Prime brokerage accounts
- Accounts trading foreign currency
- Over-the-counter derivatives contracts
- Custody accounts holding settled securities as collateral

For further guidance on correspondent banking and EDD requirements, please refer to the Correspondent Banking and Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts sections.

2122. Are broker-dealers allowed to provide services to a foreign shell bank through a correspondent account?

No. Broker-dealers are prohibited from providing any service to a foreign shell bank. In addition, they must ensure they are not providing services to a shell bank through a correspondent relationship by requesting a Foreign Bank Certification from their respondents. For additional guidance on Foreign Bank Certifications, please refer to the Foreign Bank Certifications section.

2123. What types of customers, accounts or transactions may present regulatory challenges for broker-dealers?

Challenges arise in identifying and verifying the beneficial owner of accounts and/or underlying assets within accounts maintained for these types of customers by broker-dealers.

- **Nondeposit investment products (NDIPs)** – NDIPs include various types of investment products (e.g., securities, bonds, fixed or variable annuities, mutual funds) that may be offered by a broker-dealer directly through proprietary programs with subsidiaries or affiliates, or indirectly through third-party networking arrangements (e.g., foreign finders). Reliance on third parties to conduct adequate due diligence and monitoring for potentially suspicious activity in third-party networking arrangements heighten the risks of NDIPs.
- **Correspondent accounts** – Includes accounts to purchase, sell, lend or otherwise hold securities, including securities repurchase agreements; prime brokerage accounts that clear and settle securities transactions for clients; accounts for trading foreign currency; custody accounts for holding securities or other assets in connection with securities transactions as collateral; and over-the-counter derivatives contracts.
- **Master/sub-accounts** – Master/sub-accounts are an account trading model in which a master account is established for a client that permits subordinate accounts (sub-accounts) for different

trading activities. The master account is typically established for a legal entity while sub-accounts are established for use by individual traders associated with the legal entity.

- **Omnibus accounts** – Omnibus accounts are established by financial intermediaries for the purpose of executing transactions that will clear or settle at another financial institution.

For further guidance on correspondent accounts, please refer to the Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Correspondent Banking sections. For further guidance on customer due diligence, please refer to the sections: Know Your Customer, Customer Due Diligence and Enhanced Due Diligence and Beneficial Owners.

2124. How do the obligations of the Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule), finalised in July 2016, impact obligations for broker-dealers?

FinCEN's Customer Due Diligence Requirements for Financial Institutions rule (Beneficial Ownership Rule), finalised in July 2016, requires financial institutions subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers.

Broker-dealers are already required to obtain beneficial ownership information in the following situations, as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule expands the obligation to all legal entity customers, with limited exceptions.

The Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future.

For further guidance on the Beneficial Ownership Rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

2125. Are broker-dealers required to file CTRs?

Yes. Broker-dealers are required to file CTRs. For a listing of financial institutions required to file CTRs at the time of this publication, please refer to the Currency Transaction Reports section.

2126. Can broker-dealers grant CTR exemptions?

No. Only depository institutions (e.g., banks, savings associations, thrift institutions, credit unions) can grant exemptions.

2127. Do broker-dealers have their own, unique SAR form?

No. FinCEN replaced industry-specific SAR forms with one new SAR for all covered financial institutions. As of April 1, 2013, broker-dealers must submit the new SAR (and other FinCEN Reports) electronically through the BSA E-Filing System.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2128. What types of activities require a SAR to be filed for broker-dealers?

Upon the detection of the following activities, broker-dealers should file a SAR:

- Transactions aggregating to US$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA) – Any transaction(s) totalling or aggregating to at least US$5,000 conducted by a suspect through the broker-dealer, where the broker-dealer knows, suspects or has reason to suspect that the transaction: involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
- Evasion – A SAR should be filed in any instance where the broker-dealer detects that the transaction was designed, whether through structuring or other means, to evade any BSA regulations.
- No business or apparent lawful purpose – The transaction has no business or apparent lawful purpose and there is no known reasonable explanation for the transaction after examination of available facts, including the background and possible purpose of the transaction.
- Facilitation of criminal activity – The transaction involves the use of the broker-dealer to facilitate criminal activity.

For red flags to assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

2129. Are there exceptions to the SAR requirement for broker-dealers?

Yes. The SAR requirement for broker-dealers contains three exceptions from reporting violations that otherwise would be reported to various law enforcement authorities. The following activities are not required to be reported:

- A robbery or burglary that is reported by the broker-dealer to appropriate law enforcement authorities.
- Lost, missing, counterfeit or stolen securities that are reported by the broker-dealer pursuant to the reporting requirements of Exchange Act rule 17 C.F.R. 240.17f-1 – Requirements for Reporting and Inquiry With Respect to Missing, Lost, Counterfeit or Stolen Securities. Broker-dealers are required to report to the Lost and Stolen Securities Program (LSSP Program) administered by the Securities Information Center (SIC) on behalf of the SEC. Broker-dealers are also required to

check the validity of securities certificates in excess of US$10,000 that come into their possession by querying the LSSP database. Broker-dealers can voluntarily report or inquire about other securities certificates (e.g., cancelled securities).

- A violation of the federal securities laws or rules of a self-regulatory organisation (SRO) by the broker-dealer, its officers, directors, employees or registered representatives, that is reported appropriately to the SEC or an SRO, except for a violation of the following Exchange Act rules, if the violation is appropriately reported to the SEC, or an SRO, which must be reported on a SAR:
  - 17 C.F.R. 240.17a-8 – Financial Recordkeeping and Reporting of Currency and Foreign Transactions; or
  - 17 C.F.R. 405.4 – Financial Recordkeeping and Reporting of Currency and Foreign Transactions by Registered Government Securities Brokers and Dealers.

2130. Who is responsible for reporting suspicious activity on a customer that is shared between introducing and clearing firms?

Introducing firms are often in a better position to "know the customer," and therefore, to identify potentially suspicious activity at the account opening stage, including verification of the identity of the customer and deciding whether to open an account for a customer. Clearing firms, in turn, may be in a better position to monitor customer transaction activity including, but not limited to, trading, wire transfers and the deposit and withdrawal into and out of accounts of different financial institutions. The obligation to file a SAR rests with each broker-dealer involved in the transaction, but only one SAR filing is required per transaction.

For additional guidance on third-party reliance, please refer to the Third-Party Reliance section.

2131. What are some of the statistics and trends in SAR filings for broker-dealers?

According to FinCEN, using 2016 as the frame of reference, of the 1.98 million SARs filed from January 1, 2016 through December 31, 2016, securities and futures firms (e.g., clearing brokers [securities], introducing brokers [securities], introducing brokers [commodities], futures commission merchants, investment companies, investment advisers, retail foreign exchange dealers, holding companies, subsidiaries of holding companies) filed over 19,000 SARs or 1 percent of all filings during this period. Highlights included:

- Sixteen percent of SARs were filed on activity taking place in California, 12 percent in Massachusetts, 11 percent in New York, and 10 percent in Rhode Island;
- Ninety percent of SARs were filed on customers, 7 percent on unknown/blank relationship types and 1 percent on individuals with no relationship with the securities and futures firm;
- Fifty-eight percent of SARs involved funds transfers; 34 percent involved stocks; 24 percent involved personal/business checks; 16 percent involved mutual funds; 15 percent involved penny stocks/microcap securities; and 5 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by securities and futures firms:

- Other Suspicious Activities: 42 percent (included more than 5,000 cases related to identity theft; nearly 2,700 cases related to account takeover; over 2,600 cases related to embezzlement/theft/disappearance of funds; over 1,100 cases related to unauthorised electronic intrusion; over 1,400 cases related to elder financial exploitation; and 147 cases related to corruption [foreign and domestic]);
- Fraud: 30 percent (included more than 11,800 cases related to wire transfer, ACH and check fraud) (separate from Mortgage Fraud, which accounted for less than 0.1 percent);
- Securities/Futures/Options: 8 percent (included more than 1,300 cases related to insider trading and over 1,200 cases related to market manipulation/wash trading);
- Money Laundering: 13 percent;
- Terrorism/Terrorist Financing: 0.04 percent (19 cases).

2132. What is "identity theft," and how can broker-dealers combat the rise in identity theft-related crime?

Identity theft is defined as fraud committed or attempted using the identifying information of another person without authority.

Some broker-dealers are required to implement an Identity Theft Prevention Program (ITPP) to identify, detect, prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. An ITPP requires the following four basic elements:

- Identification of relevant red flags (i.e., pattern, practice or specific activity that indicates the possible existence of identity theft);
- Implementation of a monitoring program to detect identity theft red flags;
- Establishment of appropriate responses to detected red flags to prevent and mitigate identity theft; and
- Written policies and procedures and periodic updates of the ITPP (e.g., changes to addresses as they relate to identity theft; changes in methods to detect, prevent or mitigate identity theft; changes in the types of accounts offered or maintained; changes in business arrangements, such as mergers, acquisitions, alliances, joint ventures, and service provider arrangements).

Additionally, broker-dealers must:

- Obtain approval of their initial ITPP by the board of directors, a committee of the board, or a designated employee at the level of senior management; the financial institution may determine whether ongoing changes to the ITPP require approval by the board of directors/committee/senior management;
- Involve the board of directors, a committee of the board, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the ITPP;

- Train relevant staff;
- Oversee service provider arrangements to ensure the activity of the service provider is conducted in accordance with the financial institution's ITPP; and
- Conduct periodic assessments to determine whether the financial institution offers or maintains covered accounts; the assessment should consider the types of accounts offered, the methods of account opening, the methods/channels provided to access accounts and its previous experiences with identity theft.

For further guidance, please refer to the Identity Theft and Identity Theft Prevention Program section.

2133. What is "insider trading," and is all insider trading illegal?

"Insider trading" refers to the buying and selling of stocks by corporate insiders (e.g., employees, directors). According to the SEC, there are two types of insider trading:

- **Legal insider trading** – Conducted in accordance with securities laws and internal company policies that must be reported by the broker-dealer to the SEC (e.g., statement of ownership [initial, changes, deferred] on Forms 3, 4 and 5 respectively).
- **Illegal insider trading** – Conducted in violation of securities laws (e.g., may involve a breach of fiduciary duty or violation of law such as "tipping" [e.g., disclosing material non-public information]).

For further guidance on insider trading, please refer to the following Exchange Act rules:

- 17 C.F.R. 240.10b5-1 – Trading "On the Basis of" Material and Non-public Information in Insider Trading Cases; and
- 17 C.F.R. 240.10b5-2 – Duties of Trust or Confidence in Misappropriation Insider Trading Cases

2134. Are broker-dealers required to report cases of illegal insider trading on SARs?

Broker-dealers are required to file SARs on the "facilitation of criminal activity involving the use of a broker-dealer," also referred to as insider abuse. Illegal insider trading is one example of insider abuse where employees can use their specialised knowledge to evade controls implemented to guard against noncompliance with internal policies and procedures and violations of law.

Other types of SAR characterisations specific to the securities/futures industry include, but are not limited to, the following:

- Market manipulation/wash trading
- Misappropriation
- Unauthorised pooling

2135. What are penny stocks? How can they be used to facilitate money laundering?

Penny stocks, also known as microcap securities, generally refer to securities from private or public companies trading at less than US$5 per share. Penny stocks can be traded on both the over-the-counter market and securities exchanges, both foreign and domestic.

Due to their low cost and difficulty to price, penny stocks can be vulnerable to manipulation by corporate insiders to facilitate illegal insider trading.

2136. What are bearer shares? What are the money laundering risks of bearer shares?

Bearer shares are negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate. Similar to cash and other negotiable instruments, the inability to trace the origin or owner heightens the money laundering and terrorist financing risk of bearer shares.

2137. Are owners required to report changes in ownership of bearer shares in the United States?

No. There are no requirements to report changes in ownership of bearer shares in the United States.

The international transportation of bearer shares is required to be reported on the Reports of International Transportation of Currency or Monetary Instruments (CMIRs). CMIRs must be filed on the physical cross-border movement of currency and monetary instruments in excess of US$10,000 which includes bearer shares.

For further guidance on CMIRs, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

2138. What measures does FATF suggest to mitigate the ML/TF risks of bearer shares?

In an interpretive note to Recommendation 24, FATF suggests the following measures to mitigate the risks of bearer shares:

- Prohibiting bearer shares;
- Converting bearer shares into registered shares;
- Immobilising bearer shares by requiring that they be held with a regulated financial institution or professional intermediary; or
- Requiring shareholders with a controlling interest to notify the company and the company to record their identity.

2139. Can broker-dealers share SARs and SAR information with SROs?

To enable SROs to monitor and examine broker-dealers for compliance with AML/CFT laws and regulations, FinCEN issued a ruling allowing broker-dealers to share SARs and SAR information with their SROs, under certain circumstances.

For further guidance, please refer to 31 C.F.R. 1023.320 – Reports by Brokers or Dealers in Securities of Suspicious Transactions.

2140. Are there instances in which a broker-dealer should notify regulators and law enforcement in advance of filing a SAR?

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including, but not limited to, ongoing money laundering schemes or detection of terrorist financing, broker-dealers should immediately notify regulators and law enforcement, even before the SAR is filed.

FinCEN and the SEC have both established hotlines, 1.866.556.3974 (FinCEN) and 1.202.551.SARS (SEC SAR Alert Message), for broker-dealers to expedite reports to law enforcement on suspicious transactions that may relate to recent terrorist activity against the United States.

2141. How often must broker-dealers conduct independent tests of their AML Programs?

Under FINRA Rule 3310 (consolidated NASD Rule 3011 and NYSE Rule 445), broker-dealers that do not execute transactions for customers or otherwise hold customer accounts or act as an introducing broker with respect to customer accounts (e.g., engage solely in proprietary trading or conduct business only with other broker-dealers) are obligated to independently test their AML Program every two years.

All other broker-dealers are required to test their AML Programs annually (on a calendar-year basis), with more frequent testing if circumstances warrant.

2142. What are the key recordkeeping requirements of the BSA for broker-dealers?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained by broker-dealers, such as the following:

- When required, a taxpayer identification number (TIN) (or passport number or description of a government-issued identification for non-resident aliens) of each person for whom a deposit or share account is opened and for each person who has a financial interest in the account
- List of names, addresses and account or credit line numbers of those persons from whom the broker-dealer was unable to obtain the above information
- Each document granting signature or trading authority over each customer's account
- Each record described in Exchange Act Rules 17 C.F.R. 240.17a-3(a) (1), (2), (3), (5), (6), (7), (8) and (9)
- A record of each remittance or transfer of funds or of currency, checks, other monetary instruments, investment securities or credit of more than US$10,000 to a person, account or place outside of the United States
- A record of each receipt of currency, other monetary instruments, checks or investment securities and of each transfer of funds or credit of more than US$10,000 received on any one occasion directly and not through a domestic financial institution, from any person, account or place outside of the United States

The above applies to broker-dealers. The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, currency dealers or exchangers, casinos) as well. For

further guidance, please refer to the BSA Recordkeeping Requirements, Money Services Businesses and Casinos and Card Clubs sections.

2143. How long must broker-dealers retain records?

The Exchange Act requires broker-dealers to retain records for six years in some instances. The Exchange Act also specifies that the records must be stored in an "easily accessible place" in the first two years.

Some states, as well as international jurisdictions in which U.S. broker-dealers may operate, may require longer retention periods.

2144. Are broker-dealers required to comply with OFAC and sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2145. Do broker-dealers have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Broker-dealers can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyber attacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

The **U.S. Securities and Exchange Commission (SEC)** adopted multiple rules to address cybersecurity risks including, but not limited to, the following:

- Regulation Systems Compliance and Integrity (SCI)

- Regulation S-P
- Regulation SDR
- Regulation S-ID: Subpart C: Identity Theft Red Flags
- Exchange Act Rule 13n-6
- Exchange Act Rule 15c3-5
- Investment Company Act Rule 38-1
- Investment Advisers Act Rule 206(4)-7

The SEC published guidelines on cybersecurity preparedness:

- Conducting periodic assessments on vulnerabilities, internal and external threats, controls, impact of threats, effectiveness of cybersecurity governance structure that also addresses identity theft, data protection, fraud and business continuity;
- Developing a strategy designed to prevent, detect and respond to cybersecurity threats; and
- Implementing the cybersecurity strategy through written policies and procedures and training.

While public companies are required to report any incident that causes "material harm," they are not specifically required to disclose cybersecurity failures and risks. In 2011, the SEC published guidance, not rules, on the disclosure obligations relating to cybersecurity risks and cyber incidents. Public companies are expected to disclose cybersecurity risks and cyber incidents that could have a "material adverse effect on the business." With each publicised cyber attack or data breach, more pressure is being placed on the SEC to provide more clarity on previous guidance and issue rules requiring disclosures of cybersecurity risks and failures.

Additionally, some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2146. Should broker-dealers address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the SEC settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber incident or through fines levied by regulatory authorities), broker-dealers can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2147. What common deficiencies have been identified in enforcement actions involving broker-dealers?

The following areas are some of the common deficiencies in AML/CFT compliance programs that have been identified in recent enforcement actions involving broker-dealers:

- Inadequate AML/CFT policies and procedures (e.g., not tailored to different lines of business)
- Deficient KYC/CDD/EDD programs
    - Failure to address customer due diligence (CDD) and enhanced due diligence (EDD) for high-risk customers and products/services (e.g., beneficial owners, foreign correspondents)
- Inadequate suspicious activity monitoring program and suspicious activity report (SAR) filing program, including, but not limited to, the following deficiencies:
    - Lack of coverage of high-risk customers/transactions leading to the failure of filing SARs on potentially suspicious activities (e.g., high-volume trading)
    - Incomplete data feeds into transaction monitoring systems
    - Failure to investigate alerts triggered in automated transaction monitoring systems
    - Failure to file timely SARs
- Insufficient staff to evaluate suspicious activity monitoring alert in a timely manner

For further details of enforcement actions involving broker-dealers, please refer to the Key U.S. Enforcement Actions and Settlements section. For further guidance on enforcement actions, please refer to the Enforcement Actions section.

Futures Commission Merchants and Introducing Brokers in Commodities

Definitions

2148. What is a futures commission merchant (FCM)?

An FCM is a person or entity registered, or required to register, as an FCM with the U.S. Commodity Futures Trading Commission (CFTC) under the Commodity Exchange Act (CEA), except a person who registers pursuant to 4(f)(a)(2) of the CEA. FCMs conduct transactions in the futures contract market in a manner similar to that of brokers in the securities market.

2149. What is a "futures contract"?

The CFTC defines "futures contract" as "an agreement to purchase or sell a commodity for delivery in the future:

- [A]t a price that is determined at initiation of the contract;
- [T]hat obligates each party to the contract to fulfil the contract at the specified price;
- [T]hat is used to assume or shift price risk; and
- [T]hat may be satisfied by delivery or offset."

2150. What is a "commodity" and what types are traded in the futures contract market?

The CEA defines "commodity" as including the following:

- "[T]he agricultural commodities enumerated in Section 1a(9) of the Commodity Exchange Act, 7 USC 1a(9), and all other goods and articles, except onions as provided in Public Law 85-839 (7 USC 13-1), a 1958 law that banned futures trading in onions, and all services, rights, and interests in which contracts for future delivery are presently or in the future dealt in; and
- [A]n agricultural product or a natural resource as opposed to a financial instrument such as a currency or interest rate."
- Types of commodities traded in the futures contract market include, but are not limited to, the following:
- Agriculture (e.g., live cattle, corn, soybeans, wheat)
- Energy (e.g., crude oil, Brent crude, natural gas)
- Metals (e.g., copper, gold, silver)
- Currency (e.g., Euro, Pound, Yen)

2151. What is an introducing broker (IB) in the context of FCMs?

An IB is any person or entity that is registered, or required to be registered, with the CFTC as an IB under the CEA, except a person who registers pursuant to 4(f)(a)(2) of the CEA.

2152. Who is responsible for examining FCMs and IBs for compliance with AML/CFT laws and regulations?

The CFTC is responsible for examining FCMs and IBs for compliance with AML/CFT laws and regulations.

In addition, examinations may be conducted by the firm's self-regulatory organisation (SRO). The responsible SRO is based upon where the firm is registered and/or listed.

2153. What is a self-regulatory organisation (SRO)?

A self-regulatory organisation (SRO) is a nongovernment organisation that has the power to create and enforce industry regulations and standards under the supervision of a federal agency.

Examples include, but are not limited to, the following:

- National Futures Association (NFA)
- Chicago Mercantile Exchange (CME)
- New York Mercantile Exchange (NYMEX)

2154. When FCMs and IBs are members of more than one SRO, which one is responsible for oversight and examinations?

The CFTC designates a responsible SRO as the "designated examining authority" where multiple SROs are involved.

Key AML/CFT and Sanctions Requirements

2155. With which key AML/CFT and sanctions requirements are FCMs and IBs required to comply?

FCMs and IBs must comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)
- Establishment of a Customer Identification Program (CIP) (Section 326)
- Establishment of a customer due diligence program that obtains and identifies beneficial owners under select circumstances (Section 312, Beneficial Ownership Rule)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300) (where not subject to CTR filings)

- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- Complying with Special Measures (Section 311)
- Obtaining Foreign Bank Certifications (Section 319(b))
- Establishing an enhanced due diligence (EDD) program for correspondent account relationships, private banking relationships and politically exposed persons (PEPs) (Section 312)
- OFAC and other sanctions requirements

The AML/CFT requirements for FCMs and IBs are implemented under 31 C.F.R. 1026 – Rules for Futures Commission Merchants and Introducing Brokers in Commodities.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to FCMs and IBs is provided below.

2156. Are FCMs and IBs required to conduct a risk assessment?

FCMs and IBs are required to develop and maintain risk-based AML Programs. This means that they are expected to understand their risks and document their rationale for implementing controls for their AML Programs. There has to date not been the same degree of regulatory emphasis for FCMs and IBs on preparing formal AML/CFT and sanctions risk assessments as there has been for banking organisations; however, as a leading practice, many of the same risk assessment approaches used by banking organisations could apply to FCMs and IBs.

Additionally, any NBFI that is affiliated with a bank holding company will, by necessity, need to perform a risk assessment in order for the bank holding company to meet regulatory expectations for performing an enterprisewide risk assessment.

For further guidance, please refer to the Risk Assessments section.

2157. Which futures rules parallel the AML Program requirement of Section 352?

The NFA Compliance Rule 2-9(c) (FCM and IB Anti-Money Laundering Program) and related interpretive note outline the specific requirements for an AML Program as well as other BSA requirements such as the Customer Identification Program (CIP), suspicious activity report (SAR) and information sharing requirements.

2158. Are there special requirements for the AML compliance officer of FCMs and IBs?

The CFTC's general registration requirements state that persons who engage in the supervision, solicitation or conduct of futures business for member firms need to register. Being an AML

compliance officer may not, in and of itself, trigger the need to register, but other responsibilities could.

Generally, the individual responsible for overseeing the entire AML Program should be an officer of the futures firm.

2159. How do the obligations of the Customer Due Diligence Requirements for Financial Institutions (Beneficial Owner Rule), finalised in July 2016, impact obligations for FCMs and IBs?

FinCEN's Customer Due Diligence Requirements for Financial Institutions rule (Beneficial Ownership Rule), finalised in July 2016, requires financial institutions subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers.

FCMs and IBs are already required to obtain beneficial ownership information in the following situations, as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule expands the obligation to all legal entity customers, with limited exceptions. In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance on the Beneficial Ownership Rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

2160. Do FCMs and IBs have their own, unique SAR form?

No. FinCEN replaced industry-specific SAR forms with one new SAR for all covered financial institutions. As of April 1, 2013, FCMs and IBs must submit the new SAR (and other FinCEN Reports) electronically through the BSA E-Filing System.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2161. What obligations do FCMs and IBs have with respect to SAR filings?

FCMs and IBs are obligated to file SARs in good faith and maintain the confidentiality of the SAR filing and any information that would reveal the existence of a SAR (SAR information). In other words, no FCM and IB, and no director, officer, employee or agent of the institution who files a SAR, may notify any person (or their agent, such as their attorney) involved in the transaction that it has been reported.

2162. Are there exceptions to the SAR requirement for FCMs and IBs?

Yes. The SAR requirement for FCMs and IBs contains two exceptions from reporting violations that otherwise would be reported to various law enforcement authorities. The following activities are not required to be reported:

- A robbery or burglary that is reported by the FCM or IB to appropriate law enforcement authorities. (FCMs and IBs are required to report the robbery or burglary on Form 8-R, 8-T, U-5 or any other similar with the CFTC); and
- A violation otherwise required to be reported under the CEA (7 U.S.C. 1 *et seq*.), the regulations of the CFTC (17 C.F.R. chapter I), or the rules of any registered futures association or registered entity as those terms are defined in the CEA, 7 U.S.C. 21 and 7 U.S.C. 1a(29), by the FCM or IB or any of its officers, directors, employees, or associated persons, other than a violation of 17 C.F.R. 42.2, as long as such violation is appropriately reported to the CFTC or a registered futures association or registered entity.

2163. Are there exceptions to the SAR disclosure prohibition?

Provided that no person involved in the transaction is notified that the transaction has been reported, the SAR disclosure prohibition does not include disclosures of SAR information to the following:

- FinCEN
- Any federal, state or local law enforcement agency
- Any federal regulatory agency that examines the depository institution for compliance with the BSA
- Any state regulatory authority that examines the depository institution for compliance with state laws requiring compliance with the BSA

Guidance has also been provided by FinCEN on FCMs' and IBs' ability to share SAR information within their organisational structures to fulfil their duties under the BSA. FCMs and IBs may share SAR information with the following:

- Head office or controlling companies, whether domestic or foreign
- Domestic affiliates and subsidiaries that are also subject to SAR requirements

For further guidance, please refer to the Suspicious Activity Reports and Confidentiality sections.

2164. Can FCMs and IBs share SARs and SAR information with SROs?

To enable SROs to monitor and examine broker-dealers for compliance with AML/CFT laws and regulations, FinCEN issued a ruling allowing FCMs and IBs to share SAR and SAR information with their SROs, under certain circumstances.

For further guidance, please refer to 31 C.F.R. 1026.320 - Reports by Futures Commission Merchants and Introducing Brokers in Commodities of Suspicious Transactions.

2165. Are there instances in which an FCM or IB should notify regulators and law enforcement in advance of filing a SAR?

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including, but not limited to, ongoing money laundering schemes or detection of terrorist financing, FCMs and IBs should immediately notify regulators and law enforcement, even before the SAR is filed.

FinCEN and the SEC have both established hotlines, 1.866.556.3974 (FinCEN) and 1.202.551.SARS (SEC SAR Alert Message), for FCMs and IBs to expedite to law enforcement reports of suspicious transactions that may relate to recent terrorist activity against the United States.

2166. What are some of the statistics and trends in SAR filings for FCMs and IBs?

According to FinCEN, using 2016 as the frame of reference, of the 1.98 million SARs filed from January 1, 2016 through December 31, 2016, securities and futures firms (e.g., clearing brokers [securities], introducing brokers [securities], introducing brokers [commodities], futures commission merchants, investment companies, investment advisers, retail foreign exchange dealers, holding companies, subsidiaries of holding companies) filed over 19,000 SARs or 1 percent of all filings during this period. Highlights included:

- Sixteen percent of SARs were filed on activity taking place in California, 12 percent in Massachusetts, 11 percent in New York, and 10 percent in Rhode Island;
- Ninety percent of SARs were filed on customers, 7 percent on unknown/blank relationship types and 1 percent on individuals with no relationship with the securities and futures firm;
- Fifty-eight percent of SARs involved funds transfers; 34 percent involved stocks; 24 percent involved personal/business checks; 16 percent involved mutual funds; 15 percent involved penny stocks/microcap securities; and 5 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by securities and futures firms:
    - Other Suspicious Activities: 42 percent (included more than 5,000 cases related to identity theft; nearly 2,700 cases related to account takeover; over 2,600 cases related to embezzlement/theft/disappearance of funds; over 1,100 cases related to unauthorised electronic intrusion; over 1,400 cases related to elder financial exploitation; and 147 cases related to corruption [foreign and domestic]);
    - Fraud: 30 percent (included more than 11,800 cases related to wire transfer, ACH and check fraud) (separate from Mortgage Fraud which accounted for less than 0.1 percent);
    - Securities/Futures/Options: 8 percent (included more than 1,300 cases related to insider trading and over 1,200 cases related to market manipulation/wash trading);
    - Money Laundering: 13 percent;
    - Terrorism/Terrorist Financing: 0.04 percent (19 cases).

2167. What is "identity theft," and how can FCMs and IBs combat the rise in identity theft-related crime?

Identity theft is defined as fraud committed or attempted using the identifying information of another person without authority.

Some FCMs and IBs are required to implement an Identity Theft Prevention Program (ITPP) to identify, detect, prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. An ITPP requires the following four basic elements:

- Identification of relevant red flags (i.e., pattern, practice or specific activity that indicates the possible existence of identity theft);
- Implementation of a monitoring program to detect identity theft red flags;
- Establishment of appropriate responses to detected red flags to prevent and mitigate identity theft; and
- Written policies and procedures and periodic updates of the ITPP (e.g., changes to addresses as they relate to identity theft; changes in methods to detect, prevent or mitigate identity theft; changes in the types of accounts offered or maintained; changes in business arrangements, such as mergers, acquisitions, alliances, joint ventures, and service provider arrangements).

Additionally, FCMs and IBs must:

- Obtain approval of the initial ITPP by the board of directors, a committee of the board, or a designated employee at the level of senior management; the financial institution may determine whether ongoing changes to the ITPP require approval by the board of directors/committee/senior management;
- Involve the board of directors, a committee of the board, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the ITPP;
- Train relevant staff;
- Oversee service provider arrangements to ensure the activity of the service provider is conducted in accordance with the financial institution's ITPP; and
- Conduct periodic assessments to determine whether the financial institution offers or maintains covered accounts; the assessment should consider the types of accounts offered, the methods of account opening, the methods/channels provided to access accounts and its previous experiences with identity theft.

For further guidance, please refer to the Identity Theft and Identity Theft Prevention Program section.

2168. Are FCMs and IBs required to comply with OFAC regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on

OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2169. Do FCMs and IBs have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. FCMs and IBs can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyber attacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

The **U.S. Securities and Exchange Commission (SEC)** adopted multiple rules to address cybersecurity risks including, but not limited to, the following:

- Regulation Systems Compliance and Integrity (SCI)
- Regulation S-P
- Regulation SDR
- Regulation S-ID: Subpart C: Identity Theft Red Flags
- Exchange Act Rule 13n-6
- Exchange Act Rule 15c3-5
- Investment Company Act Rule 38-1
- Investment Advisers Act Rule 206(4)-7

The SEC published guidelines on cybersecurity preparedness:

- Conducting periodic assessments on vulnerabilities, internal and external threats, controls, impact of threats, effectiveness of cybersecurity governance structure that also addresses identity theft, data protection, fraud and business continuity;

- Developing a strategy designed to prevent, detect and respond to cybersecurity threats; and
- Implementing the cybersecurity strategy through written policies and procedures and training.

While public companies are required to report any incident that causes "material harm," they are not specifically required to disclose cybersecurity failures and risks. In 2011, the SEC published guidance, not rules, on the disclosure obligations relating to cybersecurity risks and cyber incidents. Public companies are expected to disclose cybersecurity risks and cyber incidents that could have a "material adverse effect on the business." With each publicised cyber attack or data breach, more pressure is being placed on the SEC to provide more clarity on previous guidance and issue rules requiring disclosures of cybersecurity risks and failures.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2170. Should FCMs and IBs address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the SEC settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber incident or through fines levied by regulatory authorities), FCMs and IBs can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2171. How long must FCMs and IBs retain records?

CFTC Regulation 1.31 requires FCMs and IBs to retain records for five years. CFTC Regulation 1.31 also specifies that the records must be stored in an "easily accessible place" in the first two years.

Some states, as well as international jurisdictions in which FCMs and IBs operate, may require longer retention periods.

Commodity Trading Advisers and Commodity Pool Operators

Definitions

2172. What is a commodity trading adviser (CTA)?

A CTA is a person who directs (i.e., is given decision-making authority over) account activities, client commodity futures and options accounts, and is registered or required to be registered as a CTA with the CFTC under the CEA. Generally, the CEA has defined a CTA as any person who is in the business of

directly or indirectly advising others as to the value or advisability of trading futures contracts or commodity options for compensation or profit.

2173. What is a commodity pool operator?

A commodity pool operator (CPO) is an investment trust, a syndicate or a similar form of enterprise operated for the purpose of trading commodity interests.

A CPO includes an investment trust, a syndicate or a similar type of business that solicits, accepts or receives from others funds, securities or property for trading in any commodity for future delivery on, or subject to the rules of, any contract market or derivatives transaction execution facility.

Key AML/CFT and Sanctions Requirements

2174. With which key AML/CFT and sanctions requirements are CTAs and CPOs required to comply?

CTAs and CPOs are required to comply with the following key AML/CFT and sanctions requirements:

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanctions requirements

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to CTAs and CPOs is provided below.

2175. Are CTAs and CPOs required to establish an AML Program?

No. At present, the AML Program requirement of the USA PATRIOT Act does not apply to CTAs and CPOs. In 2003, FinCEN issued a proposed rule which would have required CTAs and CPOs to establish AML Programs. The proposed rule was withdrawn in 2008. In its withdrawal notice, FinCEN said the primary reason for withdrawing the regulation was "passage of time." FinCEN further indicated that it would continue to consider whether it should impose AML Program requirements on CTAs and CPOs.

2176. Are CTAs and CPOs subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, CTAs and CPOs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2177. Are CTAs and CPOs subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. CTAs and CPOs are not subject to the CIP requirement and therefore are not required to identify beneficial owners. However, the Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future.

For further guidance, please refer to the Beneficial Owners section.

2178. Are CTAs and CPOs required to file CTRs?

No. Currently, CTAs and CPOs are not required to file Currency Transaction Reports (CTRs). CTAs and CPOs are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2179. Are CTAs and CPOs required to file SARs?

While CTAs and CPOs are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of a SAR for suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious. For further guidance, please refer to the Form 8300 section.

2180. Are CTAs and CPOs required to comply with the information-sharing requirement of Section 314 of the USA PATRIOT Act?

No. Only those institutions required to establish an AML Program are obligated to comply with the information-sharing requirement (e.g., 314(a)). For further guidance on information sharing, please refer to Section 314 – Cooperative Efforts to Deter Money Laundering.

2181. Are CTAs and CPOs required to comply with OFAC regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2182. Do CTAs and CPOs have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health

or financial stability of the United States. CTAs and CPOs can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Mutual funds can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyberattacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

The **U.S. Securities and Exchange Commission (SEC)** adopted multiple rules to address cybersecurity risks including, but not limited to, the following:

- Regulation Systems Compliance and Integrity (SCI)
- Regulation S-P
- Regulation SDR
- Regulation S-ID: Subpart C: Identity Theft Red Flags
- Exchange Act Rule 13n-6
- Exchange Act Rule 15c3-5
- Investment Company Act Rule 38-1
- Investment Advisers Act Rule 206(4)-7

The SEC published guidelines on cybersecurity preparedness:

- Conducting periodic assessments on vulnerabilities, internal and external threats, controls, impact of threats, effectiveness of cybersecurity governance structure that also addresses identity theft, data protection, fraud and business continuity;
- Developing a strategy designed to prevent, detect and respond to cybersecurity threats; and
- Implementing the cybersecurity strategy through written policies and procedures and training.

While public companies are required to report any incident that causes "material harm," they are not specifically required to disclose cybersecurity failures and risks. In 2011, the SEC published guidance, not rules, on the disclosure obligations relating to cybersecurity risks and cyber incidents. Public companies are expected to disclose cybersecurity risks and cyber incidents that could have a "material adverse effect on the business." With each publicised cyber attack or data breach, more pressure is being placed on the SEC to provide more clarity on previous guidance and issue rules requiring disclosures of cybersecurity risks and failures.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2183. Should CTAs and CPOs address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the SEC settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though there financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber incident or through fines levied by regulatory authorities), CTAs and CPOs can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2184. Who is responsible for examining CTAs and CPOs for compliance with AML/CFT laws and regulations?

The CFTC is responsible for examining CTAs and CPOs for compliance with AML/CFT laws and regulations. In addition, examinations may be conducted by the firm's SRO. The responsible SRO is based upon where the firm is registered and/or listed (e.g., New York Stock Exchange [NYSE], National Futures Association [NFA]).

Mutual Funds

Definitions

2185. What is a mutual fund?

A mutual fund is an open-ended investment company that is registered or required to register with the U.S. Securities and Exchange Commission (SEC) under Section 5 of the Investment Company Act.

2186. Who is responsible for examining mutual funds for compliance with AML/CFT laws and regulations?

The U.S. Department of the Treasury has designated the SEC as responsible for examining mutual funds for compliance with AML/CFT laws and regulations.

2187. What key AML/CFT guidance has been issued related to mutual funds?

The following are examples of key guidance that has been issued related to or discussing mutual funds:

- Nonbank Financial Institutions – Overview within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- Anti-Money Laundering (AML) Source Tool for Mutual Funds (2012) by the Securities and Exchange Commission (SEC)
- Final Rule: Amendment to the Bank Secrecy Act Regulations; Defining Mutual Funds as Financial Institutions (2010) by FinCEN (Addressing requirement to file Currency Transaction Reports [CTRs])
- Frequently Asked Questions: Suspicious Activity Reporting Requirements for Mutual Funds (2006) by FinCEN
- Sharing Suspicious Activity Reports by Securities Broker-Dealers, Mutual Funds, Futures Commission Merchants, and Introducing Brokers in Commodities with Certain U.S. Affiliates (2010) by FinCEN
- Assessing the Impact of Amendments to the Regulations Defining Mutual Funds as Financial Institutions (2010) by FinCEN
- Anti-Money Laundering Guidance for Mutual Funds and Other Pooled Investment Vehicles (2012) by the Wolfsberg Group
- Foreign Asset Control Regulations for the Securities Industry (2004) by OFAC
- Opening Securities and Futures Accounts from an OFAC Perspective (2008) by OFAC
- Risk Factors for OFAC Compliance in the Securities Industry (2008) by OFAC

In addition, the website of the Investment Company Institute (www.ici.org), the national association of U.S. investment companies, includes viewpoints and comment letters on money laundering issues of interest to the mutual funds community.

Key AML/CFT and Sanctions Requirements

2188. With which key AML/CFT and sanctions requirements are mutual funds required to comply?

Mutual funds must comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)
- Establishment of a Customer Identification Program (CIP) (Section 326)
- Establishment of a customer due diligence program that identifies beneficial owners under select circumstances (Section 312, Beneficial Ownership Rule)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300) (only where not required to file a CTR)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- Complying with Special Measures (Section 311)
- Obtaining Foreign Bank Certifications (Section 319(b))
- Establishment of an enhanced due diligence (EDD) program for customers deemed to be of higher risk, correspondent account relationships, private banking relationships and politically exposed persons (PEPs) (Section 312)
- OFAC and other sanctions requirements

The AML/CFT requirements for mutual funds are implemented under 31 C.F.R. 1024 – Rules for Mutual Funds.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to mutual funds is provided below.

2189. Are mutual funds required to conduct a risk assessment?

Mutual funds are required to develop and maintain risk-based AML Programs. This means that they are expected to understand their risks and document their rationale for implementing controls for their AML Programs. There has to date not been the same degree of regulatory emphasis for mutual funds on preparing formal AML/CFT and sanctions risk assessments as there has been for banking organisations; however, as a leading practice, many of the same risk assessment approaches used by banking organisations could apply to mutual funds.

Additionally, any NBFI that is affiliated with a bank holding company will, by necessity, need to perform a risk assessment in order for the bank holding company to meet regulatory expectations for performing an enterprisewide risk assessment.

For further guidance, please refer to the Risk Assessments section.

2190. How do the obligations of the Customer Due Diligence Requirements for Financial Institutions rule (Beneficial Ownership Rule), finalised in July 2016, impact obligations for mutual funds?

FinCEN's Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule) finalised in July 2016, requires financial institutions subject to Customer Identification Program (CIP) requirements (e.g., depository institutions, securities broker-dealers, mutual funds, futures commission merchants [FCMs] and introducing brokers [IBs]) to identify and verify the identity of beneficial owners with 25 percent or greater ownership/control of legal entity customers.

Mutual funds are already required to obtain beneficial ownership information in the following situations, as outlined in Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts:

- Private banking accounts
- Correspondent accounts for certain foreign financial institutions

The Beneficial Ownership Rule expands the obligation to all legal entity customers, with limited exceptions.

The Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future.

For further guidance on the Beneficial Ownership Rule, please refer to the Beneficial Owners section. For further guidance on due diligence requirements for private banking and correspondent banking customers, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Private Banking and Correspondent Banking.

2191. Are mutual funds required to file CTRs?

Yes. As of April 2010, mutual funds are required to file CTRs. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2192. Can mutual funds grant CTR exemptions?

No. Only depository institutions (e.g., banks, savings associations, thrift institutions, credit unions) can grant exemptions. For further guidance on exemptions, please refer to the CTR Exemptions and the Designation of Exempt Persons Form section.

2193. Do mutual funds have their own, unique SAR form?

No. FinCEN replaced industry-specific SAR forms with one new SAR for all covered financial institutions. As of April 1, 2013, mutual funds must submit the new SAR (and other FinCEN reports) electronically through the BSA E-Filing System.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2194. Is it permissible for a broker-dealer, other financial institution or servicing provider that is involved in the same transaction(s) with one or more mutual funds to file a joint SAR on behalf of the mutual fund(s)?

Yes. One SAR is sufficient to report the same suspicious activity. Under the suspicious activity reporting requirement for mutual funds, joint SAR filings are permissible so long as the report contains all relevant facts, including the identification in the narrative section of all mutual funds on whose behalf the report is being filed.

It is still the responsibility of all firms involved to confirm that at least one SAR was filed on the suspicious activity, regardless of which firm actually filed the report.

2195. Does the joint filing of a SAR violate the confidentiality requirement of SAR filings?

No. The suspicious activity reporting requirement specifically permits a mutual fund to share information pertaining to a suspicious transaction with any other mutual fund or financial institution involved in the transaction provided that such mutual fund or financial institution is not expected to be the subject of the report.

2196. Is a mutual fund permitted to inform an investment adviser who is in control of the fund about a SAR filing?

Yes. A mutual fund may inform the investment adviser who controls the fund, whether domestic or foreign, about a SAR filing. Additionally, the SAR can be shared with the parent company/companies of the investment adviser.

In all exchanges of sensitive information, particularly when SARs are involved, mutual funds should ensure that the proper policies, procedures and controls are in place to protect the confidentiality of the exchanged information.

2197. Are there instances in which a mutual fund should notify regulators and law enforcement in advance of filing a SAR?

Whenever violations require immediate attention, such as when a reportable transaction is ongoing, including, but not limited to, ongoing money laundering schemes or detection of terrorist financing, mutual funds should immediately notify regulators and law enforcement, even before the SAR is filed.

FinCEN and the SEC have both established hotlines, 1.866.556.3974 (FinCEN) and 1.202.551.SARS (SEC SAR Alert Message), for mutual funds to expedite to law enforcement reports of suspicious transactions that may relate to recent terrorist activity against the United States.

2198. What are some of the statistics and trends in SAR filings for mutual funds?

According to FinCEN, using 2016 as the frame of reference, of the 1.98 million SARs filed from January 1, 2016 through December 31, 2016, securities and futures firms (e.g., clearing brokers [securities], introducing brokers [securities], introducing brokers [commodities], futures commission merchants, investment companies, investment advisers, retail foreign exchange dealers, holding companies, subsidiaries of holding companies) filed over 19,000 SARs or 1 percent of all filings during this period. Highlights included:

- Sixteen percent of SARs were filed on activity taking place in California, 12 percent in Massachusetts, 11 percent in New York, and 10 percent in Rhode Island;
- Ninety percent of SARs were filed on customers, 7 percent on unknown/blank relationship types and 1 percent on individuals with no relationship with the securities and futures firm;
- Fifty-eight percent of SARs involved funds transfers; 34 percent involved stocks; 24 percent involved personal/business checks; 16 percent involved mutual funds; 15 percent involved penny stocks/microcap securities; and 5 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by securities and futures firms:
    - Other Suspicious Activities: 42 percent (included more than 5,000 cases related to identity theft; nearly 2,700 cases related to account takeover; over 2,600 cases related to embezzlement/theft/disappearance of funds; over 1,100 cases related to unauthorised electronic intrusion; over 1,400 cases related to elder financial exploitation; and 147 cases related to corruption [foreign and domestic]);
    - Fraud: 30 percent (included more than 11,800 cases related to wire transfer, ACH and check fraud) (separate from Mortgage Fraud which accounted for less than 0.1 percent);
    - Securities/Futures/Options: 8 percent (included more than 1,300 cases related to insider trading and over 1,200 cases related to market manipulation/wash trading);
    - Money Laundering: 13 percent;
    - Terrorism/Terrorist Financing: 0.04 percent (19 cases).

2199. Are mutual funds required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2200. Do mutual funds have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Mutual funds can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyberattacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

The **U.S. Securities and Exchange Commission (SEC)** adopted multiple rules to address cybersecurity risks including, but not limited to, the following:

- Regulation Systems Compliance and Integrity (SCI)
- Regulation S-P
- Regulation SDR
- Regulation S-ID: Subpart C: Identity Theft Red Flags
- Exchange Act Rule 13n-6
- Exchange Act Rule 15c3-5
- Investment Company Act Rule 38-1
- Investment Advisers Act Rule 206(4)-7

The SEC published guidelines on cybersecurity preparedness:

- Conducting periodic assessments on vulnerabilities, internal and external threats, controls, impact of threats, effectiveness of cybersecurity governance structure that also addresses identity theft, data protection, fraud and business continuity;
- Developing a strategy designed to prevent, detect and respond to cybersecurity threats; and
- Implementing the cybersecurity strategy through written policies and procedures and training.

While public companies are required to report any incident that causes "material harm," they are not specifically required to disclose cybersecurity failures and risks. In 2011, the SEC published guidance, not rules, on the disclosure obligations relating to cybersecurity risks and cyber incidents. Public companies are expected to disclose cybersecurity risks and cyber incidents that could have a "material adverse effect on the business." With each publicised cyber attack or data breach, more pressure is being placed on the SEC to provide more clarity on previous guidance and issue rules requiring disclosures of cybersecurity risks and failures.

Additionally, some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2201. Should mutual funds address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the SEC settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the PII of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber incident or through fines levied by regulatory authorities), mutual funds can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

Registered Investment Advisers and Unregistered Investment Companies

Definitions

2202. What is an investment adviser?

In September 2015, FinCEN issued a notice of proposed rulemaking for Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Registered Investment Advisers, with the following definition for investment adviser:

"[A]ny person who is registered or required to register with the [Securities and Exchange Commission] (SEC) under section 203 of the Investment Advisers Act of 1940."

The Investment Advisor Act of 1940 defines an "investment adviser" as "any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities."

FinCEN's proposed definition includes both primary advisers and subadvisers and does not distinguish proposed AML/CFT obligations between the two. A "primary adviser" contracts directly with the client and a "subadviser" has contractual privity with the primary adviser.

2203. Are there any exemptions from the term "investment adviser"?

Yes. The term "investment adviser" does not include the following:

- A bank, or any bank holding company (BHC) as defined in the Bank Holding Company Act of 1956, which is not an investment company, except that the term "investment adviser" includes any bank or bank holding company to the extent that such bank or bank holding company serves or acts as an investment adviser to a registered investment company, but if, in the case of a bank, such services or actions are performed through a separately identifiable department or division, the department or division, and not the bank itself, shall be deemed to be the investment adviser;
- Any lawyer, accountant, engineer, or teacher whose performance of such services is solely incidental to the practice of his profession;
- Any broker or dealer whose performance of such services is solely incidental to the conduct of his business as a broker or dealer and who receives no special compensation therefore;
- The publisher of any bona fide newspaper, news magazine or business or financial publication of general and regular circulation;
- Any person whose advice, analyses, or reports relate to no securities other than securities which are direct obligations of or obligations guaranteed as to principal or interest by the United States, or securities issued or guaranteed by corporations in which the United States has a direct or indirect interest which shall have been designated by the Secretary of the Treasury, pursuant to section 3(a)(12) of the Securities Exchange Act of 1934, as exempted securities for the purposes of that Act;

- Any nationally recognised statistical rating organisation, as that term is defined in section 3(a)(62) of the Securities Exchange Act of 1934, unless such organisation engages in issuing recommendations as to purchasing, selling, or holding securities or in managing assets, consisting in whole or in part of securities, on behalf of others;
- Any family office, as defined by rule, regulation, or order of the Commission, in accordance with the purposes of this title; or
- Such other persons not within the intent of this paragraph, as the Commission may designate by rules and regulations or order.

2204. What is the role of the investment adviser in the fight against money laundering and terrorist financing?

Investment advisers play an important role in combating money laundering and terrorist financing because of their transactional knowledge. An investment adviser may be the only one with a complete understanding of the source of invested assets and the nature of the client's investment objectives and, therefore, is in a unique position to monitor customer transactions for suspicious activity.

2205. What is an investment company and are investment company AML/CFT obligations different from those of investment advisers?

According to the Investment Company Act of 1940, an "investment company" is defined as any issuer which:

- Is or holds itself out as being engaged primarily, or proposes to engage primarily, in the business of investing, reinvesting, or trading in securities;
- Is engaged or proposes to engage in the business of issuing face-amount certificates of the instalment type, or has been engaged in such business and has any such certificate outstanding; or
- Is engaged or proposes to engage in the business of investing, reinvesting, owning, holding, or trading in securities, and owns or proposes to acquire investment securities having a value exceeding 40 per centum of the value of such issuer's total assets (exclusive of government securities and cash items) on an unconsolidated basis.

In 2011, the Dodd-Frank Wall Street Reform and Consumer Protection Act (DFA) amended many financial regulations, including the Investment Advisor Act of 1940 and the Investment Company Act of 1940, eliminating previous exemptions (e.g., based on number of clients), requiring many previously unregistered investment companies (e.g., hedge funds, private equity, private investment funds) to register with the SEC.

Because of this reform, FinCEN issued a single rule to cover both investment advisers and the formerly "unregistered" investment company.

Key AML/CFT and Sanctions Requirements

2206. With which key AML/CFT laws and regulations are registered investment advisers required to comply?

Registered investment advisers must comply with the following AML/CFT requirements:

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanctions requirements

For additional guidance on the various AML/CFT laws and regulations, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to investment advisers is provided below.

2207. Are registered investment advisers required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

No. At present, the AML Program requirement of the USA PATRIOT Act does not apply to registered investment advisers. In 2002, 2003 and 2015, FinCEN issued proposed rules which would have required certain types of investment advisers and unregistered investment companies to establish AML Programs. The 2002/2003 proposed rules were withdrawn in 2008. In its withdrawal notice, FinCEN stated that the primary reason for withdrawing the regulation was "passage of time," and indicated that it would continue to consider whether it should impose AML Program requirements on investment advisers and unregistered investment companies taking into consideration the significant changes in the regulatory framework due to the passage of the Dodd-Frank Act. In 2015, FinCEN issued proposed AML Program and Suspicious Activity Report Filing Requirements for Registered Investment advisers, which covered AML/CFT obligations for unregistered investment companies that are now required to register with the SEC pursuant to the Dodd-Frank Act.

Even without further FinCEN action, registered investment advisers are still subject to the AML/CFT and sanctions requirements as noted above.

2208. Are registered investment advisers subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, registered investment advisers are not subject to the Customer Identification Program (CIP) requirement. In a 2015 proposed rule, which is still pending, FinCEN indicated that a joint rulemaking with the SEC would be issued with regard to CIP obligations of registered investment advisers. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2209. Are registered investment advisers subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Registered investment advisers are not currently subject to the CIP requirement and therefore are not required to identify beneficial owners. In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance, please refer to the Beneficial Owners section.

2210. Are registered investment advisers required to file CTRs?

No. Currently, registered investment advisers are not required to file Currency Transaction Reports (CTRs). Registered investment advisers are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. In a 2015 proposed rule, which is still pending, FinCEN indicated that if published in its current form, registered investment advisers would be required to file CTRs in lieu of Form 8300. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2211. Are registered investment advisers required to file SARs?

Currently, no; however, in September 2015, FinCEN proposed a rule requiring registered investment advisers file SARs in addition to establishing an AML Program. While registered investment advisers are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of a SAR for suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

For further guidance on SARs, please refer to the Suspicious Activity Reports section.

2212. Are registered investment advisers required to comply with the information-sharing requirement of Section 314 of the USA PATRIOT Act?

No. Only those institutions required to establish an AML Program are obligated to comply with the information-sharing requirement (e.g., 314(a)).

2213. Are registered investment advisers required to comply with the Funds Transfer Recordkeeping Requirement?

No. Registered investment advisers are not currently required to comply with the Funds Transfer Recordkeeping Requirement. In a 2015 proposed rule, which is still pending, FinCEN indicated that if published in its current form, registered investment advisers would be required to comply with AML/CFT recordkeeping requirements such as the Funds Transfer Recordkeeping Requirement of the BSA. For a listing of financial institutions required to comply with the Funds Transfer Recordkeeping

Requirement at the time of this publication, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.

2214. Are registered investment advisers required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2215. Do registered investment advisers have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Investment advisers and unregistered investment companies can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

The **U.S. Securities and Exchange Commission (SEC)** adopted multiple rules to address cybersecurity risks including, but not limited to, the following:

- Regulation Systems Compliance and Integrity (SCI)
- Regulation S-P
- Regulation SDR
- Regulation S-ID: Subpart C: Identity Theft Red Flags
- Exchange Act Rule 13n-6
- Exchange Act Rule 15c3-5
- Investment Company Act Rule 38-1
- Investment Advisers Act Rule 206(4)-7

The SEC published guidelines on cybersecurity preparedness:

- Conducting periodic assessments on vulnerabilities, internal and external threats, controls, impact of threats, effectiveness of cybersecurity governance structure that also addresses identity theft, data protection, fraud and business continuity;
- Developing a strategy designed to prevent, detect and respond to cybersecurity threats; and
- Implementing the cybersecurity strategy through written policies and procedures and training.

While public companies are required to report any incident that causes "material harm," they are not specifically required to disclose cybersecurity failures and risks. In 2011, the SEC published guidance, not rules, on the disclosure obligations relating to cybersecurity risks and cyber incidents. Public companies are expected to disclose cybersecurity risks and cyber incidents that could have a "material adverse effect on the business." With each publicised cyber attack or data breach, more pressure is being placed on the SEC to provide more clarity on previous guidance and issue rules requiring disclosures of cybersecurity risks and failures.

Additionally, some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2216. Should registered investment advisers address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the SEC settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber incident or through fines levied by regulatory authorities), registered investment advisers can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

Insurance Companies

Definitions

2217. Which types of insurance companies are required to maintain an AML Program pursuant to Section 352 of the USA PATRIOT Act?

An insurance company or insurer that is engaged within the United States as a business in the issuing or underwriting of a covered product is required to maintain an AML Program.

2218. How is the term "covered product" defined?

Covered products are defined as:

- Permanent life insurance policies, other than group life insurance policies
- Annuity contracts, other than group annuity contracts
- Any other insurance products that have cash value or investment features

2219. What are the heightened money laundering and terrorist financing risks of insurance companies?

The heightened risk in the insurance industry lies in how certain insurance products exhibit one or more of the following:

- Complexity (e.g., the involvement of multiple parties: guarantors, signatories, beneficiaries, professional service providers, agents/brokers who may manipulate the transaction(s));
- Ability to transfer value without the knowledge of the issuer;
- Payments made in cash or by third parties;
- High frequency of international transactions; and
- Historical susceptibility to abuse by criminals.

2220. Are insurance agents and brokers required to maintain an AML Program?

While insurance agents and brokers are not required to maintain an AML Program, it is critical that agents and brokers be incorporated into the AML Program of the insurance company, as they are most able to know the sources of investment assets, and the nature of the clients and their intentions for purchasing products.

2221. How do U.S. AML/CFT requirements for insurance companies correspond to the FATF Recommendations?

FATF Recommendation 10 – Customer Due Diligence suggests financial institutions offering insurance products and services (including intermediaries such as agents and brokers) implement measures to guard against money laundering and terrorist financing (e.g., conduct due diligence on beneficiaries of life or other investment-related insurance business). Simplified measures can be

applied toward low-risk insurance products (e.g., life insurance policies with annual premiums less than US/EUR 1,000, single premiums of less than US/EUR 2,500).

While U.S. AML/CFT requirements are narrower in scope, covered U.S. insurance companies are required to establish AML Programs, report potentially suspicious activities and comply with other BSA requirements as detailed further below.

2222. Have international standards been developed to supervise the insurance sector?

Yes. In 2011, the International Association of Insurance Supervisors established 26 global standards for supervising the insurance sector, known as Insurance Core Principles (ICPs). These standards cover a range of topics including AML/CFT, anti-corruption, fraud, governance and intermediaries (e.g., agents, brokers).

2223. What guidance has been issued related to insurance companies and covered products?

The following are examples of key guidance that has been issued:

- Insurance – Overview within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- FATF Recommendation 10 – Customer Due Diligence (2012) by FATF
- Frequently Asked Questions: Customer Identification Programs and Banks Serving as Insurance Agents (2006) by FinCEN
- Insurance Industry Suspicious Activity Reporting: An Assessment of Suspicious Activity Report Filings (2010) by the Financial Crimes Enforcement Network (FinCEN)
- Frequently Asked Questions from the Insurance Industry (2012) by the Office of Foreign Assets Control (OFAC)
- Risk-Based Approach for the Life Insurance Sector (2009) by the Financial Action Task Force (FATF)
- Guidance Paper on Anti-Money Laundering and Combating the Financing of Terrorism (2004) by the International Association of Insurance Supervisors (IAIS)
- Anti-Money Laundering Guidance Notes (2003) by the IAIS

Key AML/CFT and Sanctions Requirements

2224. With which key AML/CFT and sanctions requirements are insurance companies required to comply?

Insurance companies must comply with the following key AML/CFT requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, and

conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- OFAC and other sanctions requirements

The AML/CFT requirements for insurance companies are implemented under 31 C.F.R. 1025 – Rules for Insurance Companies.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to insurance companies is provided below.

2225. Are insurance companies subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, insurance companies are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2226. Are insurance companies subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Insurance companies are not subject to the CIP requirement and therefore are not required to identify beneficial owners. In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance, please refer to the sections Beneficial Owners and Section 352 – AML Program.

2227. Are insurance companies required to file CTRs?

No. Currently, insurance companies are not subject to filing Currency Transaction Reports (CTRs). Insurance companies are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300, please refer to the Currency Transaction Reports and Form 8300 sections.

2228. Do insurance companies have their own unique SAR form?

Beginning March 29, 2012, FinCEN replaced industry-specific SAR forms with a single form that must be submitted electronically. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2229. What are some of the statistics and trends in SAR filings for insurance companies?

According to FinCEN, out of 1.98 million SAR filings from January 1, 2016 through December 31, 2016, insurance companies filed nearly 2,400 SARs or 0.1 percent of all filings during this period:

- Forty-six percent of SARs were filed on activity taking place in New York and Ohio; 42 states (and territories) filed fewer than 10 SARs; 19 did not file SARs;
- Sixty-two percent of SARs were filed on customers; 14 percent on individuals with no relationship with the insurance company; 11 percent on "other" relationship types; 6 percent were filed on unknown/blank relationship types; and 5 percent on agents;
- Ninety-five percent of SARs involved insurance/annuity products; 37 percent involved money orders; 30 percent involved personal/business checks; 19 percent involved funds transfers; 6 percent involved bank/cashier's checks; and 5 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by insurance companies:
    - Other Suspicious Activities: 40 percent (involved nearly 700 cases related to "transaction with no apparent economic, business or lawful purpose" and "little or no concern for product performance penalties, fees or tax consequences"; over 170 cases related to identity theft; over 200 cases related to elder financial abuse; 32 cases related to unauthorised electronic intrusion; and 11 cases related to corruption [domestic and foreign]);
    - Money Laundering: 24 percent;
    - Structuring: 18 percent;
    - Insurance: 8 percent (included more than 430 cases related to "excessive insurance," "excessive or unusual cash borrowing against policy/annuity," "proceeds related to unrelated third party," "suspicious life settlement sales insurance," "suspicious termination of policy or contract" and "unclear or no insurable interest");
    - Fraud: 7 percent (separate from Mortgage Fraud which accounted for less than 0.1 percent);
    - Terrorism/Terrorist Financing: Less than 0.1 percent (4 cases).

2230. How do insurance companies submit BSA reports to FinCEN?

Beginning July 1, 2012, insurance companies must submit BSA reports through the BSA E-Filing System, an internet-based e-filing system developed by FinCEN to enable financial institutions to file BSA reports electronically.

2231. Are there exceptions to the suspicious activity reporting requirements for insurance companies?

Yes. Insurance companies are only required to file SARs with respect to suspicious transactions involving covered products. They are not required to report submissions involving false or fraudulent information to obtain a policy or make a claim, unless the company believes the activity relates to money laundering or terrorist financing.

2232. Which SAR filing requirements apply to an insurance company that is also registered as a broker-dealer?

Insurance companies registered with the SEC as broker-dealers are subject to the SAR filing requirements of broker-dealers and, therefore, are not obligated to file under the insurance company requirements. As registered broker-dealers, insurance companies are subject to additional AML/CFT requirements beyond those of an insurance company.

2233. Are there red flags for detecting potentially suspicious activity for insurance companies?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments, insurance) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags and Insurance Products Red Flags sections.

2234. When banks market insurance products on behalf of insurance companies, who is responsible for conducting due diligence and monitoring for potentially suspicious activities of insurance products?

The manner in which the insurance products are offered affects the AML/CFT responsibilities.

- **Co-Branded Arrangements** – AML/CFT responsibilities for completing customer due diligence (CDD) and suspicious activity monitoring and reporting can vary. Financial institutions should clearly outline each party's contractual responsibilities and ensure compliance by all parties.
- **Dual-Employee Arrangements** – When the dual employee is providing investment products and services from the insurance company, the insurance company is responsible for monitoring the registered representative's compliance with applicable securities laws and AML/CFT regulations. When the dual employee is providing products or services from the financial institution, responsibility for monitoring the employee's performance and compliance with AML/CFT requirements falls on the financial institution.
- **Third-Party Networking Arrangement** – The insurance company assumes all AML/CFT responsibilities.
- **Proprietary Insurance Products** – The financial institution offering the proprietary insurance products assumes all AML/CFT responsibilities.

2235. Are insurance companies required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2236. Do insurance companies have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Insurance companies can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyberattacks to FinCEN via its hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

In 2015, the National Association of Insurance Commissioners (NAIC) issued "Principles for Effective Cybersecurity: Insurance Regulatory Guidance" which was derived from "Principles for Effective Cybersecurity Regulatory Guidance" by the Securities Industry and Financial Markets Association (SIFMA). The NAIC guidance lists 12 principles to assist state insurance regulators develop uniform standards. Topics covered include, but are not limited to, the following:

- Safeguarding of personally identifiable consumer information including by third parties and service providers;
- Risk-based, flexible, scalable regulatory guidance on cybersecurity consistent with national efforts (e.g., National Institute of Standards and Technology [NIST]);

- Reporting of audit findings that present a material risk to the insurer to the board of directors or appropriate committee;
- Participation in information sharing with other insurers to stay informed of emerging risks, threats as well as threat intelligence analysis and sharing; and
- Periodic training for employees and other third parties on cybersecurity issues.

Additionally, some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2237. Should insurance companies address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the PII of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), insurance companies can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2238. What is the "Terrorism Risk Insurance Program" administered by the U.S. Treasury Department?

The Terrorism Risk Insurance Act of 2002 (TRIA) (amended by the Terrorism Risk Insurance Extension Act of 2005 (TRIEA) and the Terrorism Risk Insurance Program Reauthorisation Act of 2007 (TRIPRA)) created the Terrorism Risk Insurance Program (TRIP), a temporary federal program administered by the U.S. Treasury Department to stabilise the private property and casualty insurance market as it relates to certified terrorist attacks. TRIP provides billions of government dollars to cover payouts in the event a target (e.g., airport, stadium, high-rise building) is damaged by a terrorist attack.

All entities meeting the definition of an insurer are required to participate in TRIP and offer property and casualty insurance against terrorist attacks.

2239. Who is responsible for examining insurance companies for compliance with AML/CFT laws and regulations?

The Internal Revenue Service (IRS) is responsible for examining insurance companies for compliance with AML/CFT laws and regulations. As stated above, if the insurance company is registered as a broker-dealer, then the SEC and applicable SRO would be responsible for examining the insurance company for compliance with AML/CFT laws and regulations.

2240. How does FinCEN interact with state insurance regulators?

FinCEN has entered into individual memoranda of understanding (MOUs) with several state insurance regulators to enhance the level of cooperation in the fight against money laundering, fraud and other financial crimes. State insurance regulators have agreed to incorporate AML/CFT compliance reviews into their examinations of insurance companies. The MOUs also enable FinCEN and state insurance regulators to share supervisory and related information relevant to assessing risks and compliance with applicable AML/CFT laws and regulations.

Casinos and Card Clubs

Definitions

2241. What is a casino?

A casino or gambling casino is a business licensed or authorised to do business as such in the United States, whether under the laws of a state or of a territory or insular possession of the United States, or under the Indian Gaming Regulatory Act or other federal, state or tribal law or arrangement affecting Indian lands. It includes casinos that operate on the assumption that no such authorisation is required for operation on Indian lands. The term includes the principal headquarters and every domestic branch or place of business of the casino.

2242. What is a card club?

A card club is a gaming club, card room, gaming room or similar gaming establishment that is licensed or authorised to do business as such in the United States, whether under the laws of a state, territory or

insular possession of the United States, or of a political subdivision of any of the foregoing, or under the Indian Gaming Regulatory Act or other federal, state or tribal law or arrangement affecting Indian lands. It includes establishments that operate on the assumption that no such authorisation is required for operation on Indian lands for establishments of such type. The term includes the principal headquarters and every domestic branch or place of business of the establishment.

2243. Which types of casinos and card clubs are required to maintain an AML Program pursuant to Section 352 of the USA PATRIOT Act?

Casinos and card clubs that have a gross annual gaming revenue (GAGR) threshold in excess of US$1 million are required to maintain an AML Program.

2244. What types of business activities should be included when calculating the US$1 million gaming threshold?

Only customer gaming activity should be included in the calculation of gross annual gaming revenue (e.g., per table fees, per game fees). This does not include nongaming activity such as shops, restaurants, entertainment or hotels.

2245. Which types of gaming activities may qualify an institution as a casino or card club subject to the AML Program requirement of Section 352 of the USA PATRIOT Act?

The following types of gaming activities may qualify an institution as a casino or card club required to maintain an AML Program:

- Racino
- Race book or sports pool operator
- Off-track betting
- Greyhound racing clubs that generate in excess of US$1 million from poker tables
- Tribal gaming offering slot or table games

In some instances, qualification as a casino is dependent on whether an institution is licensed or authorised by state law.

2246. How is the term “racino” defined for casinos and card clubs?

The term “racino” has not yet been clearly defined for casinos and card clubs. Generally, the term “racino” refers to horse racetracks that may be authorised under state law to engage in or offer a variety of collateral gaming operations, including slot machines, video lottery terminals, video poker or card clubs.

2247. How is the term “greyhound racing club” defined for casinos and card clubs?

The term “greyhound racing club” is defined as a gaming establishment that offers the sport of racing greyhounds, in which trained dogs chase an artificial hare or rabbit around a track until they arrive at a finish line. Such clubs that offer table games that generate gross annual gaming revenue in excess of

US$1 million from poker tables are duly licensed or authorised by state or local government to do business as a gaming club or gaming room or similar establishment, and therefore, would be required to comply with AML/CFT requirements for casinos and card clubs.

2248. How is the term "business day" defined for casinos and card clubs?

For casinos, the term "business day" is the gaming day by which they keep their books and records for business, accounting and tax purposes.

2249. How is the term "customer" defined for casinos and card clubs?

The term "customer" is defined for casinos and card clubs as a person involved in a currency transaction with a casino, whether or not that person participates or intends to participate in the gaming activities offered by the casino or card club.

2250. How do the U.S. AML/CFT requirements for casinos and card clubs correspond to FATF Recommendations?

FATF addresses casinos in the following Recommendations:

- **Recommendation 22 – DNFBPs: Customer Due Diligence** and **Recommendation 23 – DNFBPs: Other Measures** suggests casinos implement risk-based measures (e.g., customer due diligence, suspicious activity reporting) to guard against money laundering and terrorist financing. For example, FATF suggests a threshold of US/EUR 3,000 on transactions executed by customers to trigger customer due diligence measures.
- **Recommendation 28 – Regulation and Supervision of DNFBPs** suggests casinos be subject to licensing requirements, AML/CFT regulations and oversight by a competent authority.

While U.S. AML/CFT requirements are narrower in scope, covered casinos and card clubs are required to establish AML Programs, report suspicious activity through Suspicious Activity Reports (SARs) and comply with other AML/CFT requirements as detailed below.

For further guidance on international standards, please refer to the Financial Action Task Force section.

2251. What AML/CFT guidance has been issued related to casinos?

The following key guidance has been issued related to casinos and card clubs:

- **Nonbank Financial Institutions – Overview** (2010) within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- **FATF Recommendation 22 – DNFBPs: Customer Due Diligence, Recommendation 23 – DNFBPs: Other Measures and Recommendation 28 – Regulation and Supervision of DNFBPs** by the Financial Action Task Force (FATF)
- **Frequently Asked Questions Casino Recordkeeping, Reporting, and Compliance Program Requirements** (2012) by FinCEN

- **Suspicious Activity Reporting in the Gaming Industry: Based on Filings of Suspicious Activity Reports by Casinos and Card Clubs from January 1, 2004 through June 30, 2011** (2012) by FinCEN
- **Money Laundering of Casinos and Gaming Sector Report** (2009) by FATF
- **Risk-Based Approach for Casinos** (2008) by the FATF
- **Guidance on Casino or Card Club Risk-Based Compliance Indicators** (2010) by FinCEN
- **Guidance (Frequently Asked Questions) – Casino Recordkeeping, Reporting and Compliance Program Requirements** (2007, 2009, 2012) by FinCEN
- **Guidance on Casino or Card Club Compliance Program Assessment** (2010) by FinCEN
- **Definition of Money Services Business (Casinos as Money Services Businesses)** (2005) by FinCEN
- **Suspicious Activity Reporting Guidance for Casinos** (2003) by FinCEN
- **Guidance on Recognising Suspicious Activity – Red Flags for Casinos and Card Clubs** (2008) by FinCEN
- **Currency Transaction Reporting: Aggregation by Casinos at Slot Machines** (2005)by FinCEN
- **Guidance on Determining Whether Tribally Owned and Operated Casinos are Eligible for Exemption from CTR Requirements** (2002) by FinCEN
- **A Cash Wager on Table Game Play Represents a "Bet of Currency"** (2006) by FinCEN
- **Casino Industry Currency Transaction Reporting: An Assessment of Currency Transaction Reports filed by Casinos Between July 1, 2006 and June 30, 2008** by FinCEN

Additionally, the **Indian Gaming Working Group (IGWG)** consists of representatives from the FBI's financial crimes, public corruption and organised crime subprograms as well as representatives from other federal law enforcement agencies that meet to address significant criminal violations in the Indian gaming arena.

Key AML/CFT and Sanctions Requirements

2252. With which key AML/CFT and sanctions requirements are casinos and card clubs required to comply?

Casinos and card clubs must comply with the following key AML/CFT requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)

- Filing of Currency Transaction Reports (CTRs)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300) (for nongaming activities, such as restaurants or shops)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- OFAC and other sanctions requirements

The AML/CFT requirements for casinos and card clubs are implemented under 31 C.F.R. Part 1021 – Rules for Casinos and Card Clubs.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to casinos and card clubs is provided below.

2253. Are casinos and card clubs subject to the CIP requirement under Section 326 of the USA PATRIOT Act?

No. Currently, casinos and card clubs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2254. Are casinos and card clubs subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Casinos and card clubs are not subject to the CIP requirement. In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance, please refer to the Beneficial Owners section.

2255. What due diligence should casinos and card clubs perform on "regular" customers?

Casinos and card clubs should apply risk-based due diligence procedures on "regular" customers, including junket representatives. For additional guidance on due diligence and enhanced due diligence (EDD) standards, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

2256. What is a "junket representative"?

A "junket representative" or "junket operator" is generally defined as the organiser of a group of well-known players, a "junket" who travel together for the purpose of gambling.

2257. What due diligence is required for junket representatives?

Casinos and banks that establish accounts for junket representatives face similar customer due diligence challenges as correspondent, omnibus and trust accounts. Financial institutions must identify and, in some instances, verify the identity of all persons participating in the junket with a financial interest in the account for the purposes of complying with CIP, CTR and SAR reporting requirements.

2258. Are casinos and card clubs required to file CTRs?

Casinos and card clubs are required to file Currency Transaction Reports (CTRs).

For additional guidance on CTRs, please refer to the Currency Transaction Reports section.

2259. Are there exceptions to the CTR filing requirement for certain transactions in casinos and card clubs?

Yes. The following transactions are exempt from the requirement to file CTRs:

- Currency transactions with domestic banks (generally, nonbank financial institutions [e.g., casino or card club] are not required to report currency transactions with commercial banks);
- Currency transactions with dealers in foreign exchange or check cashers conducted pursuant to a contractual agreement covering purchases of a casino check and exchanges of currency for currency, including foreign currency;
- Cash-ins to the extent the same physical currency was wagered previously in a money play on the same table without leaving the table;
- Bills inserted into electronic gaming devices in multiple transactions;
- Cash outs won in a money play, to the extent it is the same physical currency wagered; or
- Jackpots from slot machines or video lottery terminals.

2260. What are examples of currency transactions conducted in casinos and card clubs?

Currency transactions for casinos and card clubs include, but are not limited to, the following:

- Purchases or redemptions of chips, tokens and gaming instruments
- Front money deposits or withdrawals
- Safekeeping deposits or withdrawals
- Payments or advances on any form of credit, including markers and counter checks
- Bets or payments of bets in currency

- Currency received by a casino for transmittal of funds through wire transfer for a customer
- Purchases of checks or cashing of checks or other negotiable instruments
- Exchanges of currency for currency, including foreign currency
- Reimbursements for customers' travel and entertainment expenses by the casino

2261. What are multiple transaction logs?

Many casinos and card clubs record currency transactions within a given threshold, usually US$2,500 to US$3,000, on multiple transaction logs (MTLs) pursuant to state, tribal or local laws. Some casinos use MTLs to assist in aggregating transactions for CTR filing, as well as identifying potentially suspicious activity.

2262. Can casinos and card clubs grant CTR exemptions?

No. Only depository institutions (banks, savings associations, thrift institutions or credit unions) can grant exemptions and then only for their U.S. customers. For further guidance on exemptions, please refer to the CTR Exemptions and the Designation of Exempt Persons Form section.

2263. Do casinos and card clubs have their own, unique SAR form?

No. FinCEN replaced industry-specific SAR forms with one new SAR for all covered financial institutions. As of April 1, 2013, casinos and card clubs must submit the new SAR (and other FinCEN Reports) electronically through the BSA E-Filing System.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2264. What types of activities require a SAR to be filed for casinos and card clubs?

Upon the detection of the following activities, casinos and card clubs should file a SAR:

- Transactions aggregating to US$5,000 or more that involve potential money laundering or violations of the Bank Secrecy Act (BSA) – Any transaction(s) totalling or aggregating to at least US$5,000 conducted by a suspect through the casino or card club, where the casino or card club knows, suspects or has reason to suspect that the transaction: involved illicit funds or is intended or conducted to hide or disguise funds or assets derived from illegal activities (including, but not limited to, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any law or regulation or avoid any transaction reporting requirement under federal law; or is designed to evade any BSA regulations.
- Evasion – A SAR should be filed in any instance where the casino or card club detects that the transaction was designed, whether through structuring or other means, to evade any BSA regulations.
- No business or apparent lawful purpose – The transaction has no business or apparent lawful purpose and there is no known reasonable explanation for the transaction after examination of available facts, including the background and possible purpose of the transaction.

- Facilitate criminal activity – The transaction involves the use of the casino or card club to facilitate criminal activity.

For red flags to assist in identifying suspicious activity as outlined above, please refer to the Suspicious Activity Red Flags section.

2265. What types of information and tools do casinos and card clubs have that can aid in monitoring for potentially suspicious activity?

Casinos and card clubs use a variety of automated programs for detecting unusual or suspicious activity. These automated programs may range from core casino management systems (CMS) to other applications including automated player-tracking systems, slot ticketing, point of sales systems, and third-party check cashing.

An automated player tracking system, for example, can be used to track all of the activity of players, including slot and table game play, and cage/credit transactions. Since some players may decline to use a club player card which tracks the customers' activity, casinos must also use other monitoring systems and tools to identify potentially suspicious activity. For example, slot data systems can be used to monitor transactions and identify potentially suspicious activity such as bill stuffing (putting in large transactions into slot machines with little gaming activity). Additionally, third-party check cashing systems can also be relied upon to alert the cage of "red flags" or to identify politically exposed persons (PEPs).

2266. Are there exceptions to the suspicious activity reporting requirements for casinos and card clubs?

Yes. Casinos and card clubs are not required to file a SAR for a robbery or burglary committed or attempted that is reported to appropriate law enforcement authorities.

2267. Can casinos and card clubs share SARs with U.S. parents and affiliates?

Casinos and card clubs are permitted to share SARs and information related to SARs with parents and affiliates under the following conditions:

- Parents, affiliates, offices or other places of business are located in the United States (e.g., SARs cannot be shared with non-U.S. offices of domestic parents and affiliates);
- The U.S. parent or affiliate has their own independent SAR filing obligation (e.g., SARs cannot be shared with U.S. parents and affiliates and their employees who do not perform functions related to gaming such as shops, restaurants, hotels); and
- Person(s) involved in the transaction(s) is not notified that the transaction(s) has been reported.

2268. What is "chip walking" and should casinos file SARs when it occurs?

The term "chip walking" refers to the act of patrons leaving casinos without redeeming or cashing out. Chips may be stored for an extended period of time in a remote location (e.g., in a safety deposit box).

Although the sole act of "chip walking" may not warrant a SAR, it may serve as a red flag for illicit activity and warrant further investigation. The decision to file a SAR should be based on the institution's own investigation into the activity of the patron.

For further guidance, please refer to the sections: Transaction Monitoring, Investigations and Red Flags and Suspicious Activity Reports.

2269. Are there red flags for detecting potentially suspicious activity for casinos and card clubs?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags and Casino Red Flags sections.

2270. What are some of the statistics and trends in SAR filings for Casinos and Card Clubs?

According to FinCEN, out of 1.98 million SAR filings from January 1, 2016 through December 31, 2016, Casinos and Card Clubs filed more than 57,000 SARs or 3 percent of all filings during this period; 71 percent were filed by state-licensed casinos, 24 percent by tribal-licensed casinos and 4 percent by card clubs:

- Fifty percent of SARs were filed on activity taking place in Nevada, Louisiana, California and Oklahoma;
- Ninety percent of SARs were filed on customers, 7 percent on unknown/blank relationship types, 1 percent on agents and 1 percent on individuals with no relationship with the casino or card club;
- Forty-eight percent of SARs involved gaming instruments, 41 percent involved U.S. currency, 5 percent involved "other" instrument types and 2 percent involved funds transfers;
- Top suspicious activity categories of SARs filed by casinos and card clubs included:
    - Structuring: 36 percent
    - Casinos: 26 percent (including more than 10,500 cases related to "minimal gaming with large transactions" and more than 1,200 cases related to "suspicious intra-casino funds transfers" and "suspicious use of counter checks or markers");
    - Money Laundering: 13 percent
    - Other Suspicious Activities: 12 percent (included more than 5,000 cases related to "two or more individuals working together," over 2,100 cases related to "transaction with no apparent economic, business or lawful purpose," nearly 1,000 cases related to counterfeit instruments, 66 cases related to suspected corruption (foreign and domestic) and 11 cases related to elder financial exploitation);
    - Identification Documentation: 11 percent (included more than 9,600 cases related to questionable or false documentation, refusal to provide documentation, single individual with multiple identities, multiple individuals with same or similar

identities; separate from identity theft, which accounted for less than 0.4 percent of SARs filed by casinos and card clubs); and

- Terrorism/Terrorist Financing: 0.07 percent (61 cases).

2271. What is internet gambling and is it legal?

Simply put, internet gambling is the online wagering of money or other value. Other terms used include online gambling and the more comprehensive term, remote gambling, which includes gambling through the use of remote communications such as the internet, smartphone, telephone, radio and television.

In the United States, there is no uniformly accepted definition of internet gambling, so the legality or illegality of some activities must be determined based on the particular facts.

Under the U.S. Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA), unlawful internet gambling includes placing, receiving or otherwise knowingly transmitting a bet or wager by any means that involves the use, at least in part, of the internet, where such bet or wager is unlawful under any applicable federal or state law in the state or tribal land in which the bet or wager is initiated, received or otherwise made.

Fantasy sports wagering is considered to be a game of skill by some and not a game of chance as with other types of gambling. Fantasy sports wagering was exempted from the federal definition of a "bet or wager" under the UIGEA. While some states have sought to legalise and regulate the fantasy sports market, others have been more restrictive.

For further guidance, please refer to the Illegal Internet Gambling and Fantasy Sports Wagering section.

2272. How do casinos and card clubs submit CTRs and SARs to FinCEN?

Beginning July 1, 2012, casinos must submit CTRs and SARs through the BSA E-Filing System, an internet-based e-filing system developed by FinCEN to enable financial institutions to file CTR and SAR forms electronically.

2273. What is the requirement for casinos and card clubs to perform independent testing of their AML Programs?

The final FinCEN rule on casinos and card clubs permits these entities to determine the scope and frequency of independent reviews at their discretion based on an evaluation of the money laundering and terrorist financing risks posed by their operations.

2274. What are the key recordkeeping requirements of the BSA for casinos and card clubs?

The BSA requires the retention of all BSA reports (e.g., SARs, CTRs, FBARs, CMIRs). Additionally, other required documentation must be retained by casinos and card clubs, such as the following:

- When required, a taxpayer identification number (TIN) (or passport number or description of a government-issued identification for non-resident aliens), name and address of each person for

whom a deposit is made, an account is opened or line of credit is extended, or for each person who has a financial interest in the account

- List of names, addresses and account or credit line numbers of those persons from whom the casino or card club was unable to obtain the above information
- A record of each receipt (including, but not limited to, funds for safekeeping or front money) of funds by the casino or card club for the deposit or credit account of any person that includes the name, address and TIN or passport number of the person from whom the funds were received
- A record of each bookkeeping entry comprising a debit or credit to a customer's deposit or credit account with the casino or card club
- Each statement, ledger card or other record of each deposit or credit account with the casino or card club, showing each transaction (including deposits, receipts, withdrawals, disbursements or transfers) in or with respect to a customer's deposit or credit account with the casino or card club
- A record of each extension of credit in excess of US$2,500, the terms and conditions of such extension of credit and repayments, name, address, TIN or passport number of the customer, and date and amount of transactions
- A record of each advisement, request or instruction received or given by the casino or card club for itself or another person with respect to a transaction involving a person, account or place outside of the United States, including, but not limited to, communications by wire, letter or telephone; if the transfer was made on behalf of a third party, the record shall include the third party's name, address, TIN or passport number, signature, and date and amount of the transaction
- Records prepared or received by the casino or card club in the ordinary course of business, which would be needed to reconstruct a person's deposit or credit account with the casino or card club or to trace a check deposited with the casino or card club through the casino or card club's records to the bank of deposit
- All records, documents or manuals required to be maintained by the casino or card club under state and local laws or regulations, regulations of any governing Indian tribe or tribal government or terms of (or any regulations issued under) Tribal-State compacts entered into pursuant to the Indian Gaming Regulatory Act, with respect to the casino or card club in question
- All records that are prepared or used by a casino or card club to monitor a customer's gaming activity
- A separate record containing a list including the date and amount of the transaction, type of instrument, name and address of the customer, name of the drawee or issuer of the instrument, reference numbers (e.g., personal check number, casino account number), name or casino license number of the employee who conducted the transaction, of the following types of instruments having a face value of US$3,000 or more:
    - Personal checks (excluding instruments that evidence credit granted by a casino or card club strictly for gaming, such as markers)

  - Business checks (including casino checks)
  - Official bank checks
  - Cashier's checks
  - Third-party checks
  - Promissory notes
  - Traveller's checks
  - Money orders
- Copy of the compliance program
- In the case of card clubs only, records of all currency transactions by customers, including, without limitation, records in the form of currency transaction logs and multiple currency transaction logs, and records of all activity at cages or similar facilities, including, without limitation, cage control logs
- Any record required to be maintained under the Funds Transfer Recordkeeping Requirements
- All indexes, books, programs, record layouts, manuals, formats, instructions, file descriptions and similar materials, which would enable a person to access and review the records described above readily

The above applies to casinos and card clubs. The BSA outlines additional requirements for other types of financial institutions (e.g., depository institutions, currency dealers or exchangers, broker-dealers) as well. For further guidance, please refer to the sections: BSA Recordkeeping Requirements, Money Services Businesses and Broker-Dealers in Securities.

2275. Are casinos and card clubs required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2276. Do casinos have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Casinos can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyberattacks to FinCEN via their hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2277. Are casinos and card clubs required to comply with the information sharing provision of Section 314 of the USA PATRIOT Act?

Financial institutions required to maintain an AML Program under Section 352 of the USA PATRIOT Act are required to comply with Section 314(a) – Cooperation Among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities. Participation in 314(b) – Cooperation Among Financial Institutions is voluntary.

While casinos and card clubs are required to participate in 314(a) requests, these requests have historically not been issued to casinos. Casinos and card clubs should have existing procedures in place for responding to such information requests.

Some casinos and card clubs have opted out of participating in 314(b) information sharing due to concerns with sharing information directly with competitors. Some institutions have shared information through a third-party registered with FinCEN to address this concern. Participation in 314(b) information sharing could improve the effectiveness of the AML/CFT efforts of casinos and card clubs.

2278. Who is responsible for examining casinos and card clubs for compliance with AML/CFT laws and regulations?

The Internal Revenue Service (IRS) is responsible for examining casinos and card clubs.

2279. Do other agencies have any role in overseeing casinos and card clubs?

States have various gaming regulatory agencies that supervise the industry. (For a list of state gaming agencies, please go to www.nagra.org.) State gaming regulators license and oversee casinos' and card clubs' operations. They also hold hearings and conduct background checks on personnel who own and

are employed by these businesses as part of their effort to detect organised crime and other illegal activity.

The National Indian Gaming Commission (NIGC) is an independent federal regulatory agency whose primary mission is to regulate gaming activities on Indian lands for the purposes of ensuring that Indian tribes are the primary beneficiaries of gaming revenues, and assuring that gaming is conducted fairly and honestly by both operators and players. The NIGC is authorised to: conduct background investigations of primary management officials and key employees of a gaming operation, conduct audits, review and approve tribal gaming ordinances and management contracts, promulgate federal regulations, investigate violations of these gaming regulations, and undertake enforcement actions (including the assessment of fines and issuance of closure orders). Both Class II gaming (e.g. bingo and certain card games) and Class III gaming (e.g. baccarat, blackjack, slot machines, and electronic or electromechanical facsimiles of any game of chance) are subject to the provisions of the Indian Gaming Regulatory Act (IGRA) and oversight by the NIGC. However, in general, the primary regulator for these activities is the tribal nations themselves.

Tribal-level regulators: Many tribal gaming commissions have been established by the tribes to oversee tribal gaming. The tribal nations have primary regulatory authority over Class II gaming. Regulation of Class III gaming may be addressed in the Tribal-State compacts (i.e. agreements between a state and a tribe, which are approved by the Secretary of the Interior, concerning the rules to govern the conduct of Class III gaming within the state). Although the terms of Tribal-State compacts vary by state, in most instances, the tribes remain the primary regulator for Class III gaming.

Operators of Credit Card Systems

Definitions

2280. What is an operator of a credit card system?

An operator of a credit card system is a business in the United States that administers a system for clearing and settling transactions in which the operator's credit card, whether acting as a credit card or debit card, is used to purchase goods or services or to obtain a cash advance, and authorises another entity to serve as an issuing or acquiring institution for the operator's credit card, which must be usable in the United States. Although there are many issuing and acquiring institutions, there are few operators of such systems in the United States (e.g., MasterCard, Visa).

2281. Which types of operators of credit card systems are required to maintain an AML Program pursuant to Section 352 of the USA PATRIOT Act?

All operators of credit card systems doing business in the United States are required to establish an AML Program. There is no exemption from the definition.

2282. What is the difference between an operator of a credit card system and an issuing/acquiring institution?

Any entity authorised by the operator to issue the operator's credit card is an "issuing institution." Any entity authorised to contract with merchants to process transactions involving the operator's credit card is called an "acquiring institution." Often, the operator authorises both issuing and acquiring institutions (member institutions) and prescribes rules that member institutions must follow.

2283. What is the difference between general-purpose credit cards and merchant cards?

General-purpose credit cards (e.g., Discover, MasterCard, Visa) are cards accepted by a variety of merchants worldwide.

Other credit cards in the United States are issued by a particular merchant or vendor and may only be used in connection with purchases made from that merchant or vendor. Examples include department store and oil company credit cards.

2284. Are operators of merchant card systems required to maintain an AML Program?

Merchants, vendors or banks whose issuance of credit cards is restricted to merchant cards (i.e., a credit card that may only be used at a specified merchant) do not fall within the definition of an operator of a credit card system and, therefore, are not subject to the AML Program requirement.

Key AML/CFT and Sanctions Requirements

2285. With which key AML/CFT and sanctions requirements are operators of credit card systems required to comply?

Operators of credit card systems must comply with the following key AML/CFT requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, conducts an independent review of the AML Program and conducts ongoing monitoring and updates (Section 352)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- OFAC and other sanctions requirements

The AML/CFT requirements for operators of credit card systems are implemented under 31 C.F.R. Part 1028 – Rules for Operators of Credit Card Systems.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to operators of credit card systems is provided below.

2286. Are operators of credit card systems subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, operators of credit card systems are not subject to the Customer Identification Program (CIP) requirement. However, the operator must have written policies and procedures designed to ensure the operator does not authorise or maintain authorisation for anyone to serve as an issuing or acquiring institution to guard against that person issuing the operator's credit card or acquiring merchants who accept the operator's credit card in circumstances that facilitate money laundering or the financing of terrorist activities. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2287. Are operators of credit card systems subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Operators of credit card systems are not subject to the CIP requirement and therefore are not required to identify beneficial owners. In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance, please refer to the Beneficial Owners section.

2288. Are operators of credit card systems required to file CTRs?

No. Currently, operators of credit card systems are not required to file Currency Transaction Reports (CTRs). Operators of credit card systems are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2289. Are operators of credit card systems required to file SARs?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages operators to file a SAR voluntarily for reporting suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

2290. Are operators of credit card systems required to comply with OFAC and other sanction regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2291. Do operators of credit card systems have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Operators of credit card systems can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that will require the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2292. Should operators of credit card systems address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), operators of credit card systems can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

Dealers in Precious Metals, Precious Stones or Jewels

Definitions

2293. Which types of dealers in precious metals, precious stones or jewels are required to maintain an AML Program under Section 352 of the USA PATRIOT Act?

Anyone engaged as a business in the purchase and sale of covered goods (i.e., in precious metals, precious stones or jewels) that purchases and sells US$50,000 or more of "covered goods" in the preceding year is required to maintain an AML Program.

2294. How are the terms "covered goods," "precious metals," "finished goods," "jewels" and "stones" defined?

"**Covered goods**" include precious metals, precious stones or jewels, or finished goods that derive 50 percent or more of their value from precious metals, precious stones or jewels contained in or attached to the finished goods.

"**Precious metals**" are defined as gold, silver and certain other metals at a level of purity of 500 parts per 1,000 or greater and an alloy containing 500 or more parts per 1,000.

"**Jewels**" and "**stones**" are defined as organic substances that have a market-recognised gem level of quality, beauty and rarity.

"**Finished goods**" include, but are not limited to, jewellery, numismatic items and antiques.

2295. What is the heightened money laundering and terrorist financing risk of dealers in precious metals, precious stones or jewels?

The high value, transportability, liquidity, negotiability and global nature of trade of precious metals, precious stones and jewels make them susceptible to money laundering and terrorist financing.

2296. How should the US$50,000 sales threshold be calculated?

The US$50,000 sales threshold should be based on the value of precious metals, stones and jewels purchased and sold during the preceding year. It should not be based on the selling price of the finished goods purchased or sold. In other words, if a business purchases and sells finished goods that derive 50 percent or more of their value from precious stones, metals or jewels, the US$50,000 sales threshold should be calculated based on the value of the precious stones, metals or jewels contained in the finished goods, not the selling price of the finished goods themselves.

The rule applies only to persons who both purchased US$50,000 or more in covered goods and sold US$50,000 or more in covered goods in the preceding calendar or tax year.

2297. Are trades or exchanges considered purchases?

For purposes of meeting the definition of "dealer" only, the purchase and sale of covered goods does not include retail transactions in which the dealer or retailer accepts from a customer covered goods,

the value of which the dealer or retailer credits to the customer's account or to another purchase by the customer, and no funds are provided to the customer in exchange for the covered goods.

Trades or exchanges that are used for credit against the purchase of new covered goods should not be included in the US$50,000 sales threshold used to define a dealer. Rather, the focus is on cash purchases.

Businesses that meet the definition of dealer should still examine the risk of trades or exchanges as they would with other transactions involving covered goods. Also, this exception is not an exception to the scope of the AML Program required of a covered dealer other than a retailer.

2298. Does "toll-refining" constitute the purchase and sale of covered goods?

No. Toll-refining is the refining of scrap metal or concentrates for which the refinery is paid a fee. There is no change in ownership of the metal recovered. The payment of a fee is made in exchange for the service of refining, not for the extracted precious metal; therefore, this type of transaction would not constitute the purchase or sale of a covered good.

2299. Are retail establishments, such as department stores that sell high-end jewellery, required to establish an AML Program?

The interim final rule distinguishes between "dealer" and "retailer." A retailer is a person in the United States engaged in sales of covered goods, primarily to the public. As long as retailers purchase covered goods from U.S.-based dealers/retailers or limit purchases from non-U.S.-based dealers/retailers to less than US$50,000, they are not required to establish an AML Program.

If retailers purchase US$50,000 or more from non-U.S.-based dealers/retailers and sell more than US$50,000 of covered goods during a calendar or tax year, they are required to have an AML Program to address the risks associated with purchases from foreign suppliers.

2300. Are there additional exemptions from the definition of "dealer"?

Businesses licensed or registered as pawnbrokers under state or municipal law are exempt from the definition of "dealer." Pawnbrokers are included in the BSA's expanded definition of "financial institution." However, implementing regulations have yet to be issued.

Additionally, persons who merely facilitate the purchase and sale of covered goods (e.g., auctioneers, bankruptcy trustees) do not meet the definition of dealer.

2301. How do the U.S. AML/CFT requirements for dealers in precious metals, precious stones and jewels correspond to FATF Recommendations?

FATF Recommendations 22 – DNFBPs: Customer Due Diligence and Recommendation 23 – DNFBPs: Other Measures advises regulatory oversight of dealers in precious metals and precious stones and suggests the implementation of measures by dealers to guard against money laundering and terrorist financing such as conducting due diligence on cash transactions greater than US/EUR 15,000 (e.g., report suspicious activities).

U.S. AML/CFT laws require dealers in precious metals, precious stones and jewels to implement an AML Program and file BSA reports such as Suspicious Activity Reports (SARs), consistent with FATF Recommendations.

For further guidance on international standards, please refer to the Financial Action Task Force section.

2302. What guidance has been issued on dealers of precious metals, stones or jewels?

The following are examples of key guidance that has been issued related to precious metals, stones or jewels:

- **Frequently Asked Questions: Interim Final Rule: Anti-Money Laundering Programs for Dealers in Precious Metals, Stones or Jewels** (2012) by FinCEN
- **Definition of Precious Metals in the Interim Final Rule Requiring Anti-Money Laundering Programs for Dealers in Precious Metals, Stones or Jewels** (2011) by FinCEN
- **High-Level Principles and Procedures for Dealers in Precious Metals and Dealers in Precious Stones** (2008) by the Financial Action Task Force (FATF)
- **Money Laundering and Terrorist Financing Through Trade in Diamonds** (2013) by FATF and the Egmont Group
- **Interim Final Rule: Anti-Money Laundering Programs for Dealers in Precious Metals, Stones or Jewels** (2005) by FinCEN
- **Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold** (2015) by FATF

Key AML/CFT and Sanctions Requirements

2303. With which key AML/CFT and sanctions requirements are dealers of precious metals, precious stones or jewels required to comply?

Dealers must comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])

- OFAC and other sanctions requirements

The AML/CFT requirements for dealers in precious metals, precious stones or jewels are implemented under 31 C.F.R. 1027 – Rules for Dealers in Precious Metals, Precious Stones or Jewels.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to dealers is provided below.

2304. Are dealers subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, dealers are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2305. Are dealers subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Dealers are not subject to the CIP requirement and therefore are not required to identify beneficial owners. In its final rule, FinCEN did indicate that it will continue to consider how the principles of customer due diligence should be applied to different types of financial institutions.

For further guidance, please refer to the Beneficial Owners section.

2306. Are CMIRs required to be filed on the cross-border transportation of precious stones, precious metals or jewels valued at greater than US$10,000?

No. CMIRs are required on the cross-border physical transportation of currency and monetary instruments in excess of US$10,000. Per FinCEN guidance, precious metals, precious stones or jewels do not meet the definition of currency or monetary instruments for BSA reporting purposes. For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

2307. Are dealers required to file CTRs?

No. Currently, dealers are not required to file Currency Transaction Reports (CTRs). Dealers are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2308. Are dealers required to file SARs?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages dealers to file a SAR voluntarily for reporting suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

2309. What is trade-based money laundering (TBML) and how can precious metals, precious stones and jewels be used in these schemes?

Trade-based money laundering (TBML) refers to the process of disguising the proceeds of illegal activity and moving value through the use of trade transactions so that they appear to come from legitimate sources or activities.

Precious metals, precious stones and jewels can be used in multiple TBML schemes, including, but not limited to, the following:

- Under or over-valuing or invoicing of covered goods;
- Purchasing of covered goods to store, smuggle and ultimately transfer illicit proceeds once covered goods are liquidated.

2310. Are dealers required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2311. What is OFAC's Rough Diamond Trade Controls Sanctions program and how does it impact dealers in precious metals, precious stones and jewels?

Established by the Clean Diamond Trade Act (CDTA), IEEPA, NEA, UNPA, and Executive Order 13312 – Implementing the Clean Diamond Trade Act, OFAC's Rough Diamond Trade Controls Sanctions Program prohibits the import and export of rough diamonds from countries that do not participate in the Kimberley Process Certification Scheme (KPCS) and prohibits any transaction that evades or attempts to evade these prohibitions on or after July 30, 2003.

Dealers in precious metals, precious stones and jewels that import or export rough diamonds directly must comply with KPCS and the Rough Diamond Trade Control Program rules, which include registration, reporting and other trade control requirements.

Dealers should identify suppliers who may be involved in the rough diamond business and conduct appropriate due diligence to mitigate their AML/CFT and sanctions risks.

For further guidance on the sanctions related to rough diamonds, please refer to the Rough Diamond Trade Controls Sanctions Program section.

2312. How are "rough diamonds" defined under the Rough Diamond Trade Controls Sanctions program?

Rough diamonds are defined as "any diamond that is unworked or simply sawn, cleaved, or bruted and classifiable under subheading 7102.10, 7102.21, or 7102.31 of the Harmonised Tariff Schedule of the United States."

2313. What is the Kimberley Process Certification Scheme (KPCS)?

Launched in 2003, the Kimberley Process Certification Scheme (KPCS) is an international program that implements certification requirements and other import/export controls to prevent the production and trade in rough diamonds that are used to finance violence in countries in conflict (e.g., Democratic Republic of the Congo, Cote d'Ivoire). These diamonds are also known as "conflict diamonds" or "blood diamonds."

The Kimberley Process Certificate is a unique tamper-and forgery-resistant document that certifies that a shipment of rough diamonds was handled in accordance with KPCS. Kimberley Process Certificates can only be obtained from entities licensed by the U.S. Kimberley Process Authority (USKPA).

For imported rough diamonds, the ultimate consignee is required to report receipt of the shipment to the relevant foreign exporting authority (e.g., the agency with the authority to validate the Kimberley Process Certificate). Reports must be made within 15 calendar days of the date that the shipment arrived at a U.S. port of entry.

For exported rough diamonds, exporters must report the shipment to the U.S. exporting authority, Bureau of Census, through the Automated Export System (AES).

U.S. Customs will not release shipments of rough diamonds without formal and complete documentation.

2314. Are any other types of jewels, stones or minerals subject to sanctions by OFAC?

Yes. Section 1245 of the Iran Freedom and Counter-Proliferation Act of 2012 (IFCA) imposes sanctions on persons engaged in trade in precious metals, graphite, raw or semi-finished metals such as aluminium and steel with sanctioned persons as outlined in Executive Order 13645. Some of the other country-based sanctions programs aim to protect other "natural resources" (e.g., jade, oil) of select countries in conflict (e.g., Myanmar [Burma], Libya).

2315. Do dealers have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Dealers can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that will require the adoption of a cybersecurity program that, at a minimum, addresses the following core functions: Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed):

- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2316. Should dealers address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the PII of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), dealers can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2317. Does the Dodd-Frank Act impose any requirements relating to minerals?

Although not a sanction per se, Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act required that a company publicly disclose if it uses conflict minerals that originated in the Democratic Republic of the Congo or adjoining countries (collectively, the covered countries) that are "necessary to the functionality or production" of a product manufactured or contracted to be manufactured by the company.

The purchase of these so-called conflict minerals allegedly benefits armed rebels in these countries and the required disclosure is expected to put pressure on companies to disassociate with the covered countries.

The SEC rule implementing this provision of the Dodd-Frank Act required both domestic and foreign issuers that file with the SEC to publicly disclose their use of conflict minerals on a new form, Form SD, the first of which were to be filed by June 2, 2014, and are required annually on May 31 thereafter. In instances where a company determines that conflict minerals are from covered countries, a Conflict Minerals Report must accompany Form SD. Enforcement of the rule has been suspended by the SEC due to an April 2017 ruling by the U.S. District Court for the District of Columbia that this provision violated the First Amendment of the U.S. constitution.

For further guidance on the sanctions related to rough diamonds, please refer to the Rough Diamond Trade Controls Sanctions Program section.

2318. Who is responsible for examining dealers for compliance with AML/CFT laws and regulations?

The IRS is responsible for examining dealers for compliance with AML/CFT laws and regulations.

Loan or Finance Companies/Nonbank Residential Lenders and Originators

Definitions

2319. Which types of "loan or finance companies" are required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

At this time, only nonbank residential mortgage lenders and originators (RMLOs) fall under the definition of "loan or finance company" required to establish an AML Program. FinCEN has indicated that it has plans to add other types of entities in an incremental approach to implementing AML/CFT regulations for loan and finance companies.

2320. What is a "nonbank residential mortgage lender or originator"?

Nonbank residential mortgage lenders and originators (RMLOs) are a subset of loan and finance companies that deal directly with customers to provide loans and financing for residential mortgage loans.

A **residential mortgage** is defined as "a loan that is secured by a mortgage, deed of trust or other equivalent consensual security interest on:

- A residential structure that contains one to four units, including, if used as a residence, an individual condominium unit, cooperative unit, mobile home or trailer; or
- Residential real estate upon which such a structure is constructed or intended to be constructed."

A **residential mortgage lender** is defined as "the person to whom the debt arising from a residential mortgage loan is initially payable on the face of the evidence of indebtedness or, if there is no such evidence of indebtedness, by agreement, or to whom the obligation is initially assigned at or immediately after settlement." Individuals who finance the sale of their own dwelling or real property are not included in the definition of residential mortgage lender.

A **residential mortgage originator** is defined as "a person who accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage."

2321. Are nonbank RMLOs considered to be "financial institutions" under the Bank Secrecy Act (BSA)?

The definition of "financial institution" under the BSA, which was significantly expanded by the USA PATRIOT Act, does not specifically include nonbank RMLOs. However, the term "financial institution" includes "loan or finance companies" which now include nonbank RMLOs pursuant to FinCEN's final

rule, "Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators." FinCEN regulations do not define "loan or finance company" but do indicate that the following are excluded:

- Banks;
- Persons regulated/examined by the U.S. Securities and Exchange Commission or the Commodity Futures Trading Commission;
- Government-sponsored enterprise (GSE) regulated by the Federal Housing Finance Agency;
- Federal or state agency or authority administering mortgage or housing assistance, fraud prevention or foreclosure prevention programs; and
- An individual employed by a bank, loan or finance company, or other regulated business.

2322. Are any types of nonbank RMLOs exempt from the final rule?

No. All nonbank RMLOs are required to comply with the final rule, regardless of size or other criteria or characteristic.

2323. What is the purpose of this final rule?

In 2006, FinCEN began a series of extensive studies around mortgage fraud and other related financial crimes; this focus was heightened by the financial crisis. These efforts led to the observation that nonbank RMLOs are uniquely positioned, through their direct contact with customers, to identify, assess, and report on risks of fraudulent activity and money laundering. The imposition of these AML/CFT requirements on nonbank RMLOs is intended to close or mitigate an identified gap in reporting on this activity.

FinCEN and other government agencies, including the U.S. Department of Justice (DOJ), anticipate that requiring nonbank RMLOs to file SARs will assist their ability to uncover large-scale mortgage fraud in addition to traditional money laundering, through an increased number of SAR filings, and serve as a deterrent to criminal activity.

2324. What guidance has been issued regarding the differences in requirements for loan or finance company subsidiaries of other financial institutions?

On August 13, 2012, FinCEN issued an Administrative Ruling to clarify expectations regarding "Compliance obligations of certain loan or finance company subsidiaries of federally regulated banks and other financial institutions." The ruling indicated that loan or finance subsidiaries would be obligated to comply with the AML/CFT laws and regulations applicable to their parent financial institution. Additionally, the loan or finance subsidiary would be subject to examination by the parent financial institution's federal functional regulator.

2325. Is FinCEN focused on other participants in the mortgage market in addition to nonbank RMLOs?

Yes. In February 2014, FinCEN released a final rule requiring Housing GSEs to establish an AML Program. FinCEN has and continues to consider whether and how AML/CFT requirements should apply to other participants in the mortgage market, including persons involved in real estate closings and settlements (e.g., real estate brokers, attorneys representing buyers/sellers, title insurance companies, escrow agents, real estate appraisers).

As part of the proposed rule for Housing GSEs, FinCEN requested comments on what other mortgage-related activities and entities should be subject to AML Program and SAR filing requirements. Specifically, FinCEN has solicited feedback on the following participants in the mortgage market:

- Private mortgage insurers (and reinsurers);
- Mortgage servicers; and
- Other types of businesses in the primary and secondary mortgage markets.

For further guidance, please refer to the sections: Housing Government-Sponsored Enterprises and Persons Involved in Real Estate Settlements and Closings.

2326. What other guidance has been issued to assist nonbank RMLOs in complying with AML/CFT laws and regulations?

FinCEN has created a page on its website with publications and webinar trainings to assist RMLOs and others involved in real estate in complying with AML/CFT laws and regulations. Additionally, FinCEN has developed substantial data analytics around mortgage-related financial crimes to help RMLOs understand the significance and purpose behind the AML/CFT laws and regulations. The publications on these metrics include:

- Mortgage Fraud SAR Data Tables by State, Urban Area and County
- Suspected Mortgage Fraud (Including Quarterly Written Reports)
- Suspected Money Laundering and Fraud in the Residential Real Estate Industry
- Suspected Money Laundering and Fraud in the Commercial Real Estate Industry
- Home Equity Conversion Mortgages (Reverse Mortgages)
- Mortgage Fraud Cases Supported by FinCEN Filings
- Foreclosure Rescue Scams & Loan Modification Fraud

There is also access to links for other government agencies and initiatives, such as the Financial Fraud Enforcement Task Force (FFETF).

For additional information, please refer to the Mortgage Fraud section.

Key AML/CFT and Sanctions Requirements

2327. With which key AML/CFT and sanctions requirements are nonbank RMLOs required to comply?

Nonbank RMLOs are required to comply with the following key AML/CFT and sanctions requirements:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Information sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- OFAC and other sanctions requirements

The AML/CFT requirements for RMLOs are implemented under 31 C.F.R. Part 1029 – Rules for Loan or Finance Companies.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to RMLOs is provided below.

2328. Are nonbank RMLOs subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, nonbank RMLOs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2329. Are RMLOs subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. RMLOs are not subject to the CIP requirement and therefore are not required to identify beneficial owners. However, the Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future.

For further guidance, please refer to the Beneficial Owners section.

2330. Are nonbank RMLOs required to file CTRs?

No. Currently, nonbank RMLOs are not required to file Currency Transaction Reports (CTRs). They are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2331. What is the SAR filing requirement for nonbank RMLOs?

Nonbank RMLOs are required to report a transaction that involves funds of at least US$5,000 and that the nonbank RMLO knows, suspects, or has reason to suspect that a transaction:

- Involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- Is designed, whether through structuring or other means, to evade any reporting requirements under regulations promulgated by the BSA;
- Has no business or apparent lawful purpose or is not the sort in which the particular nonbank RMLO customer would normally be expected to engage, and the nonbank RMLO knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves the use of the nonbank RMLO to facilitate criminal activity.

For further guidance, please refer to the Suspicious Activity Reports section.

2332. Are the SAR filing requirements for nonbank RMLOs the same as for other covered financial institutions?

Yes. Nonbank RMLOs' SAR filing requirements (e.g., time frame for filing, dollar thresholds, confidentiality) are the same as those for banks and nonbank financial institutions. For additional guidance on SAR filing requirements, please refer to the Suspicious Activity Reports section.

2333. Are nonbank RMLOs afforded the same "Safe Harbor" protection as other covered financial institutions?

Yes. Nonbank RMLOs, as well as their directors, officers, employees and agents, would be covered under the Safe Harbor provision. For further guidance, please refer to the Safe Harbor section.

2334. Are nonbank RMLOs permitted to file a SAR jointly with another financial institution?

Yes, in instances where more than one nonbank RMLO or other financial institution is obligated to report on the same transaction(s), only one SAR should be filed on behalf of all the financial institutions involved. That SAR should identify all of the financial institutions involved and provide all the relevant facts relating to each institution. Each institution should retain a copy of the SAR, along

with supporting documentation. For further guidance, please refer to the Third-Party and Joint Filings of SARs section.

2335. What are some examples of red flags with which nonbank RMLOs may be concerned?

Common red flags include, but are not limited to, the following:

- Borrower arrives at a real estate closing with a significant amount of cash;
- Borrower purchases property in the name of a nominee, such as an associate or a relative;
- Borrower negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table";
- Borrower sells property below market value with an additional "under the table" payment;
- Borrower or agent of the borrower purchases property without much knowledge about the property inspection or does not appear sufficiently knowledgeable about the purpose or use of the real estate being purchased;
- Borrower purchases multiple properties in a short time period or appears to be buying and selling the same piece of real estate for no apparent legitimate purpose;
- Seller requests that proceeds be sent to a high-risk jurisdiction or offshore bank; and
- Borrower makes payments with funds from a high-risk jurisdiction or offshore bank.

For additional guidance, please refer to the sections: Mortgage Fraud, Mortgage and Real Estate Red Flags and Lending Red Flags.

2336. What are some of the statistics and trends in SAR filings for RMLOs?

According to FinCEN, out of 1.98 million SAR filings from January 1, 2016 through December 31, 2016, RMLOs filed over 3,000 SARs or 0.2 percent of all filings during this period:

- Nearly 80 percent of SARs were filed on activity taking place in Michigan, Texas and California;
- Fifty percent of SARs were filed on the "unknown/blank" relationship type, 23 percent on borrowers, 16 percent on individuals with no relationship to the loan or finance company, 7 percent on customers and 2 percent on individuals with "other" relationship type;
- Ninety-eight percent of SARs involved residential mortgages, 27 percent involved personal/business checks, 22 percent involved funds transfers, 20 percent involved bank/cashier's checks and 8 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by loan or finance companies included:
    - Mortgage Fraud: 35 percent
    - Fraud: 32 percent (included nearly 300 cases on consumer loan fraud and over 100 cases of check fraud);
    - Structuring: 1 percent

- Money Laundering: 3 percent
- Other Suspicious Activities: 16 percent (included nearly 270 cases related to forgeries, over 230 cases related to "two or more individuals working together," over 1,30 cases related to counterfeit instruments, and 33 cases related to elder financial exploitation), 24 cases related to suspected corruption (foreign and domestic) and 15 cases related to unauthorised electronic intrusion;
- Identification Documentation: 12 percent (included more than 600 cases related to questionable or false documentation and refusal to provide documentation, separate from identity theft which accounted for less than 0.3 percent of SARs filed by loan or finance companies); and
- Terrorism/Terrorist Financing: 0.01 percent (1 cases).

2337. Does delegating aspects of its AML Program to a third party mean a nonbank RMLO will not be held responsible?

No. Any nonbank RMLO that delegates responsibility to a third party remains fully responsible for the effectiveness of its AML Program and for ensuring that compliance examiners are able to obtain access to any information they need relating to the nonbank RMLO's AML Program.

2338. Are nonbank RMLOs permitted to participate in the information sharing provisions under Sections 314(a) and (b) of the USA PATRIOT Act?

Yes. Any financial institutions required to establish an AML Program under Section 352, including nonbank RMLOs, are obligated to comply with Section 314(a) information requests and may voluntarily participate in the information sharing mechanisms established by Section 314(b).

For further guidance, please refer to the sections: Section 314(a) – Cooperation Among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities and Section 314(b) – Cooperation Among Financial Institutions.

2339. Are nonbank RMLOs required to comply with OFAC and other sanction laws and regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2340. Do RMLOs have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health

or financial stability of the United States. RMLOs can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyber-attacks to FinCEN via their hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2341. Should RMLOs address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), RMLOs can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2342. Who is responsible for examining nonbank RMLOs for compliance with AML/CFT laws and regulations?

Where nonbank RMLOs do not have a federal functional regulator, they will be subject to examination by the parent financial institution's federal functional regulator or FinCEN will rely on examinations conducted by state supervisory agencies, where applicable.

Persons Involved in Real Estate Settlements and Closings

Definitions

2343. Which types of persons involved in real estate settlements and closings may be required to maintain AML Programs pursuant to Section 352 of the USA PATRIOT Act?

In a 2003 proposed (still pending), rule for persons involved in real estate settlements and closings, FinCEN defined a real estate settlement or closing as the process involving the payment of the purchase price to the seller and the transfer of title to the buyer.

The manner in which the process is carried out differs depending on a number of factors, including location. The process may be conducted by an attorney, a title insurance company, an escrow company or another party.

2344. Are all types of real estate transactions subject to the AML Program requirement?

Proposed rulings have not excluded any types of real estate transactions; however, regulators have sought comments on the possibility of exempting commercial real estate activity from the AML Program requirement.

2345. Who is considered a person "involved" in real estate settlements and closings?

Under the proposed rule, involved persons include, but are not limited to, the following:

- Real estate broker
- Attorney representing buyer/seller
- Financing entity (e.g., bank, mortgage broker)
- Title insurance company
- Escrow agent
- Real estate appraiser

2346. What factors are being considered by the U.S. Treasury Department to determine which involved persons will be subject to the AML Program requirement?

The following factors are being considered by the U.S. Treasury:

- Persons offering high-risk products/services in connection with a real estate closing and settlement (i.e., products/services that can be abused by money launderers or terrorists)
- Persons who are positioned to monitor for suspicious activity effectively (e.g., those who can identify the source, purpose and nature of transactions)

Concerned with the conflicts between the requirement to report suspicious activity and attorney-client privilege and client confidentiality, some law firms have suggested utilising the following factor to determine applicability:

- Position as financial intermediary (i.e., persons who handle the receipt and transmission of cash proceeds through accounts that they control in the act of closing a real estate transaction)

Though the financial intermediary factor may be of assistance in clearly defining "involved persons," it is important to note that individuals who do not "touch the money" may still be in positions to detect and report suspicious activity related to real estate settlements and closings (e.g., suspicious documentation, identity theft).

2347. Would any persons involved in real estate settlements and closings be exempt from the AML Program requirement?

Purchasers and sellers of their own real estate are exempted from the definition of real estate settlements and closings and are not subject to the AML Program requirement pursuant to Section 352 of the USA PATRIOT Act.

2348. What is the difference between a closing and a settlement?

The terms "closing" and "settlement" refer to the same process. Use of either term is dependent on the jurisdiction in which the activity takes place. Other terms used to describe the closing/settlement process include "New York style table closing," "Western style table closing" or "escrow closing."

2349. What AML/CFT guidance has been issued related to real estate?

The following are examples of key guidance that has been issued related to real estate:

- Lending Activities – Overview within the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual by the Federal Financial Institutions Examination Council (FFIEC)
- SRC Insights: From the Examiner's Desk: Suspicious Activity Monitoring in the Lending Function (2011) by the Federal Reserve Bank of Philadelphia
- An OFAC Primer for the Real Estate Settlement and Title Insurance Industry (2003) by the Office of Foreign Assets Control (OFAC)
- RBA Guidance for Real Estate Agents (2008) by the Financial Action Task Force (FATF)

- Money Laundering and Terrorist Financing Through the Real Estate Sector (2007) by FATF
- Money Laundering in the Commercial Real Estate Industry: An Assessment Based Upon Suspicious Activity Report Filing Analysis (2006) by the Financial Crimes Enforcement Network (FinCEN)
- SAR Analysis: Real Estate Title and Escrow Companies: A BSA Filing Study: Assessing Suspicious Activity Reports and Suspicious Form 8300 Filings Related to Real Estate Title and Escrow Businesses (2003 – 2011) (2012) by FinCEN

For additional guidance related to mortgage fraud, please refer to the Mortgage Fraud section.

Key AML/CFT and Sanctions Requirements

2350. With which key AML/CFT and sanctions requirements are persons involved in real estate settlements and closings required to comply?

Persons involved in real estate settlements and closings are required to comply with the following key AML/CFT and sanctions requirements:

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanctions requirements

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to persons involved in real estate settlements and closings is provided below.

2351. Are persons involved in real estate settlements and closings required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

No. At present, the AML Program requirement of Section 352 of the USA PATRIOT Act does not apply to persons involved in real estate settlements and closings. However, some institutions, such as banks, are already covered and required to establish an AML Program and comply with other AML/CFT requirements.

2352. Are persons involved in real estate settlements and closings subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, persons involved in real estate settlements and closings are not subject to Section 326 of the USA PATRIOT Act (the Customer Identification Program [CIP] requirement). For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2353. Are persons involved in real estate settlements and closings subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Persons involved in real estate settlements are not subject to the CIP requirement and therefore are not required to identify beneficial owners. However, the Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program for financial institutions subject to Section 352. The requirements of the Beneficial Ownership Rule could be extended in the future.

For further guidance, please refer to the Beneficial Owners section.

2354. Are persons involved in real estate settlements and closings required to file CTRs?

No. Currently, persons involved in real estate settlements and closings are not required to file Currency Transaction Reports (CTRs). They are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2355. Are persons involved in real estate settlements and closings required to file SARs?

While they are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of a SAR for suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

2356. Are there red flags for detecting potentially suspicious activity for persons involved in real estate settlements and closings?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution, and high-risk products/services/transactions (e.g., cash, wires, monetary instruments, lending) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags, Lending Red Flags and Mortgage and Real Estate Red Flags sections.

2357. Are persons involved in real estate settlements and closings required to comply with the information-sharing requirement of Section 314 of the USA PATRIOT Act?

No. Only those institutions required to establish an AML Program are obligated to comply with the information-sharing requirement of the USA PATRIOT Act.

2358. Are persons involved in real estate settlements and closings required to comply with OFAC and other sanctions regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on

OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2359. Do persons involved in real estate settlements and closings have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Persons involved in real estate settlements and closings can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that will require the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2360. Should persons involved in real estate closings and settlements address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), persons involved in real estate settlements and closings can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

Housing Government-Sponsored Enterprises

Definitions

2361. What is a government-sponsored enterprise (GSE)?

A government-sponsored enterprise (GSE) is a financial services organisation created and regulated by the U.S. government (specifically, by Congress) and functioning to increase the availability and reduce the cost of credit to targeted sectors such as education, agriculture and home finance. Examples of GSEs include, but are not necessarily limited to:

- Federal National Mortgage Association (Fannie Mae)
- Federal Home Loan Mortgage Corporation (Freddie Mac)
- Federal Agricultural Mortgage Corporation (Farmer Mac)
- The 12 Federal Home Loan Banks (FHL Banks)
- Federal Farm Credit Banks
- Financing Corporation (FICO)
- National Veterans Business Development Corporation

2362. Is a GSE considered a "financial institution" under the BSA?

The definition of "financial institution" under the BSA, which was significantly expanded by the USA PATRIOT Act, does not specifically include GSEs. However, the term, "financial institution" includes "any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any [covered financial institution] is authorised to engage." FinCEN's final rule "Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Housing GSEs," issued in February 2014, designates Housing GSEs as financial institutions.

2363. Which GSEs are required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

Pursuant to FinCEN's final rule, GSEs that are required to maintain an AML Program include the following:

- Federal National Mortgage Association (Fannie Mae)
- Federal Home Loan Mortgage Corporation (Freddie Mac)
- Federal Home Loan Banks (FHL Banks)

Collectively, these enterprises are referred to as Housing GSEs.

2364. What is the heightened money laundering and terrorist financing risk of Housing GSEs?

Of the various types of GSEs, Housing GSEs are the most vulnerable to the use of mortgages to commit financial crimes due to their close involvement with the lending processes. Additionally, their risk is heightened due to their involvement in the secondary residential mortgage market and the recent abuses of securitised mortgages and related financial instruments.

2365. What value does FinCEN see in requiring Housing GSEs to establish AML Programs and file SARs?

FinCEN indicated that the final rule is another effort to help restore the integrity of the mortgage market by providing law enforcement with quicker access to data about potential financial crimes that will help them better hold illicit actors accountable for mortgage fraud and other scams. In the last eight years, as an offshoot of the financial crisis, FinCEN has made increasing the focus on preventing, detecting and reporting mortgage fraud one of its highest priorities. For further information, please refer to the Mortgage Fraud section.

2366. Are the Housing GSEs likely to encounter any unique challenges in implementing FinCEN's final rule?

Although current practice requires that the Housing GSEs have comprehensive information related to commercial loans they acquire, they traditionally have relied on the selling institutions to analyse retail borrowers and have not collected information for individual retail borrowers. This will create an obvious challenge to identifying suspicious activity at the retail customer level even though the final rule suggests that Housing GSEs would not be expected to obtain information they don't currently collect.

2367. Who are the typical customers of Housing GSEs?

Housing GSEs support the primary mortgage market by providing liquidity through loan purchases and collateralised advances that permit their customers, typically commercial banks, credit unions and thrifts, to offer a broad range of credit products and related services. Many of their typical customers are subject to AML/CFT laws and regulations.

2368. Is FinCEN focused on other participants in the mortgage market in addition to Housing GSEs?

Yes. FinCEN issued a Final Rule in February 2012 requiring Non-Bank Residential Mortgage Lenders and Originators (RMLOs), a subset of a loan and finance company, to establish AML Programs and file SARs. For further guidance, please refer to the Loan or Finance Companies/Nonbank Residential Lenders and Originators section.

FinCEN has and continues to consider whether and how AML/CFT requirements should apply to other participants in the mortgage market, including persons involved in real estate closings and settlements. For further guidance, please refer to the Persons Involved in Real Estate Closings and Settlements section.

FinCEN requested comments on what other mortgage-related activities and entities should be subject to AML Program and SAR filing requirements. Specifically, FinCEN has solicited feedback on the following participants in the mortgage market:

- Private mortgage insurers (and reinsurers);
- Mortgage servicers; and
- Other types of businesses in the primary and secondary mortgage markets.

Key AML/CFT and Sanctions Requirements

2369. With which key AML/CFT laws and regulations are Housing GSEs required to comply?

Housing GSEs must comply with the following key AML/CFT laws and regulations:

- Establishment of an AML Program that formally designates an AML compliance officer, establishes written policies and procedures, establishes an ongoing AML training program, conducts an independent review of the AML Program and ongoing monitoring and updates (Section 352)
- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (FinCEN 8300) (only where not required to file a CTR)
- Filing of Suspicious Activity Reports (SARs)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- Recordkeeping and retention (e.g., Funds Transfer Rule, Travel Rule, Purchase and Sale of Monetary Instruments)
- Information-sharing (Section 314(a) [mandatory], Section 314(b) [optional])
- OFAC and other sanctions requirements

The AML/CFT requirements for Housing GSEs are implemented under 31 C.F.R. Part 1030 – Rules for Housing Government-Sponsored Enterprises.

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to Housing GSEs is provided below.

2370. Does delegating aspects of its AML Program to a third party mean a Housing GSE will not be held responsible?

No. Any Housing GSE that delegates responsibility to a third party remains fully responsible for the effectiveness of its program and for ensuring that compliance examiners are able to obtain access to any information they need relating to the Housing GSE's AML/CFT Compliance Program.

2371. Are Housing GSEs subject to the CIP requirement pursuant to Section 326 of the USA PATRIOT Act?

No. Currently, Housing GSEs are not subject to the Customer Identification Program (CIP) requirement. For a listing of financial institutions subject to the CIP requirement at the time of this publication, please refer to Section 326 – Verification of Identification.

2372. Are Housing GSEs subject to the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) finalised in July 2016?

No. Only institutions subject to the CIP requirement are required to identify beneficial owners for legal entity customers under the Beneficial Ownership Rule. Housing GSEs are not subject to the CIP requirement and therefore are not required to identify beneficial owners. However, the Beneficial Ownership Rule also clarified existing AML/CFT expectations by including ongoing monitoring and updates as the fifth pillar of an AML Program. The requirements of the Beneficial Ownership Rule could be extended in the future. For further guidance, please refer to the Beneficial Owners section.

2373. Are Housing GSEs required to file CTRs?

No. Currently, Housing GSEs are not required to file Currency Transaction Reports (CTRs). They are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2374. Are Housing GSEs required to file SARs?

Yes. Housing GSEs are required to file SARs. For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2375. Are the SAR filing requirements for Housing GSEs the same as for other covered financial institutions?

Yes. Housing GSE SAR filing requirements (e.g., time frame for filing, dollar thresholds, confidentiality) are the same as those for banks. For additional guidance on SAR filing requirements, please refer to the Suspicious Activity Reports section.

2376. How does the SAR filing requirement impact existing suspicious activity reporting requirements of Housing GSEs?

Under the previous FHFA requirement, Housing GSEs filed reports of fraudulent activity with the FHFA. Where appropriate, the FHFA then filed SARs with FinCEN, based on the fraud reports submitted by the Housing GSEs. Under the final rule, SARs will be filed directly with FinCEN by the Housing GSE.

Additionally, Housing GSEs will have to report on financial crimes broader than fraud, including transactions conducted or attempted by, at or through a Housing GSE that aggregate to at least US$5,000, and that the Housing GSE knows, suspects or has reason to suspect that the transaction (or a pattern of transactions of which the transaction is a part):

- Involves funds derived from illegal activity or is intended or conducted to hide or disguise funds or assets derived from illegal activity (including, without limitation, the ownership, nature, source, location or control of such funds or assets) as part of a plan to violate or evade any federal law or regulation or to avoid any transaction reporting requirement under federal law or regulation;
- Is designed, whether through structuring or other means, to evade any reporting requirements under regulations promulgated by the BSA;
- Has no business or apparent lawful purpose or is not the sort in which the particular Housing GSE customer would normally be expected to engage, and the Housing GSE knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or
- Involves the use of the Housing GSE to facilitate criminal activity.

2377. Are Housing GSEs afforded the same "Safe Harbor" protection as other covered financial institutions?

Yes. Housing GSEs, as well as their directors, officers, employees and agents, are covered under the Safe Harbor provision. This is especially important for Housing GSEs because the "Safe Harbor" enables the uninhibited filing of SARs for types of activity to which the Housing GSEs may not be accustomed. For further guidance, please refer to the Safe Harbor section.

2378. Are Housing GSEs permitted to file a SAR jointly with another financial institution?

Yes. In instances where either a second Housing GSE or other covered financial institution is involved in a transaction or activity resulting in the filing of a SAR, only one report is required to be filed. The report should contain all of the facts pertaining to each institution's involvement, and each institution should maintain a copy of the SAR filed along with supporting documentation. For further guidance, please refer to the Third-Party and Joint Filings of SARs section.

2379. What are some of the statistics and trends in SAR filings for Housing GSEs?

According to FinCEN, out of 1.98 million SAR filings from January 1, 2016, through December 31, 2016, Housing GSEs filed over 2,300 SARs or 0.1 percent of all filings during this period:

- Eighty percent of SARs were filed on activity taking place in the District of Columbia;
- Forty-five percent of SARs were filed on borrowers, 26 percent on individuals with unknown/blank relationship type, 24 percent with a relationship of "other," and 2 percent on agents;
- Ninety-nine percent of SARs involved residential mortgages, 43 percent involved funds transfers 20 percent involved personal/business checks, 17 percent involved money orders, 13 percent involved bank/cashier's check and 7 percent involved U.S. currency;
- Top suspicious activity categories of SARs filed by housing GSEs included:
    - Mortgage Fraud: 84 percent

- Money Laundering: 8 percent
- Other Suspicious Activities: 5 percent (included 22 cases related to identity theft, and 3 cases related to unauthorised electronic intrusion
- Fraud: 2 percent (separate from Mortgage Fraud which accounted for less than 84 percent of SARs filed by housing GSEs)
- Structuring: 1 percent
- Terrorism/Terrorist Financing: 0 percent (0 cases)

2380. What are some examples of red flags with which Housing GSEs may be concerned?

Common red flags for mortgage-related products and services include, but are not limited to, the following:

- Customer is looking to conduct associated transactions (e.g., real estate purchases, down payments, fees, closing costs) in cash
- Borrower purchases property in the name of a nominee, such as an associate or a relative
- Borrower negotiates a purchase for market value or above asking price, but records a lower value on documents, paying the difference "under the table"
- Borrower sells property below market value with an additional "under the table" payment
- Borrower or agent of the borrower purchases property without much knowledge about the property inspection or does not appear sufficiently knowledgeable about the purpose or use of the real estate being purchased
- Borrower purchases multiple properties in a short period of time or appears to be buying and selling the same piece of real estate for no apparent legitimate purpose
- Seller requests that proceeds be sent to a high-risk jurisdiction or offshore bank
- Borrower makes payments with funds from a high-risk jurisdiction or offshore bank
- Borrower pays off the original loan with cash and/or significantly in advance of the expected terms of the loan

For additional guidance, please refer to the sections: Mortgage Fraud, Mortgage and Real Estate Red Flags and Lending Red Flags.

2381. Are Housing GSEs permitted to participate in the information-sharing provisions under Sections 314(a) and (b) of the USA PATRIOT Act?

Yes. Any financial institutions required to establish an AML Program under Section 352, including Housing GSEs, are obligated to comply with Section 314(a) information requests and may voluntarily participate in the information sharing mechanisms established by Section 314(b).

For further guidance, please refer to the sections: Section 314(a) – Cooperation Among Financial Institutions, Regulatory Authorities and Law Enforcement Authorities and Section 314(b) – Cooperation Among Financial Institutions.

2382. Are Housing GSEs required to comply with OFAC and other sanction laws and regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2383. Do Housing GSEs have additional cybersecurity-related obligations beyond OFAC's Cyber-Related Sanctions Program requirements?

Yes. OFAC's Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Housing GSEs can access designees from the Cyber-Related Sanctions Program on the Specially Designated Nationals (SDN) List under the program tag [CYBER].

In addition to filing SARs and reporting ongoing cyber-attacks to FinCEN via their hotline, several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:

- **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
- **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and
- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:

- Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);

- Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
- Detection of cybersecurity events;
- Response to identified or detected cybersecurity events to mitigate negative impact;
- Recovery from cybersecurity events and restoration to normal operations; and
- Fulfilment of regulatory reporting obligations.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2384. Should Housing GSEs address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the U.S. Securities and Exchange Commission (SEC) settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the personally identifiable information (PII) of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), housing GSEs can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Incidents and Cybersecurity Preparedness section.

2385. Who is responsible for examining Housing GSEs for compliance with AML/CFT laws and regulations?

The Federal Housing Financing Agency (FHFA) is responsible for examining Housing GSEs for compliance with AML/CFT laws and regulations. Housing GSEs are also subject to supervision by the Office of Federal Housing Enterprise Oversight (OFHEO) and the Federal Housing Finance Board (FHFB).

Nonfinancial Businesses

Key AML/CFT and Sanctions Requirements

2386. With which key AML/CFT and sanctions requirements are nonfinancial businesses required to comply?

Nonfinancial businesses, which include all businesses not included as a "financial institution" under the BSA, must comply with the following key AML/CFT requirements:

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)

- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)
- OFAC and other sanctions requirements

For additional guidance on the various AML/CFT requirements, please refer to the respective sections within the Bank Secrecy Act and USA PATRIOT Act sections. Additional guidance specific to nonfinancial businesses is provided below.

2387. Are nonfinancial businesses required to comply with OFAC and other sanction laws and regulations?

Yes. OFAC requirements and other sanctions imposed by the U.S. apply to U.S. citizens and permanent resident aliens, regardless of where they are located in the world, all persons and entities within the United States, and all U.S. incorporated entities and their foreign branches. For additional guidance on OFAC, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2388. Are nonfinancial businesses required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

No. At present, the AML Program requirement of the USA PATRIOT Act does not apply to nonfinancial institutions. However, some nonfinancial institutions have opted to implement an AML Program voluntarily to mitigate the institution's risk of being abused for money laundering or terrorist financing and preserve the institution's reputation.

2389. Are nonfinancial businesses required to file CTRs?

No. Currently, nonfinancial institutions are not required to file Currency Transaction Reports (CTRs). Nonfinancial institutions are, however, required to file Form 8300 for cash payments over US$10,000 received in a trade or business. For a listing of financial institutions required to file CTRs and Form 8300 at the time of this publication, please refer to the Currency Transaction Reports and Form 8300 sections.

2390. Are nonfinancial businesses required to file SARs?

While nonfinancial institutions are not currently obligated to file Suspicious Activity Reports (SARs), FinCEN encourages the voluntary filing of SARs on suspected money laundering and terrorist activity. There is a checkbox on Form 8300 for indicating that a transaction is potentially suspicious.

2391. Are there red flags for detecting potentially suspicious activity for nonfinancial businesses?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to transaction execution and high-risk products/services/transactions (e.g., cash, monetary instruments) has been provided in this publication. For further guidance on red flags, please refer to the Suspicious Activity Red Flags and Retail Red Flags sections.

2392. Are nonfinancial businesses required to comply with the information-sharing requirement of Section 314 of the USA PATRIOT Act?

No. Only those institutions required to establish an AML Program are obligated to comply with the information-sharing requirement of the USA PATRIOT Act. For further guidance, please refer to Section 314 – Cooperative Efforts to Deter Money Laundering.

2393. What types of nonfinancial businesses are at heightened risk for money laundering and terrorist financing?

Business types and occupations considered to be high risk for money laundering and terrorist financing include those that are cash-intensive; those that allow for the easy conversion of cash into other types of assets; those that provide opportunity to abuse authoritative powers and assist in disguising the illegal transfer of funds; those that lack transparency; those that involve international transactions/customers; and those that offer high-risk or high-value products. High-risk business types/occupations include, but are not limited to, the following:

- Accountants/accounting firms
- Aircraft engine/part and military armoured vehicle manufacturing
- Amusement, gambling and recreation activities
- Attorneys/law firms
- Art/antiques dealers
- Businesses owned or managed by politically exposed persons (PEPs) and political organisations
- Businesses that operate privately owned automated teller machines (ATMs)
- Car washes
- Charitable organisations/Nongovernmental organisations (NGOs)
- Cigarette distributors
- Common carriers of currency (e.g., armoured car services)
- Consumer electronics rentals and dealers
- Convenience stores
- Flight training
- Gas stations
- Importers/exporters
- Leather manufacturing, finishing and goods stores
- Liquor stores
- Marijuana-related businesses [MRBs]

- Notaries
- Offshore companies
- Parking garages
- Racetracks
- Restaurants/bars
- Retail establishments
- Small arms and ammunition manufacturing
- Tobacco wholesalers
- Transportation services and equipment rental
- Textile businesses
- Vending machine operators

Certain crimes, such as human trafficking may have their own high risk types/occupations. For further guidance, please refer to the Human Trafficking and Migrant Smuggling section.

2394. What are the benefits of voluntarily implementing an AML/CFT Compliance Program in a nonfinancial business?

Nonfinancial businesses increasingly are becoming involved in money laundering and terrorist financing schemes as it becomes more difficult for criminals to introduce illicit funds into the financial system. Law enforcement investigations that result from money laundering and terrorist financing allegations may damage an organisation's reputation. Therefore, beyond the legal and regulatory requirements noted above, nonfinancial businesses need to consider and take seriously the risk of being targeted or used for money laundering and terrorist financing, either by employees or outside parties.

While a nonfinancial business is not subject to the requirements of the USA PATRIOT Act to implement an AML Program, the existence of an AML/CFT Compliance Program for such an institution may help to mitigate the organisation's money laundering and terrorist financing risk and preserve the institution's reputation.

DRUG TRAFFICKING, TERRORISM, TERRORIST FINANCING, FRAUD AND OTHER REGULATORY TOPICS

Drug Trafficking

Basics

2395. What is drug/narcotics trafficking?

The United Nations (U.N.) defines "drug trafficking" as "a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws."

The Office of Foreign Assets Control (OFAC) defines "narcotics trafficking" as "any activity undertaken illicitly to cultivate, produce, manufacture, distribute, sell, finance or transport, or otherwise assist, abet, conspire, or collude with others in illicit activities relating to narcotic drugs, including, but not limited to, cocaine."

2396. Is drug trafficking a predicate offense to money laundering?

Yes. Racketeering activity (e.g., any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter or dealing in a controlled substance or listed chemical as defined by the Controlled Substances Act [CSA]), which is chargeable under state law and punishable by imprisonment for more than one year, is one type of crime underlying money laundering and terrorist financing activity in the United States, consistent with FATF Recommendations.

2397. What is the current scale of drug trafficking and drug use?

Measuring the current scale of drug trafficking is extremely difficult. The World Drug Report (2016), published by the U.N. Office on Drugs and Crime (UNODC), provided the following statistics on global drug use:

- **Drug Trafficking (i.e., cultivation, production, manufacturing, distributing, selling)**
  - 129 countries reported cultivation of cannabis (most trafficked drug worldwide)
  - 49 countries reported cultivation of opium poppy (Afghanistan accounted for two-thirds of the global area under illicit opium poppy cultivation)
  - 7 countries reported cultivation of coca
  - 2.2 million drug seizure cases were reported to the UNODC in 2014
- **Drug Use**
  - 1 in 20 adults aged 15 to 64 years (250 million people) used one drug in 2014
    - 183 million used cannabis

        - 33 million used opiates and prescription opioids
        - Many used more than one drug, referred to as "polydrug users"
    - Nearly 30 million drug users suffer from drug use disorders
    - Over 200,000 drug-related deaths occurred in 2014, primarily from drug overdoses

2398. What are some key terms related to drug trafficking and drug prohibition?

The following are some of the key terms related to drug trafficking and drug prohibition defined by various regulatory, federal and law enforcement authorities:

- **Controlled substances (CS) –** Defined by CSA as a "drug or other substance, or immediate precursor, included in Schedule I, II, III, IV or V of Part B of [the CSA]. The term does not include distilled spirits, wine, malt beverages, or tobacco, as those terms are defined or used in Subtitle E of the Internal Revenue Code of 1986." Substances not included in the CSA are generally referred to as **non-controlled substances (NCS)**;
    - Scheduled Listed Chemical Products (SLCPs) – Defined by the DEA as follows:
        - "Contains ephedrine, pseudoephedrine, phenylpropanolamine; and
        - May be marketed or distributed lawfully in the United States under the Federal Food, Drug and Cosmetic Act as a nonprescription drug."
- **Deliver (or Delivery)** – Defined by the CSA as "the actual, constructive, or attempted transfer of a controlled substance or a listed chemical, whether or not there exists an agency relationship."
- **Dispense** – Defined by the CSA as a "means to deliver a controlled substance to an ultimate user or research subject by, or pursuant to the lawful order of, a practitioner, including the prescribing and administering of a controlled substance and the packaging, labelling or compounding necessary to prepare the substance for such delivery. The term "dispenser" means a practitioner who so delivers a controlled substance to an ultimate user or research subject."
- **Distribute** – Defined by the CSA as a "means to deliver (other than by administering or dispensing) a controlled substance or a listed chemical. The term 'distributor' means a person who so delivers a controlled substance or a listed chemical."
- **Diversion** – Defined by the Centers for Disease Control (CDC) as the theft of drugs by healthcare personnel, for personal or third-party use/sale.
- **Drug** – Defined by the CSA as follows:
        - "Articles recognised in the official United States Pharmacopoeia, official Homoeopathic Pharmacopoeia of the United States, or official National Formulary, or any supplement to any of them;
        - Articles intended for use in the diagnosis, cure, mitigation, treatment, or prevention of disease in man or other animals;

- Articles (other than food) intended to affect the structure or any function of the body of man or other animals; and
- Articles intended for use as a component of any article specified in [the aforementioned]."

– **Narcotic Drug** – Defined by the CSA as "any of the following whether produced directly or indirectly by extraction from substances of vegetable origin, or independently by means of chemical synthesis, or by a combination of extraction and chemical synthesis:

- Opium, opiates, derivatives of opium and opiates, including their isomers, esters, ethers, salts, and salts of isomers, esters, and ethers, whenever the existence of such isomers, esters, ethers, and salts is possible within the specific chemical designation. Such term does not include the isoquinoline alkaloids of opium.
- Poppy straw and concentrate of poppy straw.
- Coca leaves, except coca leaves and extracts of coca leaves from which cocaine, ecgonine, and derivatives of ecgonine or their salts have been removed.
- Cocaine, its salts, optical and geometric isomers, and salts of isomers.
- Ecgonine, its derivatives, their salts, isomers, and salts of isomers.
- Any compound, mixture, or preparation which contains any quantity of any of the substances referred to [in the aforementioned]."

– **Amphetamines –** Defined by the UNODC as "a group of amphetamine-type stimulants that includes amphetamine and methamphetamine."

– **Cannabis** – Also referred to as "marijuana" or "marihuana," and defined by the CSA as "all parts of the plant Cannabis Sativa L., whether growing or not; the seeds thereof; the resin extracted from any part of such plant; and every compound, manufacture, salt, derivative, mixture, or preparation of such plant, its seeds or resin. Such term does not include the mature stalks of such plant, fibre produced from such stalks, oil or cake made from the seeds of such plant, any other compound, manufacture, salt, derivative, mixture, or preparation of such mature stalks (except the resin extracted therefrom), fibre, oil, or cake, or the sterilised seed of such plant which is incapable of germination."

– **Cocaine** – See above definition of "narcotic drug";

– **Crack cocaine –** Defined by the UNODC as "cocaine base obtained from cocaine hydrochloride through conversion processes to make it suitable for smoking."

– **Opiates** – Defined by the CSA as a "drug or other substance having an addiction-forming or addiction-sustaining liability similar to morphine or being capable of

conversion into a drug having such addiction-forming or addiction-sustaining liability."

- **Opioids** – Defined by the UNODC as "a generic term applied to alkaloids from opium poppy (opiates), their synthetic analogues (mainly prescription or pharmaceutical opioids) and compounds synthesised in the body."
- **New Psychoactive Substances (NPSs)** – Also referred to as "**synthetic drugs**" and defined by the UNODC as "substances of abuse, either in a pure form or preparation, that are not controlled under the Single Convention on Narcotic Drugs of 1961 of the [1971 convention], but that may pose a public health threat. [N]ew does not necessarily refer to new inventions but to substances that have recently become available."
- **Counterfeit Drug** – Defined by the CSA as a "drug which, or the container or labelling of which, without authorisation, bears the trademark, trade name, or other identifying mark, imprint, or device, or any likeness thereof, of a drug manufacturer, processor, packer or distributor other than the person or persons who in fact manufactured, processed, packed, or distributed such drug and which thereby falsely purports or is represented to be the product of, or to have been packed or distributed by, such other drug manufacturer, processor, packer or distributor."

2399. Which drugs pose the greatest threat in the world?

The U.N.'s World Drug Report (2016) provides statistics on the trafficking and use of drugs world-wide. Below are a few highlights of four drugs with the highest perceived threat:

- **Opiates**
  - 17 million users of opium, morphine and heroin in 2014
  - Global surge in heroin users, particularly in North America over the previous decade
  - 75 percent of global opium seizures in 2014 were reported by the Republic of Iran
- **Cocaine**
  - Nearly 19 million users of cocaine in 2014, up from 14 million in 1998
  - Between 2007 and 2014, the number of heavy/regular cocaine users declined while the number of recreational users rose in North America
  - Global cocaine manufacturing peaked in 2007 with global cocaine output in 2014 at approximately 25 percent lower than 2007 levels
- **Cannabis**
  - The percentage of global users of cannabis has remained stable since 1998, at 3.8 percent of the population

- Most users of cannabis herb were located in the Americas followed by Africa; most users of cannabis resin were located in Europe, North Africa and the Near and Middle East
- Most cannabis herb was cultivated in the Americas, followed by Africa; most cannabis resin was produced in Morocco and Afghanistan
- In 2014, 75 percent of cannabis herb seizures occurred in the Americas, 14 percent in Africa, 5 percent in Europe
- Since the legalisation of cannabis in some parts of the United States, while the number of cannabis-related arrests and court cases have declined, recent data has shown an increase in recreational use and public health and safety indicators (e.g., emergency room visits, traffic accidents)

- **Synthetic Drugs** (e.g., amphetamine-type stimulants [ATS], new psychoactive substances [NPS])
  - More than 170 tons of ATSs (e.g., ecstasy, methamphetamine) were seized in 2014, predominantly in North America, East Asia and Southeast Asia
  - Nearly 70 new NPSs were reported to the UNODC in 2014, predominantly synthetic cannibinoids (32 tons mostly in North America out of 34 global tons seized in 2014; of which 26.5 tons were in the United States) followed by synthetic cathinones, synthetic opioids (e.g., fentanyl derivatives) and synthetic sedatives (e.g., benzodiazepines)

2400. Which drugs pose the greatest threat in the United States?

The National Drug Threat Assessment (NDTA) Report (2016) provides statistics on the trafficking and use of drugs in the United States. Below are a few highlights of seven drugs with the highest perceived threat:

- **Controlled Prescription Drugs (CPDs)**
  - Number of recent deaths involving CPDs outpaced the combined deaths involving cocaine and heroin.
  - Most recent number of CPD users was more than the combined users for cocaine, heroin, methamphetamine, 3-4-methylenedioxymethamphetamine (MDMA) (also known as Molly, Ecstasy, E) and phencyclidine (PCP).
  - Examples of top distributed CPDs include hydrocodone, oxycodone, amphetamine, methylphenidate, methadone, morphine and codeine.

- **Heroin**
  - Primary source of heroin for the U.S. market is Mexico followed by South America.
  - Although there were 10 times as many CPD users than heroin users, heroin was deadlier as overdoses from CPDs were only twice that of heroin-involved deaths.

- Heroin-involved deaths are highest in the Northeast and Midwest of the United States.

- **Fentanyl**
  - A Schedule II synthetic opioid manufactured in China and possibly in Mexico
  - Both diverted pharmaceutical fentanyl and illicitly manufactured fentanyl are abused; however, the non-pharmaceutical fentanyl is responsible for more overdoses and deaths.
  - Despite public health announcements of the lethality of fentanyl, some users specifically seek heroin laced with fentanyl to maximise the high; some traffickers have been known to manipulate the production of fentanyl to make it appear like heroin.
  - Example fentanyl brand names included Ghost, Get Right, and El Chapo.

- **Methamphetamine**
  - Primary source of methamphetamine is Mexico.
  - As a synthetic drug, there are multiple "routes" to manufacturing methamphetamine; manufacturers often adapt production methods as supplies for specific precursors (e.g., pseudoephedrine) fluctuate due to the passage of laws like the Combat Methamphetamine Epidemic Act (CMEA) of 2006 that regulated over-the-counter sales of ephedrine, pseudoephedrine and phenylpropanolamine products, precursors for manufacturing methamphetamine.
  - Conversion laboratories are designed to convert "powder methamphetamine" or to reconstitute "methamphetamine in solution" (a common concealment method) to crystal methamphetamine. In 2015, nearly 80 percent of seized conversion laboratories were located in California.

- **Cocaine**
  - [According to U.N. World Drug Report (2016), it is the second most used illicit drug in the United States and globally, after marijuana].
  - Primary source of cocaine is Colombia.
  - Trend emerging of cocaine mixed with fentanyl.
  - The use of privately-owned vehicles is the primary method of smuggling cocaine from Mexico into the United States.
  - While not common, "cocaine in solution" is a method of concealment that has proven difficult to detect as the "parent" liquid masks the colour and smell of the cocaine.

- **Marijuana**

- Most commonly used illicit drug in the United States [and globally, according to the U.N. World Drug Report (2016)].
- The DEA has denied multiple petitions to remove marijuana as a Schedule I drug under the CSA because marijuana has a high potential for abuse and does not meet the criteria of accepted medical use in treatment in the United States.
- Three types of marijuana markets operate differently: illicit markets, state-approved medical marijuana markets and state-approved personal use/recreational markets. Drug traffickers have moved into legal markets to grow marijuana to divert to illicit markets.
- Marijuana soaked in PCP is known as "wet", "dip set" or "dips."

- **New Psychoactive Substances (NPS)**
  - NPS refers to man-made drugs created to mimic controlled substances. The most common NPSs include synthetic cannabinoids (mimic marijuana) and synthetic cathinones (mimics drugs like MDMA; also referred to as "bath salts").
  - NPS providers often create altered chemical variations that have not yet been scheduled under the CSA to circumvent the law.
  - Some users prefer NPSs as some drug tests cannot detect synthetic drugs.
  - Final processing laboratories for synthetic cannabinoids are referred to as "spice processing labs."

2401. What aspects of the "drug problem" should laws attempt to address beyond drug trafficking?

As stated in the U.N.'s World Drug Report (2016), efforts to address drug trafficking should also address the following to develop a comprehensive and systematic approach to eradicate the world's drug problem consistent with several of the U.N.'s Sustainable Development Goals (SDGs):

- Access to controlled substances (e.g., prescription medication) and diversion programs;
- Drug abuse prevention and treatment programs;
- Impact of stigma of drug use disorders on those who seek out medical care and the impact on receiving quality care from healthcare professionals;
- Alternative measures to conviction and sentencing for select drug-related offenses;
- Illicit crop cultivation and environmental impact due to deforestation and pollution related to the growth of crops for illicit drug production;
- Associated crimes with drug traffickers (e.g., robbery, assault, murder) and drug users (e.g., violence against families and communities, health impact, especially Human Immunodeficiency Virus [HIV] infection rates of those who inject drugs);
- Relationship to terrorist financing and funding of other violent extremism; and

- Use of emerging technologies (e.g., "dark net") to enable drug trafficking.

2402. What are the key U.S. drug trafficking and drug-prohibition laws and regulations?

The following are key U.S. federal drug trafficking and drug-prohibition laws and regulations:

- **Controlled Substances Act (CSA) (1970)** – The CSA consolidated many of the more than 50 laws relating to the control and diversion of drugs enacted between 1914 and 1970.
- **Anti-Drug Abuse Act (1986)** – Also referred to as the **Omnibus Drug Enforcement, Education and Control Act of 1986,** this law sought "to strengthen Federal efforts to encourage foreign cooperation in eradicating illicit drug crops and in halting international drug traffic, to improve enforcement of Federal drug laws and enhance interdiction of illicit drug shipments, to provide strong Federal leadership in establishing effective drug abuse prevention and education programs, to expand Federal support for drug abuse treatment and rehabilitation efforts, and for other purposes."
- **Violent Crime Control and Law Enforcement Act of 1994** – Also referred to as the Crime Control Bill, this law amended the Omnibus Crime Control and Safe Streets Act of 1968 "to allow grants to increase police presence, to expand and improve cooperative efforts between law enforcement agencies and members of the community to address crime and disorder problems, and otherwise to enhance public safety." The "three strikes" sentencing law was part of this act, which imposed "mandatory life imprisonment without possibility of parole for Federal offenders with three or more convictions for serious violent felonies or drug trafficking crimes."
- **Foreign Narcotics Kingpin Designation Act (Kingpin Act) (1999)** – The Kingpin Act applies sanctions to designated persons involved in international narcotics trafficking as recommended by the Secretary of the Treasury, the Attorney General, the Secretary of State, the Secretary of Defense, the Director of the Central Intelligence Agency (CIA), the Department of Homeland Security and the Directorate of National Intelligence.
- **Drug Addiction Treatment Act of 2000** (DATA 2000) – DATA increased the number of patients doctors could treat for heroin and other opiate addictions with the medication buprenorphine from 30 to 100. The initial threshold was established to curb potential abuse.
- **National All Schedules Prescription Electronic Reporting** (NASPER) **Act** (2005) – NASPER established a controlled substance monitoring program in each state (e.g., Prescription Drug Monitoring Program [PDMP]) that assists practitioners detect potential abuse of prescription drugs by patients and diversion of illicitly obtained prescription drugs.
- **Combat Methamphetamine Epidemic Act (CMEA)** (2005) – Passed as Title VII of the USA PATRIOT Improvement and Reauthorisation Act of 2005, the CMEA was a law that regulated retail over-the-counter (OTC) sales of ephedrine, pseudoephedrine, and phenylpropanolamine products. Retail provisions included daily sales limits and 30-day purchase limits, placement of product out of direct customer access, sales logbooks, customer ID verification, employee training, and self-certification of regulated sellers.

2403. What key international treaties and conventions have influenced or shaped U.S. drug trafficking and drug prohibition laws?

The United States adopted several international treaties, conventions and resolutions including, but not limited to, the following:

- **United Nations Single Convention on Narcotic Drugs** (1961)
- **United Nations Convention on Psychotropic Substances** (1971)
- **United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances** (1988) (Vienna Convention)
- **United Nations Convention Against Transnational Organised Crime** (2000) (Palermo Convention)

2404. What factors determine the severity of a particular drug threat?

The severity of the threat of a particular drug can be estimated based on factors including, but not limited to, the following:

- Overdoses
- Addictions
- Deaths
- Age of victims
- Drug sales volume
- Costs associated with associated healthcare costs and impact on society
- Costs associated with counter-drug trafficking efforts
- Associated violent crimes
- Perception by law enforcement (e.g., conflicting federal and state marijuana laws)

2405. What is drug scheduling?

The Controlled Substances Act (CSA) of 1970 categorised drugs, chemicals and substances into five schedules based on the following factors:

- Potential for abuse
- Accepted medical use with or without medical supervision
- Degree of psychological or physical dependence

Descriptions and examples for each of the five schedules are provided below.

- **Schedule I Substances**
    - Drug, chemical or substance with the following characteristics:

- High potential for abuse;
- No currently accepted medical use in treatment in the United States; and
- Lack of accepted safety for use of the drug or other substance under medical supervision.
- **Examples**: Heroin, marijuana (cannabis), lysergic acid diethylamide (LSD), peyote, mescaline, methylenedioxyamphetamine (MDA) (also known as Sally, Sassafras, Sass), 3-4-methylenedioxymethamphetamine (MDMA) (also known as Molly, Ecstasy, E).

- **Schedule II Substances**
  - Drug, chemical or substance with the following characteristics:
  - High potential for abuse;
  - Has a currently accepted medical use in treatment in the United States or a currently accepted medical use with severe restrictions; and
  - Abuse may lead to severe psychological or physical dependence.
  - **Examples**: Opium, opiate, opium poppy, poppy straw, morphine, codeine, methadone, meperidine (Demerol), cocaine, oxycodone (Percodan), anileridine (Lertine), oxymorphine (Numorphan), amphetamine (Dexedrine), methamphetamine (Desoxyn), phenmetrazine (Preludine), methylphenidate (Ritalin); amobarbital, pentobarbital, secobarbital; and fentanyl (Sublimaze), etorphine hydrochloride, phencyclidine (PCP).
- **Schedule III Substances**
  - Drug, chemical or substance with the following characteristics:
  - Potential for abuse less than Schedule I and Schedule II substances;
  - Has a currently accepted medical use in treatment in the United States; and
  - Abuse may lead to moderate or low psychological or high physical dependence.
  - **Examples**: Amphetamine, phenmetrazine, methylphenidate, lysergic acid, methyprylon, sulfondiethylmethane, nalorphine.
- **Schedule IV Substances**
  - Drug, chemical or substance with the following characteristics:
  - Lower potential for abuse relative to Schedule III substances;
  - Has a currently accepted medical use in treatment in the United States; and
  - Abuse may lead to limited psychological or physical dependence relative to Schedule III substances.

- **Examples**: Ambien, barbital, phenobarbital, methylphenobarbital, chloral hydrate, ethchlorvynol (Placidyl), ethinamate, (Valmid), chlordiazepoxide (Librium), diazepam (Valium), oxazepam (Serax), clorazepate (Tranxene), flurazepam (Dalmane), lorazepam (Ativan), alprazolam (Xanax), temazepam (Restoril), triazolam (Halcion), mebutamate, dextropropoxyphene (Darvon), petazocine (Talwin).

- **Schedule V Substances**
  - Drug, chemical or substance with the following characteristics:
  - Lower potential for abuse relative to Schedule IV substances;
  - Has a currently accepted medical use in treatment in the United States; and
  - Abuse may lead to limited psychological or physical dependence relative to Schedule IV substances.
  - **Examples**: Buprenorphine, drugs generally used for antidiarrheal, antitussive and analgesic purposes such as cough preparations with less than 200 milligrams of codeine (Robitussin AC), Motofen, Lyrica, Parepectollin.

2406. What is the DEA's "five factor test" to determine if a drug can be deemed as having an "accepted medical use"?

57 Federal Register 10499 (1992) outlines the following five factors:

- The drug's chemistry must be known and reproducible;
- There must be adequate safety studies;
- There must be adequate and well-controlled studies proving efficacy;
- The drug must be accepted by qualified experts; and
- The scientific evidence must be widely available.

2407. Who is authorised to dispense controlled substances?

"Practitioners" are authorised to dispense controlled substances. The CSA defines "practitioner" as a "physician, dentist, veterinarian, scientific investigator, pharmacy, hospital, or other person licensed, registered, or otherwise permitted, by the United States or the jurisdiction in which he practices or does research, to distribute, dispense, conduct research with respect to, administer, or use in teaching or chemical analysis, a controlled substance in the course of professional practice or research."

2408. How can drug seekers obtain prescription drugs without a prescription?

The DEA provided the following examples of methods used by drug seekers to illegally obtain prescription drugs:

- Prescription forgery
- Doctor shopping

- Theft (from a family member or friend)
- Burglary/robbery of pharmacies (directly or indirectly through an employee who is a family member or friend)

2409. Is diversion of prescription drugs a significant problem in the United States?

Diversion is a significant threat as it prevents patients from receiving their medication and places them at additional risk with compromised medical personnel who utilise diverted drugs for themselves.

The DEA established the Diversion Division to investigate "physicians who sell prescriptions to drug dealers or abusers; pharmacists who falsify records and subsequently sell the drugs; employees who steal from inventory and falsify orders to cover illicit sales; prescription forgers; and individuals who commit armed robbery of pharmacies and drug distributors."

The DEA publishes actions taken against DEA registrants, including but not limited to, the following:

- **Criminal Cases Against Doctors** is a listing of "investigations of physician registrants in which the DEA was involved that resulted in the arrest and prosecution of the registrant."
- **Registrant Actions** - Administrative Actions Against Registrants from 2000 to the present.

2410. How are practitioners monitored for potentially illicit activity?

Practitioners are required to register with the DEA and are subject to ongoing monitoring. The DEA conducts regular investigations into DEA registrants who may be violating the CSA and may revoke registrations, and if warranted, bring civil and criminal charges against a registrant.

2411. What are Prescription Drug Monitoring Programs (PDMPs)?

Implemented by the NASPER Act, Prescription Drug Monitoring Programs (PDMPs), also known as Prescription Monitoring Programs (PMSs), are defined by the National Alliance for Model State Drug Laws (NAMSDL) as "statewide electronic database[s] which collect designated data on substances dispensed in the state. The PDMP is housed by a specified statewide regulatory, administrative or law enforcement agency. The housing agency distributes data from the database to individuals who are authorised under state law to receive the information for purposes of their profession."

2412. Are PDMPs required to share prescription data with other states?

While they are not required to share prescription data with other states, several initiatives have been implemented to encourage information exchange:

- The Bureau of Justice Assistance (BJA), the Alliance of States with Prescription Monitoring Programs (ASPMP) and other partners established the Prescription Drug Monitoring Information Exchange (PMIX) Architecture; and
- The National Association of Boards of Pharmacy (NAPB) created a secure system called InterConnect for participating PDMPs to voluntarily exchange information.

2413. Who are the primary targets in counter-drug trafficking efforts?

Many law enforcement agencies target the drug-trafficking system and its leaders as opposed to low-level dealers. Targets include, but are not limited to, the following:

- **Transnational Criminal Organisations (TCO)** – OFAC defines TCOs as a group of persons that "engages in an ongoing pattern of serious criminal activity involving the jurisdictions of at least two foreign states; and threatens the national security, foreign policy or economy of the United States."
- **Drug Cartels** – Defined by the U.S. Department of Justice as "large, highly sophisticated organisations composed of multiple DTOs [drug trafficking organisations] and cells with specific assignments such as drug transportation, security/enforcement, or money laundering. Drug cartel command-and-control structures are based outside the United States; however, they produce, transport, and distribute illicit drugs domestically with the assistance of DTOs that are either a part of or in an alliance with the cartel."
- **Drug Trafficking Organisations (DTOs)** – Defined by the DOJ as "complex organisations with highly defined command-and-control structures that produce, transport, and/or distribute large quantities of one or more illicit drugs."
- **Kingpin** – Generally refers to the leaders or significant members of a criminal organisation. Under OFAC's Counter Narcotics Trafficking Sanctions Program, kingpins are tagged with [SDNTK].
- **Gang** – Defined by the DEA as "three or more individuals, whose members collectively use a group identity of a common name, slogan, tattoo, style or colour of clothing, or hand sign. The purposes of their association are to engage in criminal activity and use violence or intimidation to further their criminal objectives."
    - **Street Gang –** Defined by the DEA as "criminal organisations that form at a local level; vary in membership, race and structure."
        - "**Neighbourhood-based gangs** are confined to a specific neighbourhood and jurisdiction with no known leadership beyond their communities."
        - "**National-level gangs** typically have a presence in multiple jurisdictions, large membership numbers and scores of members who migrate throughout the country. [They] usually identify by a common name and tattoo, hand signs and some form of structure that includes by-laws."
    - **Prison Gang** – Defined by the DEA as a "criminal organisation that originates in the penal system and continues to operate within correctional facilities throughout the United States. Prison gangs are self-perpetuating criminal entities that also continue their operations outside of prison."
    - **Outlaw Motorcycle Gang (OMG) –** Defined by the DEA as an "ongoing organisation, association, or group of three or more persons with a common interest or activity characterised by the commission of, or involvement in, a pattern of

criminal conduct. Members must possess and be able to operate a motorcycle to achieve and maintain membership within the group."

2414. What are some examples of TCOs, DTOs and gangs?

The National Drug Threat Assessment (NDTA) (2016) provides details on key TCOs operating in the United States including, but not limited to, the following:

- Organisation and Characteristic
- Collaboration with Other TCOs
- Operational Structure in the United States
- Drug Smuggling and Transportation Methods
- Other Criminal Activity
- Communication Methods
- Rural Expansion

The NDTA provides an overview of TCOs with the most activity in the United States. Examples include, but are not limited to, the following:

- **Mexican TCOs**
  - **Primary Drugs Trafficked**: Heroin, methamphetamine, cocaine, marijuana and to a lesser extent fentanyl
  - **Mexican TCO Examples**:
    - Sinaloa Cartel
    - Jalisco New Generation Cartel (CJNG)
    - Juarez Cartel
    - Beltran-Leyva Organisation
- **Colombian TCOs**
  - **Primary Trafficked Drugs**: Cocaine, heroin
  - **Colombian TCO Examples**:
    - Fuerzas Armadas Revolucinarios de Colombia (FARC) (also designated as a foreign terrorist organisation [FTO] under OFAC's Terrorism Sanctions Program)
    - Gulf Clan (previously known as Clan Usuga)
    - Los Rastrojos
- **Dominican TCOs**
  - **Primary Trafficked Drugs**: Cocaine, heroin, prescription drugs

  - **Dominican TCO Examples**: Small organisations consisting of family members and close associates

- **Asian TCOs**
  - **Primary Trafficked Drugs**: Marijuana (indoor grow houses), 3-4-methylenedioxymethamphetamine (MDMA, also known as Molly, ecstasy, E) and to a lesser extent, cocaine and methamphetamine
  - **Asian TCO Examples**: Organisations often recruit Asian Americans to blend into immigrant communities primarily on the East and West Coasts

- **Street Gangs**
  - **Primary Trafficked Drugs:** Depends on relationship with particular TCO/cartel
  - **Street Gang Examples**:
    - Tango Blast and Tango Cliques
    - Aryan Brotherhood Texas
    - Barrio Azteca
    - Latin Kings
    - Mara Salvatrucha (MS-13) (also designated as a TCO under OFAC's Transnational Criminal Organisation Sanctions Program)

- **Outlaw motorcycle gangs (OMGs)**
  - **Primary Trafficked Drugs**: Methamphetamine, cocaine and marijuana
  - **OMG Examples**:
    - Hell's Angels
    - Bandidos
    - Phantoms
    - Pagans

Many of these groups engage in other types of criminal activity in addition to drug trafficking, including, but not limited to, the following:

- Assault
- Murder
- Robbery
- Auto theft
- Kidnapping
- Cybercrime

- Human trafficking
- Sex trafficking
- Weapons trafficking

2415. What is a High Intensity Drug Trafficking Area (HIDTA)?

Financial HIDTAs were authorised in the Anti-Drug Abuse Act of 1988 to assist law enforcement with concentrating its efforts with drug control at the federal, state and local levels. HIDTAs are designated by area. Since the original designation of five HIDTAs in 1990, the program has expanded to 28 areas of the country which include nearly 20 percent of all counties in the United States and over 60 percent of the U.S. population. These include, but are not limited to, the following:

- Transaction Appalachia (e.g., counties in Tennessee, Kentucky, Virginia and West Virginia)
- New York/New Jersey
- Rocky Mountain (e.g., counties in Colorado, Utah, Wyoming and Montana)
- South Florida
- Southwest Border (e.g., southern regions of California, Arizona, New Mexico and Texas)

Funding for HIDTAs has faced some challenges under the Trump administration, as the White House Office of Management and Budget (OMB) has called the program duplicative with other federal programs (e.g., Drug-Free Communities [DFC]). However, funding was ultimately provided, as many officials argued for the need for these federal programs during the country's opioid crisis.

For further guidance on HIDTAs, please refer to the Risk Assessments section.

2416. What is the relationship between drug trafficking and terrorist financing?

Terrorist organisations use multiple methods to raise funds for their operations, including drug trafficking. The following provides additional insight into the interrelationship between drug trafficking and terrorist financing:

- **United Nation's "Digest of Terrorist Cases"** – Explores the relationship between terrorism and other forms of crime (e.g., corruption, narcotics trafficking, organised crime, using minor offences to catch major criminals, false identity and immigration offences)
- **FATF's Financial Flows Linked to the Production and Trafficking of Afghan Opiates (2014) –** Provides an overview of Afghanistan's dominance in the global opiate market (of US$68 billion, US$60 billion was from Afghan opiates in 2011) and how designated terrorist organisations such as the Afghan Taliban use the proceeds from drug trafficking to fund their operations and terrorist acts.

For further guidance on terrorist financing, please refer to the Terrorism and Terrorist Financing section.

2417. What are some examples of international anti-drug trafficking initiatives?

Begun in 2008, the Merida Initiative is a partnership between the United States and Mexico to combat organised crime. Activities under the Merida Initiative include, but are not limited to the following:

- Training of Mexican personnel (e.g., police, investigators, prosecutors, defence counsel) in support of justice sector reforms;
- Establishment of anti-corruption and whistleblowing programs;
- Delivery of equipment and trained canines to detect illicit goods at checkpoints and ports of entry;
- Establishment of cross-border telecommunications systems between U.S. and Mexico sister cities;
- Support for Mexican prisons to achieve independent accreditation from the American Correctional Association (ACA); and
- Establishment of Drug Treatment Courts across multiple Mexican states as an alternative to incarceration for drug abusers.

2418. How does the Financial Action Task Force (FATF) address drug trafficking?

In 1990, FATF drafted its original Recommendations to combat the laundering of drug money. Since then, the Recommendations have been updated four times, in 1996, 2001, 2003 and 2012.

- FATF Recommendation 3 – Money Laundering Offence suggests countries criminalise money laundering based on the following conventions:
- United Nations Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (1988) (Vienna Convention)
- United Nations Convention Against Transnational Organised Crime (2000) (Palermo Convention)

"Illicit trafficking in narcotic drugs and psychotropic substances" and "participation in an organised criminal group and racketeering" are listed by FATF as designated categories of offence.

For further guidance, please refer to Financial Action Task Force section.

2419. Are drug traffickers and terrorists the primary focus of AML/CFT laws?

While they are a major focus, AML/CFT laws are also concerned with all types of criminal activity as indicated by the comprehensive list of predicate crimes outlined by FATF and the United States. This includes, but is not limited to, the following criminal activity:

- Proliferators of WMDs
- Corrupt senior foreign political figures (senior foreign political figures are also known as politically exposed persons [PEPs])
- Human traffickers and migrant smugglers
- Sanctions evaders

For more guidance on predicate crimes, please refer to the Financial Action Task Force section.

2420. What are some examples of significant drug trafficking cases in the United States?

Following are examples of significant drug trafficking cases in the United States:

- In May 2015, the DEA announced a four-state enforcement action, called Operation Pilluted, the largest single pharmaceutical operation case in law enforcement history. Operation Pilluted resulted in nearly 300 arrests, including 22 doctors and pharmacists, in Arkansas, Alabama, Louisiana and Mississippi. The DEA targeted pill mills (e.g., doctors prescribing for non-medical purposes, illicit pharmacies) and seized drugs, more than 50 vehicles, 200+ weapons, more than US$11 million in cash and nearly US$7 million in real property.
- In January 2017, Joaquín Archivaldo Guzmán Loera, better known as El Chapo, kingpin of the Sinaloa Cartel, the world's largest drug trafficking organisation, was extradited from Mexico to the United States to face multiple charges, including drug trafficking, murder, criminal conspiracy, firearms violations and money laundering in multiple states (e.g., California, New York, Texas) spanning multiple decades. El Chapo allegedly trafficked cocaine, heroin, methamphetamine and marijuana. New York's indictment includes a notice of criminal forfeiture related to all charges in the amount of US$14 billion, representing illegal proceeds from El Chapo's narcotics trafficking activities.

2421. What are some examples of red flags for detecting drug trafficking?

A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires, monetary instruments, insurance) has been provided in this publication. Drug trafficking red flags include, but are not limited to, the following:

- Customer with an excessive number of individual accounts
- A common mobile number, address and/or employment references that are used to open multiple accounts under different names
- Cash deposits conducted by multiple unrelated third parties
- Cash deposits that smell like marijuana
- High volume of transactions with businesses or individuals located in different states or countries
- Excessive payments made to the business owner, manager or employees
- Designee or close associate of designee under OFAC's Counter Narcotics Trafficking Sanctions Program

For additional examples, please refer to the Transaction Monitoring, Investigations and Red Flags section.

2422. What key guidance and resources have been provided related to drug trafficking and drug-related activity?

The following key guidance and resources have been provided related to drug trafficking and drug-related activity:

- **Drug Enforcement Administration (DEA)** – Established in 1973, the DEA is the lead agency for domestic enforcement of federal drug laws.
  - The mission of the **Diversion Control Division** "is to prevent, detect, and investigate the diversion of controlled pharmaceuticals and listed chemicals from legitimate sources while ensuring an adequate and uninterrupted supply for legitimate medical, commercial, and scientific needs."
  - The DEA runs multiple programs to conduct chemical analysis of drugs in the United States to determine the geographic origin, purity and synthetic routes, including, but not limited to, the following:
    - Heroin Signature Program (HSP) and the Heroin Domestic Monitoring Program (HDMP)
    - Methamphetamine Profiling Program (MPP)
    - Cocaine Signature Program (CSP)
    - Potency Monitoring Program (PMP) (marijuana)
  - Publications issued by the DEA include, but are not limited to, the following:
    - Controlled Substances Security Manual
    - National Drug Threat Assessment (NDTA)
    - National Heroin Threat Assessment Summary
    - U.S. Areas of Influence of Major Mexican Transnational Criminal Organisations
    - Practitioner's Manual: A Guideline to the Practitioner's Responsibilities under the Controlled Substances Act of 1970 (2006)
    - Mid-Level Practitioner's Manual: An Informational Outline of the Controlled Substances Act of 1970 (1993)
    - Pharmacist's Manual: An Informational Outline of the Controlled Substances Act of 1970 (2010)
    - A Pharmacist's Guide to Prescription Fraud
    - Pharmacy Robbery & Burglary: Tips to Protect Your Customers, Your Business and Yourself
    - How Sick People Get Their Medicines: A Primer for Children of All Ages
    - Narcotic Treatment Programs: Best Practice Guideline (2000)

        - Chemical Handler's Manual: A Guide to Chemical Control Regulations (2013)
        - A Security Outline of the Controlled Substances Act of 1970 (1991)
        - Policy Statement: Dispensing Controlled Substances for the Treatment of Pain (2006)
        - Guidance Regarding Petitions for Religious Exemption from the Controlled Substances Act Pursuant to the Religious Freedom Restoration Act (2009)

- **Federal Bureau of Investigation (FBI)** – Established in 1908, the FBI is a national security organisation tasked with protecting against terrorism, espionage, cyber attacks and major criminal threats.
    - The **National Gang Report (NGR)** is a report of current gang activities in the United States published by the National Alliance of Gang Investigators' Associations (NAGIA) and the FBI's Safe Streets and Gang Unit (SSGU)
- **National Gang Intelligence Center (NGIC)** – Established in 2005, the NGIC is a multi-agency center created to provide support to law enforcement as it relates to gangs. The NGIC includes members from the FBI, DEA, ATF, Federal Bureau of Prisons (BOP), United States Marshals Service (USMS), Department of Defense (DOD) and the U.S. Customs and Border Patrol (CBP). In addition to administering several data warehouses (e.g., Gang Encyclopedia; Signs, Symbols and Tattoo Database; Gang Terms Dictionary; Intelligence Library; Gang Training and Events Calendar), the NGIC periodically publishes the National Gang Report (NGR).
- **U.S. Department of Health & Human Services (HHS)** – Established in 1953, HHS is tasked with protecting the health of Americans through the provision of numerous health and welfare-related programs (e.g., Medicare, Medicaid). The HHS is also responsible for regulating food products and new pharmaceutical drugs. HHS includes, but is not limited to the following:
    - Food & Drug Administration (FDA)
    - Centers for Disease Control (CDC)
    - National Institutes of Health (NIH)
    - National Institute on Drug Abuse (NIDA)
    - Substance Abuse & Mental Health Service Administration (SAMHSA)
        - Center for Substance Abuse Treatment (CSAT)
        - Division of Pharmacologic Therapies (DPT)
- **Office of National Drug Control Policy (ONDCP)** – Created by the Anti-Drug Abuse Act of 1988, within the executive office of the U.S. President, the ONDCP provides oversight of the U.S. anti-drug program. The primary goals of the **National Drug Control Strategy** are to reduce illegal drug use, drug manufacturing and trafficking, drug-related crime and violence and drug-related health consequences.

- **U.S. Bureau of Alcohol, Tobacco and Firearms (ATF)** – Established in 1972, the ATF is a law enforcement agency within the DOJ tasked with protecting against the illegal use and trafficking of firearms, the illegal use and storage of explosives, acts of arson and bombings, acts of terrorism and the illegal diversion of alcohol and tobacco products.
- **U.S. Department of State**
  - The **Bureau of International Narcotics and Law Enforcement Affairs (INL)**, established in 1978, combats transnational crime (e.g., money laundering, cybercrime, intellectual property theft, trafficking in goods, people, weapons and drugs) that impacts the United States, by assisting foreign governments develop effective law enforcement institutions.
  - The **International Narcotics Control Strategy Report (INCSR)** is an annual report that describes the efforts to attack, country by country, all aspects of the international drug trade, as well as chemical control, money laundering and financial crimes.
- **Financial Crimes Enforcement Network (FinCEN)**
  - Information on Narcotics and Bulk Currency Corridors (2011)
  - BSA Expectations Regarding Marijuana-Related Businesses (2014)
  - Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML (2014)
  - Update on U.S. Currency Restrictions in Mexico (2012)
  - Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency (2010)
  - Guidance to Financial Institutions on the Repatriation of Currency Smuggled into Mexico from the United States (2006)
  - Black Market Peso Exchange Update (1999)
  - Combating Transnational Organised Crime (2011)
- **National Alliance for Model State Drug Laws (NAMSDL)** is a nonprofit funded by U.S. congressional appropriations that provides research and analysis of state statutes, policies and regulations as well as model drug laws to assist local, state and federal stakeholders in implementing comprehensive and effective drug and alcohol laws, policies, regulations and programs. Some publications released by NAMSDL include, but are not limited to, the following:
  - Marijuana: Comparison of State Laws Allowing Use for Medicinal Purposes (2015, 2017)
  - Marijuana: Comparison of State Laws Legalizing Personal, Non-Medical Use (2016)
  - Marijuana: Laws Allowing the Limited Use of Low-THC for Medicinal Purposes (2015)

  - The Legalization of Marijuana in Colorado: Volume 2 (2014)
  - Prescription Drug Misuse, Abuse and Addiction in the United States (2014)
  - Mandated Use of State Prescription Drug Monitoring Programs: Highlights of Key State Requirements (2016)
  - State Prescribing and Dispensing of Controlled Substances Profiles (2015)
  - Model Prescription Monitoring Program (PMP) Act (2015)

- **United Nations Office on Drugs and Crime (UNODC)** – Established in 1997, the UNODC assists member states to combat illicit drugs, crime and terrorism.
  - The **UNODC Annual Report (World Drug Report)** (2007, 2008, 2009, 2010, 2014) is an annual report that provides an overview of major developments in drug markets related to production, trafficking, consumption and impact on health. Covered drugs included opiates, cocaine, cannabis and amphetamines (including ecstasy).
  - Additional drug-related resources and publications issued by the UNODC include, but are not limited to, the following:
    - The Afghan Opiate Trade Project (AOTP)
    - Individual Drug Seizure (IDS) Reports
    - Price and Purity of Drugs
    - Illicit Crop Monitoring

- **Financial Action Task Force (FATF)** – Established in 1989, FATF is an intergovernmental policy-making body composed of more than 30 countries whose purpose is to establish and promote international legislative and regulatory standards in the areas of money laundering, terrorist financing and other related threats; and to monitor members' progress in adhering to these standards. Drug-related publications issued by FATF include, but are not limited to, the following:
  - Financial Flows Linked to the Production and Trafficking of Afghan Opiates (2014)

- Additional organisations providing key guidance on drug trafficking and drug use include, but are not limited to, the following:
  - International Narcotics Control Board (INCB)
  - National Association of State Controlled Substances Authorities (NASCSA)
  - National Council for Prescription Drug Programs (NCPDP)
  - Prescription Drug Monitoring Program Training and Technical Assistance Center (PDMP TTAC)
  - Federation of State Medical Boards (FSMB)

- National Association of Boards of Pharmacy (NABP)
- American Society in Pharmacy Standards (ASAP)
- American Society of Interventional Pain Physicians (ASIPP)
- Society of Interventional Pain Management Surgery Centers (SIPMS)
- North American Neuromodulation Society (NANS)

Cannabis-Related Businesses

2423. Are cannabis-related businesses legal?

Marijuana is a Schedule I controlled substance under the CSA, making it illegal under federal law to manufacture, import, possess, use and distribute certain substances. However, numerous states have legalised certain marijuana-related activities. According to the Office of National Drug Control Policy (ONDCP), state-level marijuana-related laws have ranged from legalising marijuana for medicinal uses to decriminalising marijuana (e.g., reducing penalties of existing laws to civil penalties) to legalising marijuana for recreational use.

2424. How many states have passed or proposed legalising marijuana-related activities?

According to the ONDCP, at the time of this publication, more than 20 states have passed legislation legalising marijuana-related activities for medical purposes and nearly 10 states have legalised marijuana for recreational use.

2425. What countries have passed or proposed decriminalising marijuana-related activities?

The following are examples of countries that have, at least partially, decriminalised marijuana for medicinal or recreational use:

- Australia
- Canada
- Czech Republic
- India
- Iran
- France
- North Korea
- Mexico

2426. Are there red flags for detecting unlicensed marijuana-related businesses [MRBs]?

Yes. A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires,

monetary instruments, insurance) has been provided in this publication. Marijuana-related activity red flags include, but are not limited to, the following:

- To detect unlicensed marijuana-related activities of existing customers:
  - Business unable to provide state license;
  - Business unable or refuses to demonstrate legitimate source of funds of account activity or other investment(s);
  - Business deposits currency that smells like marijuana;
  - Excessive payments made to owners or employees;
  - Frequent inter-state transactions with third parties (e.g., customers, vendors, suppliers) in high-risk jurisdictions (e.g., located in or near states that have legalised marijuana-related activities, high intensity drug trafficking areas [HIDTAs]);
  - Business is located on federal property or in close proximity to a school in violation of federal and state laws;
  - Marijuana sold by the business was grown on federal property in violation of federal law; and
  - Searches of publicly available sources reveal business owners, employees or other related parties are involved in the illegal purchase of drugs, violence or other criminal activity or have been subject to sanctions for violations of state or local marijuana-related laws.

For additional examples of red flags, please refer to the Transaction Monitoring, Investigations and Red Flags section. For further guidance on MRBs, please refer to the Marijuana-Related Businesses section.

2427. What guidance has been provided to address the conflicting federal and state marijuana-related laws?

Multiple petitions and laws have been proposed on the federal and state-level to resolve the conflict by decriminalising marijuana on a federal level, rescheduling marijuana for medical use, providing protection to financial institutions when providing financial services to marijuana-related businesses, allowing for the creation of banking cooperatives by marijuana-related businesses or by granting states the power to regulate the industry themselves, similar to alcohol. Examples include, but are not limited to, the following:

- **Ending Federal Marijuana Prohibition Act of 2013**
- **States' Medical Marijuana Patient Protection Act** (2013)
- **Respect State Marijuana Laws Act of 2013**
- **Marijuana Businesses Access to Banking Act of 2013**
- **Legitimate Use of Medicinal Marijuana Act** (2014)

- **Colorado House Bill 14-1398 – Concerning the Provision of Financial Services to Licensed Marijuana Businesses**
- **Regulate Marijuana Like Alcohol Act (H.R.1013)** (2015)
- **Consolidated Appropriations Act** (2017)

Under the Obama administration, the U.S. Department of Justice (DOJ) also issued two memoranda highlighting enforcement priorities as they relate to marijuana-related activities under federal law, specifically the CSA:

- **Memorandum for All United States Attorneys: Guidance Regarding Marijuana Enforcement (Cole Memo)** (August 2013)
- **Memorandum for All United States Attorneys: Guidance Regarding Marijuana Related Financial Crimes** (February 2014)

The Cole Memo included eight priorities covering public safety, public health and other law enforcement priorities:

- Preventing the distribution of marijuana to minors;
- Preventing revenue from the sale of marijuana from going to criminal enterprises, gangs, and cartels;
- Preventing the diversion of marijuana from states where it is legal under state law in some form to other states;
- Preventing state-authorised marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity;
- Preventing violence and the use of firearms in the cultivation and distribution of marijuana;
- Preventing drugged driving and the exacerbation of other adverse public health consequences associated with marijuana use;
- Preventing the growing of marijuana on public lands and the attendant public safety and environmental dangers posed by marijuana production on public lands; and
- Preventing marijuana possession or use on federal property.

The 2014 DOJ memorandum provided guidance on the impact on financial crimes for which marijuana-related activities are predicate crimes. Persons found to violate any of the enforcement priorities outlined by the Cole Memo could be prosecuted under the following money laundering statutes:

- **Prohibition on engaging in financial and monetary transactions with proceeds from a specified unlawful activity (SUA) pursuant to 18 U.S.C 1956 and 1957**;
- **The unlicensed money transmitter statute pursuant to 18 U.S.C. 1960**; and

- **Reporting of financial transactions involving marijuana-related violations of the CSA pursuant to the BSA**.

As with the money laundering offense, prosecution under the aforementioned offenses does not require conviction on an underlying marijuana-related crime under federal or state law.

Under the Trump administration, in a May 2017 letter addressed to the U.S. Congress, Attorney General Jefferson B. Sessions III indicated his desire to enforce the Controlled Substances Act (CSA) against medical marijuana growers and distributers, regardless of each state's marijuana laws.

2428. What guidance has been issued related to the marijuana-related industry?

The following, though not intended to be all inclusive, lists key resources and guidance that have been issued on the marijuana-related industry:

- **National Alliance for Model State Drug Laws (NAMSDL)** is a nonprofit funded by U.S. congressional appropriations that provides research and analysis of state statutes, policies and regulations as well as model drug laws to assist local, state and federal stakeholders in implementing comprehensive and effective drug and alcohol laws, policies, regulations and programs. Some publications released by NAMSDL include, but are not limited to, the following:
  - **Marijuana: Comparison of State Laws Allowing Use for Medicinal Purposes** (2015, 2017)
  - **Marijuana: Comparison of State Laws Legalizing Personal, Non-Medical Use** (2016)
  - **Marijuana: Laws Allowing the Limited Use of Low-THC for Medicinal Purposes** (2015)
- **The Legalization of Marijuana in Colorado: Volume 2** (2014) by the Marijuana Resource Center administered by the Office of National Drug Control Policy (ONDCP) of the United States Government provides the following resources:
  - Answers to Frequently Asked Questions About Marijuana
  - State Laws Related to Marijuana
  - The Public Health Consequences of Marijuana Legalization
- **BSA Expectations Regarding Marijuana-Related Businesses** (2014) by Financial Crimes Enforcement Network (FinCEN)
- **Frequently Asked Questions: Marijuana and Banking** (2014) by the American Bankers Association (ABA)
- **Memorandum for All United States Attorneys: Guidance Regarding Marijuana Enforcement** (2013) (also known as the "Cole Memo") by the Department of Justice (DOJ) Deputy Attorney General James M. Cole

- **Memorandum for United States Attorneys: Guidance Regarding the Ogden Memo in Jurisdictions Seeking to Authorise Marijuana for Medical Use** (2011) by the DOJ Deputy Attorney General James M. Cole
- **Memorandum for Selected United States Attorneys: Investigations and Prosecutions in States Authorizing the Medical Use of Marijuana** (2009) (also known as the "Ogden Memo") by the DOJ Deputy Attorney General David. W. Ogden
- **Medical Marijuana: Review and Analysis of Federal and State Policies** (2010) by the U.S. Congressional Research Service's Mark Eddy, Specialist in Social Policy

Additional key guidance and resources on drugs and various aspects of the drug trade include, but are not limited to, the following:

- **World Drug Report** – An annual report by the United Nations Office on Drugs and Crime (UNODC) that provides an overview of major developments in drug markets related to production, trafficking, consumption and impact on health. Covered drugs included opiates, cocaine, cannabis and amphetamines (including ecstasy).
- **International Narcotics Control Strategy Report (INCSR)** – An annual report issued by the U.S. Department of State that describes over 200 countries' efforts to combat the international drug trade, money laundering and financial crimes. Highlighted groups involved in domestic and multilateral efforts to combat drug trafficking and money laundering include, but are not limited to, the following:
    - Office of Overseas Prosecutorial Development, Assistance and Training
    - Asset Forfeiture and Money Laundering Section
    - FinCEN
    - Internal Revenue Service, Criminal Investigative Division (IRS-CI)
    - United Nations Global Programme Against Money Laundering, Proceeds of Crime and the Financing of Terrorism
    - The Organisation of American States Inter-American Drug Abuse Control Commission Group of Experts to Control Money Laundering

OFAC Counter Narcotics Sanctions Program and Transnational Criminal Organisation Sanctions Program – Sanctions programs administered by OFAC that block the property and interests of persons designated as significant narcotics traffickers and transnational criminal organisations.

Impact on Financial Institutions

2429. What are the obligations of financial institutions as they relate to drug trafficking?

Financial institutions are obligated to implement the following measures as they relate to drug trafficking:

- Design and conduct risk assessments that address high-risk jurisdictions such as HIDTAs and bulk currency corridors;
- Design and implement due diligence program that identifies high-risk customers including authorised providers of controlled substances (e.g., pharmacies, MRBs);
- Design and implement suspicious activity monitoring program tailored to identify all types of illicit drug activity (e.g., drug traffickers, illicit pharmacies, non-compliant state-sponsored MRBs);
- File Suspicious Activity Reports (SARs) on potentially suspicious drug-related activity (e.g., inclusion of "Marijuana Limited," "Marijuana Priority" and "Marijuana Termination" in SAR narratives, as appropriate);
- Notify law enforcement if potentially suspicious activity is ongoing; and
- Implement OFAC Sanctions Programs which require screening transactions and customers against lists including, but not limited to, the following:
    - Established by the Foreign Narcotics Kingpin Designation Act (Kingpin Act) (1999), International Emergency Economic Powers Act (IEEPA) (1977), National Emergencies Act (NEA) (1976) and Executive Order 12978 – Blocking Assets and Prohibiting Transactions with Significant Narcotics Traffickers (1995), the **Counter Narcotics Trafficking Sanctions Program** blocks the property and property interests of specially designated individuals and entities involved in significant narcotics trafficking in Colombia or other significant foreign narcotics traffickers, or that materially assist in, or provide financial or technological support for, or goods or services in support of, the narcotics trafficking activities. The program tags for designees under the Counter Narcotics Trafficking Sanctions Program on the Specially Designated National (SDN) List are as follows:
        - Specially Designated Narcotics Traffickers (SDNT)
        - Specially Designated Narcotics Traffickers – Kingpins (SDNTK)
        - Blocked Pending Investigation, Foreign Narcotics Kingpin (BPI-SDNTK)

For further guidance, please refer to the Counter Narcotics Trafficking Sanctions Program section.

- Established by IEEPA, NEA and Executive Order 13581 – Blocking Property of Transnational Criminal Organisations (2011), OFAC's **Transnational Criminal Organisations (TCO) Sanctions Program** blocks the property and property interests of individuals and entities determined to be significant transnational criminal organisations or to have provided material support for, or to be owned or controlled by, or to have acted on behalf of such organisations. The Executive Order states that the activities of the listed transnational criminal organisations threaten the stability of international political and economic systems and constitute an unusual and extraordinary threat to the national security, foreign policy and economic interests of the United States. The program tag for designees under the Transnational Criminal Organisations Sanctions program on the SDN List is [TCO].

Terrorism and Terrorist Financing

Basics

2430. What is "terrorism"?

18 United States Code (USC) § 2331 defines domestic and international terrorism separately:

- **Domestic terrorism** is defined as activities that:
  - "[I]nvolve acts dangerous to human life that are a violation of the criminal laws of the United States or of any State;
  - [A]ppear to be intended—
    - [T]o intimidate or coerce a civilian population;
    - [T]o influence the policy of a government by intimidation or coercion; or
    - [T]o affect the conduct of a government by mass destruction, assassination, or kidnapping; and
  - [O]ccur primarily within the territorial jurisdiction of the United States."
- **International terrorism,** sometimes referred to as transnational terrorism, is defined as activities that:
  - "[I]nvolve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State;
  - [A]ppear to be intended:
    - [T]o intimidate or coerce a civilian population;
    - [T]o influence the policy of a government by intimidation or coercion; or
    - [T]o affect the conduct of a government by mass destruction, assassination, or kidnapping; and
  - [O]ccur primarily outside the territorial jurisdiction of the United States, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to intimidate or coerce, or the locale in which their perpetrators operate or seek asylum."

2431. Is "home-grown terrorism" another term for "domestic terrorism"?

"Home-grown terrorism" typically refers to those perpetrators who have become radicalised by joining a terrorist organisation in a foreign country such as Pakistan or Afghanistan, and returning to their home countries to commit acts of terror. Home-grown terrorism typically does not include terrorism committed by citizens of the United States, either as a lone actor or on behalf of domestic terror groups, even if committed acts of terrorism took place in the United States.

2432. Are there published lists of terrorists?

The **Counter Terrorism Sanctions Program,** administered by the Office of Foreign Assets Control (OFAC), blocks the property and property interests of individuals, entities and regimes involved in terrorism-related activities, including countries that have been designated as state sponsors of terrorism. The program tags for designees under the Counter Terrorism Sanctions Program on the Specially Designated Nationals (SDN) List are as follows:

- Specially Designated Terrorists (SDT)
- Specially Designated Global Terrorists (SDGT)
- Foreign Terrorist Organisations (FTO)

Many other countries and the United Nations (UN) maintain lists of sanctioned persons and entities involved in terrorism-related activities and financial crimes as well (e.g., UN Consolidated List, European Union [EU] Consolidated List, Bank of England [BOE] List, Hong Kong Monetary Authority [HKMA] List).

For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2433. What are "foreign terrorist organisations"?

"Foreign terrorist organisations" (FTOs) are groups designated by the U.S. Secretary of State as being engaged in terrorist activities. Currently, there are nearly 60 organisations designated as FTOs, including, but not limited to, the following:

- Al-Qaeda (AQ) (1999)
- Al-Qaeda in the Islamic Maghreb (AQIM) (2002)
- Al-Qaeda in the Arabian Peninsula (AQAP) (2010)
- Boko Haram (2013)
- Hamas (1997)
- Hizballah (1997)
- Mujahidin Shura Council in the Environs of Jerusalem (MSC) (2014)
- Real Irish Republican Party (RIRA) (2001)
- Revolutionary Armed Forces of Colombia (FARC) (1997)
- Tehrik-e Taliban Pakistan (TTP) (2010)
- Hilal Ahmar Society Indonesia (Indonesia) (2014)
- Al-Furqan Foundation Welfare Trust (Al-Furqan) (2015)
- Al-Rahmah Welfare Organisation (RWO) (Pakistan) (2016)

2434. What are "state sponsors of terrorism"?

"State sponsors of terrorism" are countries that have repeatedly provided support for acts of international terrorism as designated by the U.S. Secretary of State. Currently, there are three countries that have been designated as state sponsors of terrorism:

- Iran (1984)
- Sudan (1993)
- Syria (1979)

Rescinded designations included:

- Cuba (Designated in 1982; removed in 2015)
- Iraq (Designated in 1979; removed in 2004)
- Libya (Designated in 1979; removed in 2006)
- North Korea (Designated in 1988; removed in 2008; possible re-designation in 2017)
- South Yemen (Designated in 1979; removed in 1990)

2435. Who has the authority to designate an individual, organisation or state as a "terrorist"?

In the United States, multiple parties are responsible for identifying terrorism-related threats and make recommendations to the Treasury Department for ultimate designation as a terrorist, including, but not limited to, the following:

- **U.S. State Department**
  - The U.S. State Department publishes a press release on its website, Terrorism Designations Press Release, with each new designation of a terrorist or terrorist organisation pursuant to Executive Order 13224 - Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism (September 2001). The full list of designations is administered by OFAC on the SDN List under the Counter Terrorism Sanctions Program.
- **Federal Bureau of Investigation's** (FBI) Most Wanted Lists
  - The FBI publishes multiple "Most Wanted" lists including "Most Wanted Terrorists" which includes people who have been charged with federal crimes in the United States (e.g., Conspiracy to Kill U.S. Nationals, Use Weapons of Mass Destruction Against U.S. Nationals, Bombing Resulting in Death, Attempted Murder of Federal Employees).

Outside of the United States, the Security Council of the United Nations is empowered to take enforcement measures to maintain or restore international peace and security under Chapter VII of its charter. One such enforcement measure is the imposition of sanctions, including economic and trade sanctions, arms embargoes, travel bans, and other financial or diplomatic restrictions. The Security Council has imposed sanctions on individuals and organisations through a variety of resolutions; each

list is maintained by the relevant Security Council Committee. Examples include the Al-Qaida Sanctions List, Taliban Sanctions Lists, and resolutions related to the proliferation of weapons of mass destruction [WMDs]. For further guidance, please refer to the section, Office of Foreign Assets Control and International Sanctions Programs.

2436. What organisations make up the Intelligence Community (IC) of the United States?

The Intelligence Community (IC) includes, but is not limited to the following:

- Air Force Intelligence, Surveillance and Reconnaissance (ISR)
- Central Intelligence Agency (CIA)
- Coast Guard Intelligence (CGI)
- Defense Intelligence Agency (DIA)
- Bureau of Intelligence and Research (INR) (U.S. Department of State)
- Federal Bureau of Investigations (FBI) (U.S. Department of Justice [DOJ])
- Marine Corps Intelligence (U.S. Marines)
- Military Intelligence Corps (U.S. Army)
- National Geospatial-Intelligence Agency
- National Reconnaissance Office (NRO)
- National Security Agency (NSA)
- Office of the Director of National Intelligence (DNI)
- Office of Intelligence and Analysis (I&A) (U.S. Department of Homeland Security [DHS])
- Office of Intelligence and Analysis (OIA) (U.S. Department of the Treasury)
- Office of Intelligence and Counterintelligence (U.S. Department of Energy [DOE])
- Office of National Security Intelligence (Drug Enforcement Administration [DEA])
- Office of Naval Intelligence (U.S. Navy)

2437. Is the Pentagon considered a part of the Intelligence Community (IC)?

The Pentagon is the headquarters of the Department of Defense, which includes the uniformed services (e.g., Air Force, Army, Coast Guard, Marine Corps, National Guard, Navy) and many other departments and agencies including, but not limited to some members of the IC.

2438. What are some foreign equivalents of U.S. IC members?

Like the United States, other countries have multiple IC members. Foreign examples include, but are not limited to, the following:

- Military Intelligence Section 6 (MI6) (United Kingdom)

- Canadian Security Intelligence Service (CSIS) (Canada)
- National Intelligence Center (CNI) (Mexico)
- Ministry of State Security (MSS) (China)
- Dirección General De Inteligencia (DGI) (Cuba)
- Agência Brasileira de Inteligência (ABIN)
  Brazilian Intelligence Agency (Brazil)
- General Intelligence Directorate (Gihaz El Mukhabarat El 'Amma) (Egypt)
- Institute for Intelligence and Special Operation (HaMossad leModiʿin uleTafkidim Meyuḥadim [Mossad]) (Israel)
- Bundesnachrichtendienst (BND) (Germany)
- Federal Security Bureau of Russian Federation (FSB) (Russia)
- Australian Secret Intelligence Service (ASIS) (Australia)
- Direction Generale De La Securite Exterieure (DGSE) (France)
- Inter-Service Intelligence (ISI) (Pakistan)
- Iraqi Intelligence Service (IIS) (Iraq)
- Ministry of Intelligence and Security (MOIS) (Iran)
- National Directorate of Security (NDS) (Afghanistan)
- National Intelligence Agency (NIA) (Nigeria)
- Research and Analysis Wing (RAW) (Republic of India)
- Ministry of State Security (MSS) (Democratic People's Republic of Korea [DPRK], North Korea)
- National Intelligence Service (NIS) (Republic of Korea [ROK], South Korea)

2439. How are attacks classified as "terrorist attacks"?

While the media may report an incident as a "terrorist attack," in the United States, the FBI must review preliminary evidence before pursuing a case as if it were a "terrorist attack."

2440. Who has claimed responsibility for most of the terrorist attacks globally and in the United States?

According to the Global Terrorism Index: Measuring and Understanding the Impact of Terrorism (GTI) (2016), published by the Institute for Economics & Peace, the worst year for terrorism was 2014, with 32,765 killed. The second worst year occurred in 2015 with 29,376 killed.

- **Globally:** Of the 274 known terrorist groups, approximately 74 percent of terrorist attacks were attributed to the following:

  - Islamic State of Iraq and the Levant (ISIL), also known as Daesh, and its affiliates (active in almost 30 countries including Syria and Iraq; responsible for 6,141 deaths)
  - Boko Haram (active in countries such as Nigeria, Niger, Cameroon and Chad; responsible for 5,478 deaths)
  - Taliban (active in countries such as Afghanistan and Pakistan; responsible for 4,502 deaths)
  - Al-Qaeda (active in countries such as Iraq, Syria and Yemen; responsible for 1,620 deaths)
- **United States:** Since 2006, 98 percent of terror-related deaths were committed by lone actors, resulting in 156 deaths.

2441. What is the global economic impact of terrorism?

According to the GTI, the global economic impact of terrorism was US$89.6 billion in 2015, which was equivalent to approximately 1 percent of the total global economic impact of violence of US$13.6 trillion. Of the US$89.6 billion, economic resources allocated to peacekeeping and peacebuilding account for approximately 2 percent.

2442. What types of violence have had a greater impact than terrorism?

According to the GTI, major armed conflicts and homicides have resulted in more deaths and destruction to economies than terrorism.

2443. What is "countering-violent extremism (CVE)"?

According to the Fact Sheet: The White House Summit on Countering Violent Extremism (2015), countering-violent extremism (CVE) is a public-private partnership to "develop community-oriented approaches to counter hateful extremist ideologies that radicalise, recruit or incite to violence."

According to the GTI, terrorist acts occurred more frequently in countries with the following characteristics:

- State-sponsored terrorism (e.g., extra-judicial deaths, torture, imprisonment without trial)
- Violent (or armed) conflict (e.g., war)
- Poor socio-economic factors (e.g., lack of opportunities for youth, lack of confidence in the electoral system, high levels of criminality, access to weapons)

2444. How has social media been used by terrorists?

Social media (e.g., Twitter, Facebook, YouTube) has been used by terrorists in the following manner:

- Direct solicitation through social media coupled with a payment mechanism (e.g., person-to-person payment platforms, crowdfunding platform)
- Spread propaganda

2445. What are some examples of types of terrorist acts?

Many terrorist attacks involve bombs and result in the loss of life. Terrorist attacks can, however, include multiple types of other threats and weapons, aimed at destruction of life and property, including, but not limited to the following:

- Malware
- Guns
- Vehicles (e.g., trucks, airplanes)

2446. What is the Global Terrorism Database (GTD)?

The Global Terrorism Database (GTD) is a database with annual updates of more than 150,000 domestic and international terrorist events from 1970 through 2015. The GTD is administered by the National Consortium for the Study of Terrorism and Responses to Terrorism (START) program at the University of Maryland with support from the Center for Terrorism and Intelligence Studies (CETIS) and the U.S. Department of Homeland Security (DHS).

2447. What is the Global Terrorism Index (GTI)?

Developed by the Institute for Economics and Peace (IEP), the Global Terrorism Index (GTI) is a publication that provides a summary of global trends and patterns in terrorism and ranks countries based on the "impact of terrorism," using data from the GTD. Each country is assigned a composite GTI score from 0 (zero impact) to 10 (highest impact). The GTI (2016) listed the following six countries as having the highest impact of terrorism with scores greater than eight:

- Iraq (9.96)
- Afghanistan (9.444)
- Nigeria (9.314)
- Pakistan (8.613)
- Syria (8.587)
- Yemen (8.076)

Over 30 countries had a GTI score of "0," including, but not limited to, the following:

- Cuba (0)
- Haiti (0)
- North Korea (0)
- Panama (0)
- Singapore (0)

The United States had a GTI score of 4.877, ranking 36th out of over 160 countries, similar to the United Kingdom (5.08), Israel (5.248), Saudi Arabia (5.404), France (5.603) and Palestine (5.659).

2448. What criteria are used to calculate the GTI score?

According to the GTI report, the GTI score utilises the following four factors:

- Total terrorist incidents in a given year
- Total fatalities caused by terrorists in a given year
- Total injuries caused by terrorists in a given year
- Total property damage from terrorist incidents in a given year (e.g., less than US$1 million, between US$1 million and US$1 billion, greater than US$1 billion)

Fatalities had the greatest weighting with additional five-year weighted averages applied to "reflect the latent psychological effect of terrorist acts over time."

Terrorist incidents were included based on the following criteria:

- Intentional (i.e., the result of a conscious calculation on the part of a perpetrator);
- Entail some level of violence or threat of violence (e.g., property damage, violence against people); and
- Perpetrators are subnational actors (not acting on behalf of the state).

Terrorist Financing Basics

2449. What is terrorist financing?

Terrorist financing is a financial crime that uses funds to support the agenda, activities or cause of a terrorist organisation in addition to terrorist attacks. The funds raised may be from legitimate sources, such as charitable organisations or donations from supporters, as well as criminal sources, such as the drug trade, weapons smuggling, fraud, kidnapping and extortion for illegal activities.

2450. What are some common methods of terrorist financing?

According to the National Terrorist Financing Risk Assessment (2015), major funding sources of terrorist organisations such as ISIL, al-Qaeda and Boko Haram include, but are not limited to, the following:

- Kidnapping for ransom
- Private donations, solicited directly or indirectly through charitable organisations;
- Extortion of the population and resources in controlled territory;
- Revenue from legitimate businesses located in controlled territory;
- Illicit revenue from criminal activities (e.g., smuggling, narcotics trafficking); and
- State sponsorship.

2451. Is terrorist financing considered a predicate crime for money laundering in the United States?

Yes. Terrorist financing is a predicate crime for money laundering in the United States, consistent with Financial Action Task Force (FATF) Recommendations.

2452. What are the primary methods of disrupting terrorist financing?

According to the National Terrorist Financing Risk Assessment (2015), two primary methods of disrupting terrorist financing are:

- Sanctions
- Forfeiture

2453. What is the Terrorist Finance Tracking Program (TFTP)?

Following the terrorist activity on September 11, 2001, the U.S. Department of Treasury established the Terrorist Finance Tracking Program (TFTP) to identify, track and pursue terrorists by conducting targeted searches on data provided by SWIFT. The U.S. Department of Treasury submits subpoenas to the U.S. and European operating centres of SWIFT for financial messaging data related to specific terrorism investigations.

2454. What is the National Terrorist Financing Risk Assessment Report?

The National Terrorist Financing Risk Assessment Report was first published by the Office of Terrorist Financing and Financial Crimes (TFFC) in 2015. The report included three main sections:

- Global Terrorist Financing Threat
- Countering Terrorist Financing [efforts by law enforcement, financial and international community]
- Terrorist Financing Risks and Vulnerabilities in the United States

Highlights from the report, include, but are not limited to, the following areas of focus:

- Residual TF risks in the charitable sector;
- Use of online communication networks (e.g., social media) to directly solicit support and funds;
- Nontraditional value transfer systems (e.g., money services businesses [MSBs], unlicensed money transmitters);
- Cross-border cash smuggling operations;
- Cybercrimes (e.g., identity theft) to raise funds;

2455. Is the financing of weapons of mass destruction or the trafficking of arms considered terrorism/terrorist financing?

If the proliferator or trafficker is a terrorist, financing weapons of mass destruction (WMDs) or arms trafficking could be considered a type of terrorist financing. However, not all proliferators or traffickers are terrorists; therefore the development of measures to prevent, suppress and disrupt the

proliferation and financing of WMDs and arms trafficking, distinct from terrorist financing, is necessary.

Many countries have implemented non-proliferation measures to combat money laundering and terrorist financing.

2456. What is the difference between money laundering and terrorist financing?

In contrast to money laundering, which involves the disguising of funds derived from illegal activity so they may be used without detection of the illegal activity, terrorist financing can involve the use of legally derived money to carry out illegal activities. The objective of money laundering is financial gain or the hiding or disguising of illicit proceeds, whereas with terrorism, the objective is to promote the agenda or cause of the terrorist organisation. For example, it is widely believed that the terrorist activities of September 11, 2001, were partially financed by legally obtained funds that had been donated to charities. Both money launderers and terrorists, however, do need to disguise the association between themselves and their funding sources.

2457. Are the stages of terrorist financing the same as money laundering?

In general, yes, however, in the placement phase, funds could be derived from both legitimate and illegal activities. The methods of layering to disguise the source of funds are the same with money laundering and terrorist financing. In the integration phase, funds are typically disbursed to the terrorist or terrorist organisation, directly or indirectly through a third party to obscure the beneficiary and the ultimate objective of supporting a terrorist act.

2458. Are drug traffickers and terrorists the primary focus of AML/CFT laws?

While they are a major focus, AML/CFT laws are also concerned with all types of criminal activity as indicated by the comprehensive list of predicate crimes outlined by FATF and the United States. This includes, but is not limited to, the following criminals:

- Proliferators of WMDs
- Corrupt senior foreign political figures (senior foreign political figures are also known as politically exposed persons [PEPs])
- Human traffickers and migrant smugglers
- Sanctions evaders

Key Counter Terrorism and CFT Laws and Guidance

2459. What are the key U.S. counter terrorism and CFT laws and regulations?

The following are key U.S. federal terrorism-related laws and regulations:

- **Trading With the Enemy Act (TWEA)** (1917), amended a number of times, including but not limited to the International Emergency Economic Powers Act (IEEPA) Enhancement Act (2007), prohibits trade with enemies or allies of enemies and authorises the president of the United States to declare a national emergency, regulate domestic and international commerce during time of war

and national emergencies, and activate existing statutory provisions to address the threat to national security.

- **International Emergency Economic Powers Act (IEEPA)** (1977), amended by the IEEPA Enhancement Act (2007), authorised the president to regulate commerce after declaring a national emergency in response to an unusual and extraordinary threat to the United States which has a foreign source. It further authorises the president, after such a declaration, to block transactions and freeze assets to deal with the threat. In the event of an actual attack on the United States, the president can also confiscate property connected with a country, group or person who aided in the attack.
- **National Emergencies Act (NEA)** (1976), limits open-ended states of national emergency and formalises the power of Congress to provide checks and balances on the president's emergency powers. It also imposes "procedural formalities" on the president when invoking such powers (e.g., Proclamation 7463: Declaration of National Emergency by Reason of Certain Terrorist Attacks [September 14, 2001]; Proclamation 8693: Suspension of Entry of Aliens Subject to United Nations Security Council Travel Bans and International Emergency Economic Powers Act Sanctions [July 24, 2011]).
- **U.S. Anti-Terrorism Act of 1992** – Introduced in 1991, the U.S. Anti-Terrorism Act of 1992 provided "a new civil cause of action in Federal law for international terrorism that provides extraterritorial jurisdiction over terrorist acts abroad against United States nationals."
- **Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA)** – The AEDPA criminalised activities dealing with terrorism and terrorist financing, including providing material support or resources to designated terrorists or terrorist organisations, providing or collecting terrorist funds, concealing or disguising material support or funds to terrorists, and receiving military-type training from terrorist organisations. The AEDPA also required U.S. financial institutions to block funds of designated terrorists and terrorist organisations.
- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act** (2001) – The USA PATRIOT Act made significant changes to money laundering regulations, imposed enhanced requirements for AML Programs, and significantly expanded the scope of coverage to nonbank financial institutions (NBFIs). It requires financial institutions to establish AML Programs that include policies, procedures and controls; designation of a compliance officer; training; and independent review. It also requires, among other things, that certain financial institutions establish customer identification procedures for new accounts, as well as enhanced due diligence (EDD) for correspondent, private banking accounts maintained by non-U.S. persons and senior foreign political figures also referred to as politically exposed persons (PEPs).
- **The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) –** The IRTPA amended federal laws related to terrorism (e.g., improvement to intelligence agencies, money laundering and financial crime strategy reauthorisations, border protection, immigration and visa matters). Under IRTPA, FinCEN proposed a rulemaking requiring the reporting of cross-border electronic transmittals of funds (CBETFs). The IRTPA included eight sections:

  - Reform of the Intelligence Community (Intelligence Reform and Terrorism Prevention Act of 2004)
  - Federal Bureau of Investigation
  - Security Clearances
  - Transportation Security (National Strategy for Transportation Security)
  - Border Protection, Immigration and Visa Matters
  - Terrorism Prevention (Stop Terrorist and Military Hoaxes Act of 2004, Weapons of Mass Destruction Prohibition Improvement Act of 2004, Prevention of Terrorist Access to Destructive Weapons Act of 2004)
  - Implementation of 9/11 Commission Recommendations
  - Other Matters

- The **Office of Foreign Assets Control (OFAC)** administers two programs addressing terrorism and weapons of mass destructions (WMDs):
  - **Counter Terrorism Sanctions Program**
  - **Non-Proliferation Sanctions Program**

  OFAC also administers country-specific programs (e.g., North Korean Sanctions Program, Iranian and Syrian Sanctions Program) to address, among other things, nuclear proliferation.

  For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

- The **National Terrorist Financing Risk Assessment** (2015) report issued by TFFC covered the following terrorist financing offenses of the U.S. criminal code:
  - Title 18, Section 2339 A – Providing Material Support to Terrorists
  - Title 18, Section 2339 B – Providing Material Support or Resources to Designated Foreign Terrorist Organisations
  - Title 18, Section 2339 C – Prohibitions Against the Financing of Terrorism
  - Title 18, Section 2339 D – Receiving Military-Type Training from a Foreign Terrorist Organisation
  - Title 18, Section 1960 – Prohibition of Unlicensed Money Transmitting Businesses
  - Title 21, Section 960a – Foreign Terrorist Organisations, Terrorist Persons and Groups
  - Title 50, Section 1705 – War and National Defense Penalties

2460. What key international treaties and conventions have influenced or shaped U.S. counter-terrorism laws?

The United States adopted several international treaties, conventions and resolutions including, but not limited to, the following:

- **Convention on Offences and Certain Other Acts Committed on Board Aircraft** (1963)
- **Convention for the Suppression of Unlawful Seizure of Aircraft** (1970)
- **Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation** (1971)
- **Convention on the Prevention and Punishment of Offences against Internationally Protected Persons, Including Diplomatic Agents** (1973)
- **International Convention against the Taking of Hostages** (1979)
- **Convention on the Physical Protection of Nuclear Material** (1980)
- **Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation** (1988)
- **Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation** (1988)
- **Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf** (1988)
- **Convention on the Marking of Plastic Explosives for the Purpose of Detection** (1991)
- **International Convention for the Suppression of Terrorist Bombings** (1997)
- **International Convention for the Suppression of the Financing of Terrorism** (1999) (Terrorist Financing Convention)

2461. How do the U.S. counter-terrorism laws correspond to the Financial Action Task Force (FATF) Recommendations?

The U.S. counter-terrorism laws parallel the Financial Action Task Force (FATF) Recommendations as outlined below:

- **Recommendation 4 – Confiscation and Provisional Measures** – FATF recommends the implementation of measures to freeze or seize proceeds from criminal activity (e.g., predicate offenses outlined by FATF), laundered funds, funds used to finance terrorism or support a terrorist act or organisation, or property of corresponding value.
- **Recommendation 6 – Targeted Financial Sanctions Related to Terrorism and Terrorist Financing** – FATF recommends compliance with various UNSCRs requiring the freezing of property of persons designated by relevant authorities as terrorists or terrorist organisations.

- **Recommendation 7 – Targeted Financial Sanctions Related to Proliferation** – FATF recommends compliance with various UNSCRs requiring the freezing of property of persons designated by relevant authorities as proliferators of weapons of mass destruction (WMDs).
- **Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation** – FATF recommends the implementation of international instruments to assist with foreign requests to identify, freeze and seize affected property.

For further guidance on international standards, please refer to the Financial Action Task Force section.

2462. Did the FATF Recommendations always address terrorism and terrorist financing?

After the terrorist attacks in the United States on September 11, 2001, many countries intensified their counter-terrorism efforts by focusing their existing AML efforts on terrorism and terrorist financing. In 2001, the FATF added Nine Special Recommendations to its Forty Recommendations to specifically address terrorism:

- **Special Recommendation I: Ratification and Implementation of UN Instruments**
- **Special Recommendation II: Criminalising the Financing of Terrorism and Associated Money Laundering**
- **Special Recommendation III: Freezing and Confiscating Assets**
- **Special Recommendation IV: Reporting Suspicious Transactions Related to Terrorism**
- **Special Recommendation V: International Cooperation**
- **Special Recommendation VI: Alternative Remittance**
- **Special Recommendation VII: Wire Transfers**
- **Special Recommendation VIII: Non-Profit Organisations**
- **Special Recommendation IX: Cash Couriers**

In 2012, FATF consolidated the Recommendations and integrated the Nine Special Recommendations into the Forty Recommendations. For additional guidance, please refer to the Financial Action Task Force section.

2463. What are some examples of significant terrorism or terrorist financing cases?

According to the IEP's GTI report (2016), the twenty most fatal terrorist attacks in 2015 occurred in the following countries:

- Syria (3 attacks; 654 deaths by Islamic State of Iraq and the Levant [ISIL] and Ansar Al-Din Front)
- Nigeria (4 attacks; 473 deaths by Boko Haram and Fulani Militants)
- Iraq (2 attacks; 421 deaths by ISIL)
- Afghanistan (2 attacks; 340 deaths by the Taliban)
- Niger (230 deaths by Boko Haram)

- Egypt (224 deaths by Sinai Province of the Islamic State)
- Yemen (2 attacks; 166 deaths by Houthi Extremists)
- Kenya (154 deaths by Al-Shabaab)
- Cameroon (144 deaths by Boko Haram)
- Ukraine (143 deaths by Donetsk People's Republic)
- Turkey (105 deaths by ISIL)
- France (92 deaths by ISIL)

Summaries of significant terrorism-related cases in the United States including suspects, their causes, methods of attack, methods of capture and charges are available in Key U.S. Terrorist Cases in the Appendix. Following are some outcomes from some of these terrorism-related attacks and cases in the United States:

- **Unabomber** (3 deaths; 1978 - 1995 by Theodore Kaczynski [United States]) – Although officials debated over whether to publish Kaczynski's manifesto, publishing it lead to Kaczynski's capture after his brother recognised the writing and lead authorities to him.
- **World Trade Center Bombing** (6 deaths; February 1993 by Ramzi Yousef [Pakistan] and six others) – Considered a dress rehearsal to the September 11 attacks, Yousef, nephew to Khalid Sheikh Mohammed, attempted to topple one of the World Trade Center buildings with a van filled with 1,000+ pounds of explosives.
- **Oklahoma City (OKC) Bombing** (168 deaths; April 1995 by Timothy McVeigh [United States], Terry Nichols [United States] and Michael Fortier [United States]) – Shortly after the OKC Bombing, the Antiterrorism and Effective Death Penalty Act of 1996 (AEDPA) was passed, criminalising activities dealing with terrorism and terrorist financing, including providing material support or resources to designated terrorists or terrorist organisations, providing or collecting terrorist funds, concealing or disguising material support or funds to terrorists, and receiving military-type training from terrorist organisations. The AEDPA also required U.S. financial institutions to block funds of designated terrorists and terrorist organisations.
- **September 11 Attacks** (Nearly 3,000 deaths; September 2001 by pilots Mohammed Atta [Egypt], Marwan al Shehhi [United Arab Emirates (UAE)], Hani Hanjour [Saudi Arabia], Ziad Jarrah [Lebanon] and 15 others) – The passage of the Uniting and Strengthening America through the Provision of Appropriate Tools to Obstruct Terrorism (USA PATRIOT) Act of 2001 and its subsequent renewals shifted the U.S. strategy from prosecution to prevention of terrorist acts, according to Remarks by the President of Signals Intelligence (2014). The Transportation Security Administration (TSA) was created in November 2001.
- **Amerithrax** (5 deaths; October 2001 by Bruce E. Ivins [United States]) – Although initially thought to be an attack by al-Qaeda shortly after the September 11 attacks, the FBI concluded in 2008 that microbiologist, Ivins, was responsible, motivated to garner support for his lifelong work to develop an anthrax vaccine. In response, the U.S. bolstered its bioterrorism defence. In 2003,

BioWatch was launched, a system designed to detect biological agents that have been intentionally released into the air.

- **Shoe Bomber** (0 deaths; December 2001 by Richard Colvin Reid [United Kingdom]) – The TSA updated their procedures to include random checks of passenger's shoes for pre-boarding security checks at airports after this failed attempt to detonate a bomb on a plane. In later years, the TSA updated security procedures to include the removal of shoes from all passengers for all flights.
- **Sony Pictures Entertainment (SPE) Cyberattack** (0 deaths; November 2014 by North Korean actor Guardians of Peace [GOP]) – Though this attack did not result in any deaths, it was an example of how cyberattacks by hostile foreign actors could damage U.S. institutions. Some believes the cyberattack was in direct retaliation to the film "The Interview" that involved a plot to assassinate North Korea's leader Kim Jong-Un.
- **Emanuel African Methodist Episcopal (AME) Church Shooting** (9 deaths; June 2015 by Dylann Roof [United States]) – This attack sparked a debate about the application of "terrorism" to domestic hate crimes.
- **San Bernardino Attack** (14 deaths; December 2015 by Syed Rizwan Farook [United States] and Tashfeen Malik [Pakistan/Saudi Arabia]) – The investigation into this attack involved a request from the FBI to Apple to unlock the personal smartphone of one of the attackers, which Apple refused. After finding an alternative means of accessing the information on the locked phone, the request was withdrawn by the FBI. This attack was likely partially funded by a US$28,500 loan from Prosper Funding LLC, a peer to peer crowdfunding platform that offered unsecured loans. After the attack, various crowdfunding platforms were also utilised to raise funds for the victims and their family members.
- **Pulse Nightclub Shooting** (49 deaths; June 2016 by Omar Mateen [United States]) – This attack sparked a debate about gun control (e.g., whether buyers should be screened against terrorist watch lists), since the shooter, Mateen, had appeared on government watch lists.

2464. How many of the Suspicious Activity Reports (SARs) filed in a calendar year involve terrorism or terrorist financing?

Using 2016 as the frame of reference, of the 1.98 million SARs filed from January 1, 2016 through December 31, 2016, reports involving terrorism or terrorist financing totalled nearly 2,000 (0.1 percent) and were distributed across financial institution types as follows:

- Money services businesses (MSBs): 1,074 cases (54 percent)
- Depository institutions: 778 cases (39 percent)
- Casinos and card clubs: 61 cases (3 percent)
- Other types of financial institutions: 57 cases (3 percent) (SAR filings by housing government-sponsored enterprises [GSEs], nonbank residential mortgage lenders or originators [RMLOs] and institutions that file voluntarily)
- Securities and futures firms: 19 cases (1 percent)

- Insurance companies: 4 cases (0.2 percent)
- Loan or finance companies: 1 case (0.05 percent)

2465. What was the National Commission on Terrorist Attacks Upon the United States (2002) and what was learned from it?

The National Commission on Terrorist Attacks Upon the United States (2002), also referred to as the 9/11 Commission, was established to examine evidence regarding the facts and causes of the terrorist attacks of September 11, 2001

In 2004, the 9/11 Commission published the 9/11 Commission Report. Following are some highlights from the report:

- Background on the Evolving Terrorist Threat:
  - In the 1980s, Osama Bin Laden joined other Muslim fighters in Afghanistan to fight against the Soviet Union; Bin Laden emerged as a terrorist threat in the late 1990s; until 1997, he was viewed as a financier of terrorism and not as a terrorist leader; Bin Laden organised al-Qaeda under a close alliance with the Taliban.
  - Al-Qaeda launched several attacks that served to increase the visibility of and promote the growth of the organisation. In October 1993, in the same year as the World Trade Center Bombing, assisted by al-Qaeda, Somali citizens shot down a U.S. helicopter, killing 18 and wounding 73 in an incident known as "Black Hawk Down." In August 1998, al-Qaeda attacked two U.S. embassies in Kenya and Tanzania, resulting in 200 deaths by two nearly simultaneous exploding truck bombs.
- Findings included, but were not limited to, the following:
  - Diplomatic pressure between 1997 and 2001, including warnings and sanctions, failed to persuade the Taliban regime to expel Bin Laden.
  - Lack of coordination and other problems (e.g., flat budgets, bureaucratic rivalries) in the intelligence community failed to address transnational terrorist threats. Lack of actionable intelligence lead to the non-use of military options to attack al-Qaeda prior to the September 11 attacks.
  - Permeable borders and immigration controls were exploited (e.g., presentation of passports in a fraudulent manner, false statements on visa applications, false statements to border officials, violations of immigration laws).
  - Permeable aviation security was exploited (e.g., hijackers smuggled weapons with less metal content than guns, the Federal Aviation Administration (FAA) did not screen against the U.S. TIPOFF terrorist watchlist, aircraft personnel trained only in nonconfrontational tactics with respect to hijackers).
  - The civilian and military defenders of North American air space, the FAA and the North American Aerospace Defense Command (NORAD), were unprepared for the unprecedented challenge of the September 11 attacks.

  - Emergency response by firefighters, police officers, emergency medical technicians and emergency management professionals saved lives but was hampered by communication problems (e.g., radios incapable of enabling multiple commands to respond in a unified fashion).
  - Although the source of funds used for the September 11 attacks was unknown, the operatives established bank accounts in their real names using their passports and other identification documents. The attacks reportedly cost between US$400,000 and US$500,000 to execute.

- Recommendations included, but were not limited to, the following:
  - Attack terrorists and their organisations
  - Prevent the continued growth of Islamist terrorism
  - Protect against and prepare for terrorist attacks
  - Develop a national counterterrorism center
  - Create a new national intelligence director
  - Establish a specialised, integrated national security workforce at the FBI
  - Improve congressional oversight for intelligence and counterterrorism
  - Develop an effective information sharing mechanism

Multiple congressional hearings have been held on counter-terrorism and intelligence reforms efforts since the issuance of the 9/11 Commission, including, but not limited to, the following:

- Confronting the Terrorist Threat to the Homeland (Multiple) (2007, 2009, 2010)
- Ten Years After 9/11: Is Intelligence Reform Working? (Parts I & II) (2011)
- Ten Years After 9/11: Preventing Terrorist Travel (2011)
- Ten Years After 9/11: Improving Emergency Communications (2011)
- Defending the Nation Since 9/11: Successful Reforms and Challenges Ahead at the Department of Homeland Security (2011)
- Ten Years After 9/11: Are We Safe? (2011)
- Ten Years After 9/11: A Status Report on Information Sharing (2011)
- Ten Years After 9/11 and the Anthrax Attacks: Protecting Against Biological Threats (2011)

Multiple reforms and laws to address gaps have been passed since then.

2466. What are some examples of red flags for detecting terrorist financing and/or terrorism?

A comprehensive list of red flags for detecting potentially suspicious activity relating to account opening, transaction execution and high-risk products/services/transactions (e.g., cash, wires,

monetary instruments, insurance) has been provided in this publication. Terrorist financing red flags include, but are not limited to, the following:

- An account for which several persons have signature authority, yet these persons appear to have no relation to each other
- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organisation
- Shared address for individuals involved in cash transactions, particularly when the address is also a business location and/or does not seem to correspond to the stated occupation (e.g., student, unemployed, self-employed)
- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (e.g., countries designated by national authorities)
- Cross-border transfers of funds using prepaid cards
- Transactions to/from nonprofit or charitable organisation for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organisation and the other parties in the transaction
- Designee or close associate of designee under OFAC's Counter Terrorism Sanctions Program

For additional examples, please refer to the Transaction Monitoring, Investigations and Red Flags section.

2467. How much has the United States blocked/rejected in assets tied to terrorism?

Based on the recent Terrorist Assets Report issued by OFAC, the United States has blocked over US$2.0 billion relating to state sponsors of terrorism, of which more than 80 percent was related to Iran.

2468. What civil remedies exist for victims of terrorist attacks?

The Anti-Terrorism Act of 1992 permits U.S. citizens to sue for damages arising from international terrorism.

2469. What key groups have provided guidance and resources on terrorism and terrorist financing?

Key groups that have provided guidance or resources related to terrorism and terrorist financing include, but are not limited to, the following:

- The **Office of Terrorism and Financial Intelligence (TFI)** marshals the department's intelligence and enforcement functions with the twin aims of safeguarding the financial system against illicit use and combating rogue nations, terrorist facilitators, weapons of mass destruction (WMD) proliferators, money launderers, drug kingpins, and other national security threats.
- **Office of Foreign Assets Control (OFAC) –** The **Counter Terrorism Sanctions Program,** administered by OFAC, blocks the property and property interests of individuals,

entities and regimes involved in terrorism-related activities, including countries that have been designated as state sponsors of terrorism. Terrorism-related guidance provided by OFAC includes, but is not limited to, the following:

  - **Terrorist Assets Report** - An annual report submitted to Congress concerning the nature and extent of assets held in the United States by terrorist-supporting countries and organisations.
  - **Protecting Charitable Organisations** – A web portal established to protect charitable organisations from abuse by terrorists. Types of resources provided include guidance on providing humanitarian assistance to regions in conflict such as Iran, Somalia and Syria, protecting charitable giving and a risk matrix to assist in evaluating ML/TF risks.

- **Anti-Terrorist Financing Guidelines: Voluntary Best Practices for U.S.-Based Charities** (2010) by the U.S. Department of the Treasury (updates previous versions and comments published in 2002 and 2005) - These guidelines, which are intended to build upon pre-existing controls and protective measures, provide recommendations for the charitable sector to consider in adopting practices to better protect it from the risk of abuse or exploitation by terrorist organisations.
- **National Terrorist Financing Risk Assessment (Annual Report) by the U.S. Department of the Treasury -** The 2015 National Money Laundering Risk Assessment (NMLRA) identifies the money laundering risks that are of priority concern to the United States, while explaining the safeguards in Place to address the threats and vulnerabilities that create money laundering opportunities, and the residual risk to the financial system and national security.
- **National Strategy on Counterterrorism (2011) by the White House -** Former President Barack Obama presented the National Strategy for Counterterrorism on June 29, 2011, that articulates the United States' broad, sustained and integrated campaign against al-Qaeda, its affiliates and its adherents.
- **Countering Violent Islamist Extremism: The Urgent Threat of Foreign Fighters and Homegrown Terror** (2015) – Report of congressional hearing by the National Counterterrorism Center (NCTC)
- **United Nations**
  - **Digest of Terrorist Cases** – A publication created in 2010 that provides practical ideas and expert insights on how to deal with cases of terrorism. Topics include, but are not limited to, the following:
    - Violent Offences Not Requiring a Specific Terrorist Intent
    - Association for the Purpose of Preparing Terrorist Acts
    - Relationship Between Terrorism and Other Forms of Crime (e.g., corruption, narcotics trafficking, organised crime, using minor offences to catch major criminals, false identity and immigration offences)
    - The Statutory Framework for Terrorism Prosecutions

        - Investigation and Adjudication Issues
        - International Cooperation
        - Innovations and Proposals
    - **Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols** – A publication created in 2004 that provides a summary of the development and requirements of the international terrorism conventions to assist those responsible for incorporating anti-terrorism conventions in national legislation.
    - **Guide for Legislative Incorporation of the Provisions of the Universal Legal Instruments Against Terrorism** – A publication created in 2006 that provides guidance on how anti-terrorism conventions and protocols can be integrated and harmonised with domestic law and other international standards.
    - **Preventing Terrorist Acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments** – A publication created in 2006 that provides guidance on topics including, but not limited to, the responsibility to protect against terrorism, scope and elements of a preventive criminal justice strategy against terrorism, offenses, procedural improvements and mechanisms for international cooperation.
    - **Criminal Justice Responses to Terrorism Handbook** – A publication created in 2009 that provides guidance on the key components of an effective criminal justice response to terrorism and criminal justice accountability and oversight mechanisms.
    - **Counter-Terrorism Legislation Database** – An online resource of legal resources on international terrorism established in 2009.
    - **Frequently Asked Questions on International Law Aspects of Countering Terrorism** – A publication created in 2009 that provides an overview of the international law framework in which counter-terrorism works, including general principles of international criminal law, humanitarian law, refugee law and human rights law, which may be relevant in a counter-terrorism context.
- **Financial Action Task Force (FATF)**
    - **Risk of Terrorist Abuse in Non-Profit Organisations** (2014) - A publication released in June 2014 that details the vulnerabilities of nonprofit organisations to abuse by terrorists (e.g., raising of funds, diversion of funds, use of logistical networks and programs to garner ideological support for recruitment).
    - **Terrorism Financing: Regional Risk Assessment 2016** – This regional risk assessment for the South East Asia & Australia region, published by Australia's financial intelligence agency (AUSTRAC) and its Indonesian counterpart financial intelligence unit, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), identifies primary terrorism financing risks from across a broad spectrum of assessed risks to focus on the highest priority risks, including: self-funding from legitimate sources, at-risk nonprofit organisations, cross-border movement of funds/value, and external funding into the region.

- **FATF Report: Emerging Terrorist Financing Risks** –Published in October 2015, this report explores the emerging terrorist financing threats and vulnerabilities posed by foreign terrorist fighters (FTFs), fundraising through social media, new payment products and services, and the exploitation of natural resources.
- **FATF Report: Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)** – A publication created in February 2015 that analyses how this terrorist organisation generates and uses its funding, and highlights a number of new and existing measures to disrupt ISIL financing.
- **The Role of Hawalas and Other Similar Service Providers in Money Laundering and Terrorist Financing** – A publication created in October 2013, which details vulnerabilities of hawalas and other similar service providers (HOSSPs).
- **FATF Report: Financial Flows Linked to the Production and Trafficking of Afghan Opiates-** A publication released in June 2014 that provides an overview of drug trafficking of opiates through Afghanistan and the interrelationship between drug trafficking and terrorist financing.
- **International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)** – A publication created in June 2013, which details best practices for implementing financial sanctions (e.g., freezing of assets) of designated persons in accordance with FATF Recommendation 6 and relevant United Nations Security Council Resolutions (UNCSRs).
- **FATF Report: Terrorist Financing in West Africa** – A publication created in October 2013, in collaboration with the Inter Governmental Action Group against Money Laundering in West Africa (GIABA) that identifies typologies related to terrorism and terrorist financing in West Africa and general observations of the regions' AML/CFT efforts.
- **Guidance for Financial Institutions in Detecting Terrorist Financing** – A publication created in 2002 that provides guidance to financial institutions in detecting terrorist financing, including, but not limited to, account opening and transaction red flags, common sources of funds for terrorist organisations (e.g., kidnapping, extortion, use of nonprofit organisations as front companies, skimming from legitimate businesses).
- **FATF Terrorist Financing Report** – A publication created in February 2008 that analyses the methods of raising and moving funds between terrorist organisations. The report also covers suggested controls for mitigating the risks of this activity.

- **World Bank (WB)**
  - **Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management** – A publication created in 2009 that summarises more than a hundred recommendations on issues relating to terrorist financing, including, but not

limited to, new technologies, nonprofit organisations, informal remittance providers, and international cooperation.

  - **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** (2010) – This paper explores value cards, mobile financial services, online banking and payments, and digital currencies, outlining how they work, analysing their risks, and identifying some ways in which governments and providers are attempting to reduce their attractiveness to financiers of terrorism.
  - **Who Supports Violent Extremism in Developing Countries? Analysis of Attitudes Based on Value Surveys** – Drawing on information on attitudes toward extreme violence and other characteristics of 30,787 individuals from 27 developing countries around the world, and employing a variety of econometric techniques, this paper, published in June 2016, identifies the common characteristics among radicalised individuals willing to justify attacks targeting civilians.

- **International Monetary Fund (IMF)**
  - **Islamic Finance and Anti-Money Laundering and Combating the Financing of Terrorism** (AML/CFT) – A publication released in February 2016 that explores the ML/TF risks associated with Islamic finance to help national regulators gain a better understanding of the specific risks associated with this form of financing and to develop an appropriate response.
  - **The Impact of Terrorism on Financial Markets** – A publication created in 2005 that details how financial markets have reacted to terrorism.
  - **Suppressing the Financing of Terrorism** – A Handbook for Legislative Drafting – A publication created in 2003 that summarises international measures to combat terrorist financing and provides guidance on topics such as criminalising the financing of terrorism; freezing, seizing and confiscating terrorist assets; establishing jurisdiction; international cooperation; alternative remittance systems; and nonprofit organisations.
  - **Regulatory Frameworks for Hawalas and Other Remittance Systems** – A publication created in 2005 that summarises the regulatory frameworks for hawalas and other informal remittance systems. For additional guidance on informal value transfer systems (IVTS), please refer to the Money Services Businesses and Informal Value Transfer Systems sections.

- **Egmont Group**
  - **"Countering of Terrorism Financing" Complementary Interpretive Note** – A document created in 2004 intended to complement the Interpretive Note Concerning the Egmont Definition of an FIU, which further clarifies the definition of an FIU by also explaining the minimum requirements of an FIU to comply with the Egmont Group's definition of an FIU.

- **Wolfsberg**

  - **Wolfsberg Statement on the Suppression of the Financing of Terrorism** (2002) – Guidance describing the role financial institutions have in preventing the flow of terrorist funds through the world's financial systems.

- **National Consortium for the Study of Terrorism and Responses to Terrorism (START) –**START is a research and education center at the University of Maryland, which studies the causes and consequences of terrorism in the United States and around the world, while maintaining the Global Terrorism Database, which includes over 125,000 terrorist attacks.
- **Anti-Defamation League (ADL) -** The Anti-Defamation League (ADL) is an international Jewish non-governmental organisation based in the United States focused on protecting the Jewish people from defamation.
  - **Center on Extremism** - ADL's research and investigative arm, which maintains information about extremism of all types.

AML/CFT Compliance and Anti-Fraud Programs

2470. Is fraud a predicate crime for money laundering?

Yes. Fraud, or any scheme or attempt to defraud is one type of crime underlying money laundering and terrorist financing activity in the United States, consistent with FATF Recommendations.

2471. What types of fraud have been cited with some frequency in Suspicious Activity Reports (SARs)?

FinCEN has issued advisories and guidance on the following fraud-related activities that have appeared with some frequency in SARs in recent years:

- **Mortgage Fraud** - Generally defined as any material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan. For further guidance, please refer to the Mortgage Fraud section.
- **Identity Theft** - Fraud committed or attempted using the identifying information of another person without authority. For further guidance, please refer to the Identity Theft and Identity Theft Prevention Program section.
- **Email Fraud** – Targeting of emails (personal and business) to misappropriate funds by deceiving financial institutions and/or their customers into conducting financial transactions (e.g., wire transfers). Email fraud is distinct from identity theft/account takeover in that the victim retains control over the email account(s). For further guidance, please refer to the Cyber-Related Events and Cybersecurity Preparedness section.
- **Tax Refund Fraud** – Theft of taxpayer identification numbers (TINs), phishing schemes and posing as fraudulent tax preparation businesses to redirect tax refunds, through direct deposits into fraudulently established accounts, prepaid access or other methods.
- **Healthcare/Medicare Fraud** – Submission of fraudulent Medicare claims by fraudulent businesses (often existing only on paper) and collection of reimbursements, often with kickbacks

to complicit doctors. Reimbursements were often cashed at a money services business (MSB) (e.g., check casher).

- **Elder Financial Abuse** – Also referred to as elder financial exploitation; involves the exploitation of a relationship with an elder or dependent adult in order to steal, embezzle or improperly use the person's money, property or other resources; elders are often the victims of the aforementioned frauds. For further guidance, please refer to the Elder Financial Abuse section.

2472. Why are some financial institutions considering integrating their AML/CFT compliance program with other regulatory areas such as anti-fraud and cybersecurity?

Financial institutions that are considering integrating AML/CFT compliance programs with other regulatory areas such as anti-fraud and cybersecurity are motivated by the potential synergy available through cross channel alerts, access to broad financial intelligence as well as the possibility of cost savings by leveraging technology platforms and pooling resources.

In addition, financial regulators, as well as the Director of FinCEN, have specifically expressed support of the combined AML/CFT compliance and anti-fraud approach to take advantage of the potential efficiencies.

For further guidance, please refer to the Cyber-Related Events and Cybersecurity Preparedness section.

2473. What is a cross channel alert?

A cross channel alert involves the sharing of information between groups that has utility for all involved groups (e.g., AML/CFT compliance and anti-fraud units).

2474. How do cross channel alerts aid in the process of detecting financial crimes?

The triggering of more than one type of alert, from money laundering and/or fraud sources, may increase the likelihood of detecting truly suspicious activities. Further, one channel could be used to heighten awareness in another channel and better focus the investigative process.

For example, if a customer generates an AML/CFT alert for activity out of profile, the fraud team may also benefit from this information, particularly if the fraud system has also detected unusual behaviour. This practice is already used within AML/CFT compliance where receipt of a subpoena, National Security Letter (NSL) or an alert for a possible sanctions violation may trigger an investigation for potentially suspicious activity. For further guidance on monitoring and investigative processes, please refer to the Transaction Monitoring, Investigations and Red Flags section. For further guidance on sanctions, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2475. Historically, how have AML/CFT compliance and anti-fraud programs within the same financial institution interacted?

Historically, AML/CFT compliance and anti-fraud programs viewed their missions as separate and distinct. Anti-fraud managers focused their efforts on internal and external embezzlement schemes resulting in financial loss to the institution, while AML/CFT compliance managers primarily sought to

protect the institution against money launderers and terrorists through the detection of potentially suspicious activity and potential sanctions violations.

Today, many financial institutions recognise that most perpetrators of fraud schemes seek to launder their ill-gotten gains and most money launderers have committed other frauds. From this perspective, anti-fraud units and AML/CFT compliance units have a shared mission that is quite clear – to prevent and detect criminal activity.

2476. What is the financial services industry's view on merging AML/CFT and anti-fraud activities?

Conceptually, the idea of merging AML/CFT and anti-fraud activities is widely embraced, but the actual seamless merger of process and technology has yet to be accomplished broadly in the industry today. It is not uncommon for the AML/CFT compliance and anti-fraud units to report to the same executive, but "reporting to" and truly leveraging each other in an established process, leveraging technology across disciplines and from a true financial intelligence perspective are two entirely different things.

2477. What responsibilities could (or typically do) reside in an integrated AML/CFT compliance and anti-fraud unit?

Suspicious Activity Report (SAR) filing is an "easy" answer. Clearly there is a benefit to collaboration and not filing duplicative SARS (duplicative in the sense that multiple SARS are being filed on the same customer for essentially the same suspicious activity). Another "easy" answer is case management. Simply, it is hard to conceive of a reason to not have a common case management system. Cross channel alerts, as discussed previously, benefit both groups and should be a shared activity.

For further guidance on SARs, please refer to the Suspicious Activity Reports section.

2478. How do the backgrounds and experience of AML/CFT and anti-fraud personnel compare?

Both AML/CFT and anti-fraud professionals are knowledgeable about how the products and services offered by their institutions can be used for illicit purposes, relevant laws and regulations and are adept at conducting research, completing complex analytics, interviewing people at all professional levels and writing comprehensive reports. As a result, cross-training individuals between these groups should be relatively easy.

2479. What are examples of policies and procedures which tend to be shared across AML/CFT compliance and anti-fraud programs?

AML/CFT compliance and anti-fraud programs may share many policies and procedures within financial institutions, whether they operate as one unit or independently. Examples include, but are not limited, to the following:

- Investigative protocols

- Referral of information to law enforcement
- Disbarment/termination of customers for inappropriate activity
- Procedures for the receipt of information
- Due diligence activities and activities concerning the filing of SARs

2480. Have anti-fraud units and AML/CFT units within the same financial institution been successful with sharing monitoring systems?

Often, AML/CFT monitoring systems and fraud detection systems operate on independent platforms with their own case management systems. As a result, AML/CFT and anti-fraud units may not always be aware of each other's cases.

2481. Should separate mechanisms exist for the receipt of allegations of money laundering/terrorist financing and fraud and misconduct?

In keeping with the notion that all frauds may have a money laundering dimension and that money laundering may involve an underlying fraud, it makes sense to have one reporting mechanism for fraud and money laundering allegations.

Regulators and regulations encourage financial institutions to implement a fraud hotline as a confidential communication channel to identify fraud and reduce fraud-related losses. In its guidance to financial institutions, the FDIC, for example, recommends that to minimise inappropriate calls or complaints to the hotline that do not involve wrongdoing, institutions should communicate the hotline's purpose and define guidelines about what types of improprieties are reportable events. However, the FDIC does not explicitly state what violations, improprieties or crimes should be reportable to the hotline.

2482. What are some key challenges to integrating AML/CFT compliance and anti-fraud programs?

Some key challenges for merging AML/CFT compliance and anti-fraud programs include, but are not limited to, the following:

- Incorrectly assuming that merging of reporting lines is the same as integrating separate programs
- Organisational alignment without process/technology alignment only guarantees that everyone has a common manager and accomplishes little in reality
- Leadership from one or the other discipline may lack the knowledge and experience to manage the area effectively when dealing with issues outside of his/her traditional comfort zone
- Recognising that effective fraud monitoring needs to be real time, while AML/CFT monitoring is often after the fact
- Management may see one program as more important than the other, and, as a result, may not allocate resources effectively

- Challenges with process redesign
- Cost of implementing technology solutions
- Cultural barriers

If the integration is done thoughtfully and with purpose, however, these challenges can be overcome.

Identity Theft and Identity Theft Prevention Program

Basics

2483. How is the term "identity theft" defined by the Fair and Accurate Credit Transactions Act of 2003 (FACT Act)?

Identity theft is defined as fraud committed or attempted using the identifying information of another person without authority.

2484. What is the difference between identity theft and identity fraud?

Identity theft involves the theft of another person's identifying information, whereas identity fraud involves the use of false identifying information that may or may not belong to someone else (e.g., a fabricated SSN).

2485. How is the term "identifying information" defined?

Identifying information is defined as:

- Any name or number that may be used, alone or in conjunction with any other information, to identify a person, including:
  - Name, taxpayer identification number (TIN), Social Security Number (SSN), employer identification number (EIN), date of birth (DOB), official state- or government-issued driver's license number or identification number, alien registration number or government passport number
  - Unique biometric data, such as a fingerprint, voice print, retina or iris image or other unique physical representation
  - Unique electronic identification number, address or route code
  - Telecommunication identifying information or access device

2486. What are some methods of identity theft?

Some methods of identity theft include, but are not limited to, the following:

- Dumpster diving
- Employee/insider theft
- Electronic intrusions or hacking

- Pharming
- Shoulder surfing or browsing social networks for identity or other sensitive information
- Skimming
- Social engineering (e.g., phishing, spyware, keystroke loggers)

2487. What is "pharming"?

Pharming is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by secretly redirecting users from legitimate websites to websites created by scammers.

2488. How is the term "skimming" defined with respect to identity theft?

Skimming is a method of fraudulently obtaining and storing credit/debit card information through the use of computers or specialised card readers in order to re-encode the account information onto the magnetic strips of blank credit/debit cards, which then can be used to make purchases.

2489. What is "phishing," "vishing," and "smishing"?

Phishing is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by masquerading as a legitimate entity in an electronic communication (e.g., email, spyware). For example, an individual may receive an email that appears to be from his or her bank that requests identity and/or password information under the guise of "verification" purposes.

Vishing (voice phishing) and smishing are similar to phishing, but conducted through the telephone/voicemails and texting (SMS messages) respectively.

Impact on Financial Institutions

2490. What are the requirements of an Identity Theft Prevention Program?

A financial institution must implement an Identity Theft Prevention Program (ITPP) to identify, detect, prevent and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. An ITPP requires the following four basic elements:

- Identification of relevant red flags (i.e., pattern, practice or specific activity that indicates the possible existence of identity theft)
- Implementation of a monitoring program to detect identity theft red flags
- Establishment of appropriate responses to detected red flags to prevent and mitigate identity theft
- Written policies and procedures and periodic updates of the ITPP (e.g., changes to addresses as they relate to identity theft; changes in methods to detect, prevent or mitigate identity theft; changes in the types of accounts offered or maintained; changes in business arrangements, such as mergers, acquisitions, alliances, joint ventures, and service provider arrangements)

Additionally, financial institutions must:

- Obtain approval of the initial ITPP by the board of directors, a committee of the board, or a designated employee at the level of senior management; the financial institution may determine whether ongoing changes to the ITPP require approval by the board of directors/committee/senior management
- Involve the board of directors, a committee of the board, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the ITPP
- Train relevant staff
- Oversee service provider arrangements to ensure the activity of the service provider is conducted in accordance with the financial institution's ITPP
- Conduct periodic assessments to determine whether the financial institution offers or maintains covered accounts; the assessment should consider the types of accounts offered, the methods of account opening, the methods/channels provided to access accounts and its previous experiences with identity theft

2491. Which institutions are required to implement an ITPP?

The following financial institutions, which directly or indirectly maintain "covered accounts," are required to implement an ITPP:

- Banks
- Savings and loan associations
- Mutual savings banks
- Credit unions
- Entities regulated by the U.S. Securities and Exchange Commission (SEC) (e.g., broker-dealers, investment companies, investment advisers)
- Entities regulated by the Commodity Futures Trading Commission (CFTC) (e.g., futures commission merchants [FCM], commodity trading advisers [CTA], commodity pool operators [CPO], introducing brokers, swap dealers, major swap participants, retail foreign exchange dealers)
- Any person who directly or indirectly holds a transaction account belonging to a consumer and creditors (i.e., persons who participate in a credit decision, including those who arrange for the extension, renewal or continuation of credit, which in some cases could include third-party debt collectors or brokers)

Applicability of the Red Flags Rule to depository banks is fairly clear, and these institutions have been required to comply with the final Red Flags Rule since November 2008. In December 2010, the ITPP amended the definition of "creditor" to include creditors that regularly, and in the ordinary course of business, meet one of three general criteria. They must:

- Obtain or use consumer reports in connection with a credit transaction;
- Furnish information to consumer reporting agencies in connection with a credit transaction;
- Advance funds to, or on behalf of, someone, except for funds for expenses incidental to a service provided by the creditor to that person.

Entities regulated by the SEC and CFTC became subject to the Red Flags Rule on April 10, 2013, pursuant to the Dodd-Frank Wall Street Reform and Consumer Protection Act.

2492. How is the term "transaction account" defined?

The term "transaction account" is defined by the Federal Reserve Act as a "deposit or account on which the depositor or account holder is permitted to make withdrawals by negotiable or transferable instrument, payment orders of withdrawal, telephone transfers or other similar items for the purpose of making payments or transfers to third persons or others (e.g., demand deposits, negotiable orders of withdrawal accounts, savings deposits subject to automatic transfers, share draft accounts)."

2493. How is the term "covered account" defined?

A covered account is defined as:

- An account primarily for personal, family or household purposes that involves or is designed to permit multiple payments or transactions
- Any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution from identity theft

2494. Are covered accounts limited to consumer accounts only?

No. Although identity theft occurs more frequently in consumer accounts than commercial accounts, the ITPP is not limited to consumer accounts. Financial institutions are expected to take a risk-based approach in identifying other types of accounts beyond consumer accounts that should be covered under the ITPP (e.g., small business accounts).

2495. How is the term "service provider" defined?

A service provider is a person who provides a service directly to the financial institution. A financial institution is ultimately responsible for complying with the ITPP requirement even if it outsources an activity (e.g., account opening) to a service provider.

2496. How can a financial institution detect identity theft red flags?

A financial institution can do the following to detect identity theft red flags:

- Obtain and verify identifying information at account opening
- Authenticate customers
- Monitor transactions
- Verify the validity of change of address requests

2497. What is a "notice of address discrepancy"?

A notice of address discrepancy is a notice sent to a user by a consumer reporting agency that informs the user of a substantial difference between the address for the consumer that the user provided to request the consumer report and the address(es) in the agency's file for the consumer.

Upon receipt of a notice of address discrepancy, users (e.g., card issuers) are required to develop and implement policies and procedures to enable the user to form a reasonable belief that a consumer report relates to the consumer about whom it has requested the report (e.g., comparison of the information in the consumer report against the information maintained on the consumer).

2498. What are some examples of "appropriate responses" to the detection of identity theft red flags?

Some examples of appropriate responses include (depending upon the circumstances presented), but are not limited to, the following:

- Contacting the customer
- Changing passwords, security codes or other security devices that permit access to an account
- Reopening an account with a new account number
- Not opening a new account
- Closing an existing account
- Not attempting to collect on a covered account or not selling a covered account to a debt collector
- Notifying law enforcement
- Filing a Suspicious Activity Report (SAR)
- No response

For further examples of red flags, please refer to the Suspicious Activity Red Flags section.

2499. Does the ITPP require the use of any specific technology or systems?

No. The ITPP does not require the use of any specific technology or systems to detect identity theft.

2500. What other legal requirements should a financial institution consider when implementing its ITPP?

A financial institution should consider related legal requirements when implementing its ITPP that include, but are not limited to, the following:

- Filing of SARs
- Implementation of limitations on the extension of credit when fraud is detected

- Implementation of requirements for furnishing of information to consumer reporting agencies to correct or update inaccurate or incomplete information and to not report information that the financial institution has reasonable cause to believe is inaccurate
- Complying with prohibitions on the sale, transfer and placement for collection of certain debts resulting from identity theft

2501. Where can a financial institution obtain examples of red flags for identity theft?

An appendix to the Red Flags Rule provides a list of nonexclusive red flags that should be considered when performing an ITPP risk assessment. The red flags are organised into the following categories:

- Alerts, notifications or warnings from a consumer reporting agency
- Suspicious documents
- Suspicious personal identifying information
- Unusual use of or suspicious activity related to the covered account
- Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft

2502. How many instances of identity theft have been reported on Suspicious Activity Reports (SARs)?

Of the 1.98 million Suspicious Activity Report (SAR) filings from January 1, 2016, through December 31, 2016, reports of identity theft totalled over 150,000 (8 percent) and were distributed across financial institution types as follows:

- Depository institutions: 111,000 cases (73 percent)
- Money services businesses (MSBs): 21,000 cases (14 percent)
- Other types of financial institutions: 13,500 cases (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily) (9 percent)
- Securities and futures firms: 5,000 cases (3 percent)
- Casinos and card clubs: 372 cases (0.2 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 181 cases (0.1 percent)
- Insurance companies: 171 cases (0.1 percent)
- Housing GSEs: 22 cases (less than 0.1 percent)

2503. How is the ITPP different from the Customer Identification Program?

The ITPP and the Customer Identification Program (CIP) differ in the following manner:

- CIP is limited to new customers only

- CIP requires a one-time verification at account opening
- CIP requires verification of four elements: name, DOB, physical address and TIN
- ITPP applies to both new and existing customers
- ITPP requires monitoring of identifying information beyond what is included in CIP
- ITPP requires ongoing monitoring of existing customers, not just new customers
- ITPP is concerned with both verification of identifying information and authentication

For further guidance on CIP, please refer to Section 326 – Verification of Identification.

2504. What is the difference between "verification" and "authentication"?

Verification confirms that the information provided by a customer is valid (e.g., an individual with the provided name, address and TIN matches with an independent source, such as a credit reporting database).

Authentication attempts to ensure that the individual providing the information, or accessing the account(s), is the person he or she claims to be. Authentication is accomplished by requesting information that is not necessarily "found in a wallet" (e.g., previous address, previous employer). Often, once an individual has been verified, financial institutions will ask customers to create custom security questions (e.g., mother's maiden name, favourite movie, pet's name) that serve to authenticate customers.

2505. What is the Stolen Identity Refund Fraud (SIRF) enforcement unit?

The Stolen Identity Refund Fraud (SIRF) enforcement unit is a national program administered and enforced by the Internal Revenue Service (IRS) to combat identity theft fraud used to file fake tax returns that claim tax refunds. In past years, the IRS has been able to stop or recover over 80 percent of fraudulent claims.

2506. What key guidance has been provided on identity theft?

The following key guidance has been provided on identity theft:

- **Interagency Guidelines on Identity Theft Detection, Prevention and Mitigation** (2010) by the Federal Financial Institutions Examination Council (FFIEC)
- **Guidance to Assist Financial Institutions with Identifying and Reporting Account Takeover Activity** (2011) by FinCEN
- **Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems** (2012) by the Financial Action Task Force (FATF)
- **Guide for Assisting Identity Theft Victims** (2013) by the Federal Trade Commission (FTC)
- **Identity Theft Checklist** (2012) by the U.S. Department of Justice (DOJ)
- **Authentication in an Internet Banking Environment** (2005) by the FFIEC

- **Advisory: Tax Refund Fraud and Related Identity Theft** (2012) by FinCEN
- **Update on Tax Refund Fraud and Related Identity Theft** (2013) by FinCEN
- **FinCEN Study Examines Rise in Identity Theft on SARs** (2010) by FinCEN
- **FinCEN Examines Identity Theft-Related SARs Filed by Securities & Futures Firms** (2011) by FinCEN
- **Identity Theft: Trends, Patterns, and Typologies Reported in Suspicious Activity Reports** (2010) by FinCEN

Mortgage Fraud

2507. How is the term "mortgage fraud" defined?

Mortgage fraud is generally defined as any material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan.

There are two types of mortgage fraud: fraud for housing/property and fraud for profit. The former typically involves misstatements about income, debt or property value by the borrower in order to qualify for a mortgage in which he/she usually intends to pay. The latter typically involves collusion among industry professionals involved in the mortgage process (e.g., mortgage brokers, real estate agents, appraisers, attorneys, title examiners) in order to qualify for a mortgage and generate a profit with no intention to pay the mortgage. Profits can be generated in multiple ways, such as by obtaining a mortgage and not paying it back or by flipping properties with inflated property values. In both types of mortgage fraud, lenders may extend credit that the lender would likely not have offered if the true facts were known.

2508. Which types of loan products typically have been used in mortgage fraud schemes?

A variety of loan products have been used in mortgage fraud schemes, including purchase loans, refinancing, home equity, second trust and construction loans. Over the last couple of years, there has been a significant increase in new mortgage fraud schemes involving distressed loans of all types.

2509. What are some examples of mortgage fraud schemes?

Some common schemes include, but are not limited to, the following:

- **Occupancy Fraud** – A borrower wants to obtain a mortgage on an investment property, but claims on his/her application that he/she will occupy the house in order to obtain a better interest rate than is warranted.
- **Property Flipping** – Property is purchased, falsely appraised at a higher value, and then quickly sold.
- **Property Flopping** – Foreclosed property is sold at an artificially low price to a straw buyer, who then sells the property at a higher price and pockets the difference.

- **Income Fraud** – Particularly during the period of lax underwriting standards that existed between approximately 2004 and 2007, many borrowers who could not qualify for loans based on their verified income chose – or were encouraged by unscrupulous brokers or lenders – to apply for stated income loans, and provided income amounts significantly in excess of what they actually earned in order for their applications to be approved. (This is discussed further below.) Income fraud also includes borrowers understating income to qualify for hardship concessions and modifications.
- **Failure to Disclose Liabilities** – Prospective borrowers may attempt to conceal certain financial obligations, such as other mortgages or credit card debt in an effort to try and reduce the appearance of recurring debt. This omission of liabilities helps to artificially lower the debt-to-income ratio (which is used by lenders in order to help quantify how much a prospective borrower may qualify for), in the hope of qualifying for a larger loan.
- **Occupation/Employment Fraud** – This type of fraud may rise as unemployment levels increase (e.g., as the result of an economic crisis). Prospective borrowers may claim self-employment in a non-existent company; may claim a higher position; or may claim that they still hold their previous position, to facilitate falsifying income.
- **Silent Second** – The buyer of a property borrows the down payment from the seller through the issuance of a non-disclosed second mortgage; the primary lender believes the borrower has invested his/her own money in the down payment and therefore, approves a mortgage for a borrower who typically would not have been approved.
- **Nominee Loan/Straw Borrower** – The identity of the borrower is concealed through the use of a nominee, and the borrower uses the nominee's name and credit history to apply for a loan. Sometimes, the nominee is a willing participant in the scheme. It is considered identity theft in instances in which the nominee is not a willing participant.
- **Asset Rental Fraud** – A borrower "rents" assets by temporarily depositing funds into his/her account to inflate the stated value of his/her assets in order to qualify for a mortgage. Funds are withdrawn after the borrower qualifies for the mortgage. In some instances, the borrower pays a "rental fee" for the borrowed assets.
- **Cash-Back Fraud** – This is frequently seen as part of money laundering activity, where the price of a property is illegally inflated, such that parties involved in the sale are eligible for "cash back" which is not disclosed to the lender.
- **Shotgunning** – A property owner applies for home equity loans with multiple lenders at the same time, and the lenders may not be aware of the other loans (e.g., lenders may not report to the same credit bureau, lag in reporting to credit bureaus); or a property owner, who may not be the rightful owner, sells the same property multiple times to different buyers.
- **Air Loans** – Non-existent property loans where there is usually no collateral and often no real borrower.

- **Appraisal Fraud** – This type of fraud occurs when a borrower overstates home value to obtain more money from a sale or refinancing, or understates home value to purchase property at a lower cost. In instances when a home's value is overstated, more money can be obtained by the borrower in the form of a cash-out refinance. Additionally, identity theft can facilitate mortgage fraud, when an individual applies as a would-be borrower under a stolen identity. For additional guidance on identity theft-related fraud, please refer to the Identity Theft and Identity Theft Prevention Program section.

2510. What are some of the factors that give rise to mortgage fraud?

There are a number of variables that may contribute to the occurrence of mortgage fraud including greed, as people look for "get-rich-quick" opportunities, and economic/personal financial conditions that may prompt individuals, or groups of individuals, to commit mortgage fraud. Indicators of these variables may include:

- Loan delinquencies
- Defaults
- Foreclosures
- Poor credit
- Unemployment
- Increases in negative equity
- Overall housing prices and availability of properties

2511. What are some vulnerabilities that increase the fraud risks of the mortgage industry?

Some vulnerabilities of the mortgage industry include, but are not limited to, the following:

- Non-face-to-face/automated loan processing channels (e.g., internet, telephone)
- Innovative loan products (e.g., interest-only loans, no- or low-documentation products, adjustable-rate mortgages) and subprime loans
- Applications taken by entities other than regulated financial institutions (e.g., mortgage brokers)
- Involvement and abuse by, and possible collusion among, multiple third parties (e.g., borrower, mortgage broker, real estate agent, appraiser, underwriter, lender, closing/settlement agent)

For a list of red flags, please refer to the Lending Red Flags and Mortgage and Real Estate Red Flags sections.

2512. What resources and guidance are available on mortgage fraud?

Organisations such as the U.S. Federal Bureau of Investigation (FBI), the Financial Crimes Enforcement Network (FinCEN), and the Financial Fraud Enforcement Task Force (FFETF) have developed websites and annual reports intended to provide both the industry and consumers with valuable information about the extent of mortgage fraud:

- **FFETF** – In 2009, the FFETF was created in order to develop a working group (or multiple working groups) all operating toward the same goal of improving government efforts to identify, investigate, prosecute and prevent various financial crimes. With the rise in fraudulent scams related to the mortgage industry, this particular financial crime has been a significant area of focus for the FFETF. While the resources offered by the FFETF, available on its website, are largely aimed at protecting consumers against being victims of fraud, the information can also be leveraged by the industry to help stay apprised of ongoing developments in mortgage-related fraud, as well as efforts to combat this activity. This includes press releases and news articles of recent investigations and prosecutions, the FFETF's annual report publication, and links to other agencies also involved in the prevention of mortgage fraud (e.g., the U.S. Department of Housing and Urban Development). (http://www.stopfraud.gov/about.html)
- **FBI** – The FBI has developed a website, which provides access to both general information about mortgage fraud, as well as analytics reports dating back to 2006, coverage of recent incidents of identified mortgage fraud, details about key and emerging mortgage fraud scams, and potential ways to prevent consumers from becoming the target of mortgage fraud. (http://www.fbi.gov/about-us/investigate)
- **FinCEN** – FinCEN, as a member of the FFETF, has a page on its website that is solely dedicated to providing information (both to the industry as well as consumers) about mortgage fraud. The website provides access to detailed reports, which similar to the FFETF and FBI reports, highlight new trends in mortgage fraud prevalence. There is also detailed information available regarding the number of Suspicious Activity Reports (SARs) filed relating to mortgage fraud and trends in the volume of mortgage fraud, ongoing investigations, and multiagency crackdowns. (http://www.fincen.gov/news_room/rp/mortgagefraud.html)

  Specifically, FinCEN has published the following releases:

  - **FinCEN Final Rule: Anti-Money Laundering Programs and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators** (2012)
  - **FinCEN Guidance: Compliance Obligations of Certain Loan or Finance Company Subsidiaries of Federally Regulated Banks and Other Financial Institutions** (2012)
  - **Mortgage Fraud SAR Data Tables by State, Urban Area and County**
  - **Suspected Mortgage Fraud (Including Quarterly Written Reports)**
  - **Suspected Money Laundering and Fraud in the Residential Real Estate Industry** (2012)
  - **Suspected Money Laundering and Fraud in the Commercial Real Estate Industry** (2011)
  - **Home Equity Conversion Mortgages (Reverse Mortgages)** (2012)
  - **Mortgage Fraud Cases Supported by FinCEN Filings** (2012)

- **Foreclosure Rescue Scams & Loan Modification Fraud** (2009)
- **Multi-Agency Crackdown Targeting Foreclosure Rescue Scams, Loan Modification Fraud** (2009)
- **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding Loan Modification/Foreclosure Rescue Scams** (2009)
- **Mortgage Loan Fraud Update: Suspicious Activity Report Filings from July 1-September 30, 2009**
- **Mortgage Loan Fraud Update (published in *The SAR Activity Review*) – Trends, Tips & Issues** (Issue 16, October 2009)
- **Suspicious Activity Related to Mortgage Loan Fraud** (2012)
- **FinCEN Assesses Suspicious Activity Involving Title and Escrow Companies** (2012)
- **California, Nevada, Florida Top Mortgage Fraud SAR List** (2012)
- **FinCEN Attributes Increase in Suspicious Activity Reports Involving Mortgage Fraud to Repurchase Demands** (2012)
- **Mortgage Loan Fraud Connections with Other Financial Crime** (2009)
- **Filing Trends in Mortgage Loan Fraud** (2007)
- **Mortgage Loan Fraud: An Update of Trends Based Upon an Analysis of Suspicious Activity Reports** (2008)
- **Mortgage Loan Fraud Assessment** (2006)
- **Mortgage Fraud Report: SAR Filings Up; Potential Abuse of Bankruptcy Identified** (2010)

2513. Is mortgage fraud typically perpetrated at certain stages in the lending process?

Mortgage fraud can occur at any stage in the mortgage lending process and can involve any of the following market participants:

- Licensed/registered and non-licensed/registered mortgage brokers
- Lenders
- Appraisers
- Underwriters
- Accountants
- Real estate agents
- Settlement attorneys
- Land developers

- Investors
- Builders
- Bank account representatives and trust account representatives
- Organised criminal groups

Additionally, individuals applying for mortgages can be perpetrators of mortgage fraud, even though they may not be involved in the loan administration process.

2514. How many instances of mortgage fraud have been reported on SARs?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports of mortgage fraud totalled nearly 30,000 (2 percent) and were distributed across financial institution types as follows:

- Depository institutions: 21,721 cases (73 percent)
- Other types of financial institutions: 3,248 cases (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily) (11 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 2,502 cases (8 percent)
- Housing GSEs: 2,099 cases (7 percent)
- Money services businesses (MSBs): 76 cases (0.3 percent)
- Securities and futures firms: 31 cases (0.1 percent)
- Insurance companies: 11 cases (less than 0.1 percent)
- Casinos and card clubs: 7 cases (less than 0.1 percent)

2515. Are mortgage lenders and originators required to establish AML Programs pursuant to Section 352 of the USA PATRIOT Act?

Yes. As a subset of loan or finance companies, residential mortgage lenders and originators (RMLOs) are required to establish AML Programs and file Suspicious Activity Reports (SARs).

For additional guidance on the AML/CFT requirements for nonbank RMLOs, please refer to the Loan or Finance Companies/Nonbank Residential Lenders and Originators section.

2516. Are any other AML/CFT rulemakings under consideration with regard to other participants in the mortgage market?

Yes. Due to the rise in abusive and fraudulent sales and financing practices in both the primary and secondary residential mortgage markets, FinCEN has issued or proposed rules for the following participants:

- Housing Government-Sponsored Enterprises (GSEs) (e.g., Federal National Mortgage Association [Fannie Mae], Federal Home Loan Mortgage Corporation [Freddie Mac], Federal Home Loan Banks [FHL Banks])
- Persons involved in real estate settlements and closings (e.g., real estate brokers, attorneys representing buyers/sellers, title insurance companies, escrow agents, real estate appraisers)

Housing GSEs are required to establish AML Programs, file suspicious activity reports (SARs) and comply with other AML/CFT requirements.

The 2003 proposed rulemaking for persons involved in real estate settlements and closings has yet to be finalised. Although not required to establish an AML Program, they are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, they are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations.

Together, these regulations, along with the requirements for RMLOs, are expected to increase the number of SAR filings from the mortgage industry and provide regulators and law enforcement with more information on mortgage fraud.

For further guidance, please refer to the Loan or Finance Companies/Nonbank Residential Lenders and Originators, Housing Government-Sponsored Enterprises and Persons Involved in Real Estate Closings and Settlements sections.

Elder Financial Abuse

Basics

2517. What is elder abuse?

Elder abuse generally refers to intentional or negligent actions taken by a caregiver or other person presumed to be in a position of trust who causes harm or a serious risk of harm to a vulnerable, older adult. It can be a single act or a series of actions that causes harm or distress to an older person and may include physical, psychological or financial abuse, as well as neglect.

2518. What is elder financial abuse?

Elder financial abuse, also referred to as elder financial exploitation, involves the exploitation of a relationship with an elder or dependent adult in order to steal, embezzle or improperly use the person's money, property or other resources. The exploitation may occur by deception, coercion, misrepresentation, undue influence or theft, and can include deprivation of money and/or property.

2519. Why is elder financial abuse so insidious?

The occurrence of elder financial abuse is becoming more frequent and yet, at the same time, the crime is often underreported. Victims may not recognise that they are being exploited, due to the nature of the relationship with the perpetrator and/or due to their own diminished capacity. Additionally, many

elders are reluctant to report the crime for reasons that include embarrassment that they have fallen prey to a confidence scheme, fear of retribution from the perpetrator, and even a desire to protect the loved ones who exploit them.

Elder financial abuse is particularly devastating because victims may lose all of their life savings and may never recover financially. Elder victims' inability to provide for their own needs and uncertainty as to what will become of them can have a permanent effect on their mental state, with victims often suffering from depression.

2520. What is an example of an elder financial abuse case?

In December 2012, MoneyGram agreed to a Deferred Prosecution Agreement (DPA) with a forfeiture of US$100 million with the DOJ for aiding and abetting wire fraud and failing to maintain an effective AML Program. Often targeting the elderly, scams ranged from individuals posing as relatives in need, false promises of prize money, false offers for deeply discounted items and false employment offers. Each scam required victims to send funds through MoneyGram.

Despite thousands of customer complaints and red flags raised by concerned personnel with regard to mass marketing and phishing schemes by foreign agents, MoneyGram's sales executives allegedly refused to terminate agents suspected of involvement in these fraudulent scams. Reports of fraud by customers grew from nearly 1,600 instances in 2004 to almost 20,000 in 2008, totalling to at least US$100 million.

2521. Who is at risk of being victimised?

Older persons with physical or mental health issues may be vulnerable because their dependence on other individuals for daily care isolates them and/or because a diminished capacity leaves them unaware of the abuse or limits their ability to provide informed consent or otherwise respond appropriately. However, any older adult, regardless of potential health concerns, may be at increased risk of exposure to unscrupulous individuals who specifically target elders. Characteristics that perpetrators may exploit include, but are not limited to, the following:

- The isolation of individuals who may not physically be able to leave or object to the treatment;
- The elder's need for interaction with other individuals;
- Vulnerable experiences, such as traumas suffered by the elder or a close loved one;
- The elder's naiveté in wanting to believe the perpetrator is telling the truth; and
- The elder's desire to help an individual in need.

With 70 percent of wealth in the United States under the control of persons over the age of 50, the pool of potential victims for elder financial abuse is substantial.

2522. Who are common perpetrators of elder financial abuse?

Perpetrators of elder financial abuse can include anyone in a position of trust, control or authority; often, these individuals are well known to the victims. These perpetrators can include family members,

neighbours and friends, as well as paid service providers – such as attorneys, doctors and financial advisers – and other persons who befriend the elder specifically to exploit him/her in the future. Additionally, perpetrators may be con artists who impersonate people in a position of trust.

2523. What common schemes are used to perpetrate elder financial abuse scams?

Elder financial abuse can take many forms, depending on the nature of the relationship being exploited. It can be as simple as directly removing money or property from the elder's possession, such as taking it from a wallet, or it can involve a complex confidence scam designed specifically to prey upon certain vulnerabilities. It may involve a series of ongoing activities, or it can be a onetime transaction. It may involve persons well-known to the victim, or it could be perpetrated by con artists or other criminals who target elders. Common categories of schemes involve, but are not limited to, the following:

- **Exerting undue influence, misrepresentation or fraud to obtain money or property** – The perpetrator manipulates, intimidates or otherwise threatens the elder into giving or signing over assets.
- **Exploiting a power of attorney or fiduciary authority** – The perpetrator takes advantage of his/her role as power of attorney or fiduciary to alter the elder's will, borrow money in the elder's name, or dispose of an elder's assets or income.
- **Misappropriation of money or property** – The perpetrator obtains access to the elder's bank accounts, credit cards, pension, or forges the elder's signature in order to take money or property and/or to use the elder's property or possessions without permission.
- **Overcharging for services or withholding services** – The perpetrator may provide services for basic needs, such as food or medicine, at an exorbitant or unreasonable fee when the elder is not in a position to obtain the services elsewhere. Also, the perpetrator may agree to perform work, such as household repairs or other home improvement projects, at a reasonable fee, but once the work is under way, refuses to complete the job until the elder pays more for it.
- **Confidence crimes** – The perpetrator gains the victim's confidence and deceives or tricks him/her into paying money. These scams may involve claims of lottery winnings or inheritances, where the victim is persuaded to provide an amount upfront as a show of good faith, or may involve fictitious accidents or stories of loved ones needing immediate medical treatment to induce the elder to send money quickly.
- **Telemarketing and mail fraud** – The perpetrator calls victims or sends flyers that use deception, scare tactics or exaggerated claims to induce them to send money and can be difficult to distinguish from legitimate calls or correspondence. The fraud may involve selling a valueless product, collecting donations to a fake charity and the perpetrator may make repetitive charges against victims' credit cards without authorisation.
- **Predatory lending practices** – Elders may be pressured into high-interest loans they cannot repay, such as home equity loans to finance home repairs, debt consolidation or healthcare costs, or they may be coerced into a reverse mortgage transaction.

2524. What are the warning signs of elder abuse?

Victims of elder abuse often demonstrate changes in their behaviour and patterns of financial activity. The financial institution may be unable to speak with the customer, despite repeated attempts to contact him/her. When the institution does have customer contact, the elder may be accompanied by another person who won't allow the elder to speak alone with personnel or make any independent decisions. This person could be a new caregiver to the elder, a new "best friend" or someone known to the institution, such as a family member, but who may take excessive interest in the elder's finances or who suddenly takes control of the elder's financial decisions.

Behavioural warning signs may include:

- **Physical changes** – The elder's appearance and grooming may deteriorate noticeably. Inadequately explained fractures, bruises, cuts or burns may appear. The elder may have unexplained sexually transmitted diseases;
- **Mood or personality changes** – The elder may increasingly become withdrawn or secretive, could be reluctant to engage in conversation, and may appear frightened of or submissive to an individual accompanying him/her; and
- **Changes in intellectual capacity** – The elder may appear disoriented or forgetful, or demonstrate a lack of understanding, and may repeatedly ask the same question. The elder may have no awareness of his/her finances and appear confused about past transactions or missing funds.

Elders who have recently lost a spouse or moved into a nursing home are particularly vulnerable because of the emotional stress these types of life changes can create.

Although the presence of warning signs is not conclusive evidence that the elder is the victim of abuse, these indicators could signify the customer is at heightened risk.

2525. What are some common red flags of elder financial abuse?

If a financial institution notes the presence of warning signs for elder financial abuse, it should investigate or perform other due diligence to determine whether potentially suspicious activity is present. The following are examples of financial activity red flags:

- **Changes in transaction activity** – The elder's spending pattern may change, including:
    - Decreased spending on essential items (e.g., food, medication, utilities);
    - Increased spending and purchases of unnecessary items or items he/she can't use;
    - Numerous withdrawals, including the maximum ATM withdrawal;
    - Checks written out of sequence; and
    - Large wire transfers to third-party beneficiaries who have unclear relationships with the elder.

- **Unexplained activity** – The activity may not make logical sense, given known details about the customer:
    - ATM withdrawals when the elder is homebound;
    - The sudden presence of overdrafts, when previously there had been limited to no insufficient funds activity;
    - Numerous unpaid bills, when someone has been designated to pay them;
    - An appearance of checks or signed documents when the elder cannot write or lacks the capacity to understand what he/she is signing, or the signature on checks and documents may not resemble the elder's signature.
- **Changes in account features** – The elder may request the addition of account features or changes to existing features, including:
    - Requesting the issuance of a credit or debit card for the first time;
    - Seeking to enrol in online banking;
    - Changing the account beneficiary; and
    - Requesting that statements be sent to an address besides his/her own.
- **Uncharacteristic requests** – The elder may seek to undertake a non-routine transaction, including:
    - Refinancing a mortgage;
    - Closing a certificate of deposit without regard to penalties for early withdrawal; or
    - Requesting to wire a large sum for no apparent purpose.

For guidance on additional red flags, please refer to the Suspicious Activity Red Flags section.

2526. What statistics and observations are available on elder financial abuse?

Following are some notable statistics and observations related to elder financial abuse:

- Multiple resources suggest that at least 20 percent of individuals over 65 years of age will be a victim of a financial crime.
- FinCEN has issued multiple advisories related to the rise in the targeting of elders in mortgage and healthcare fraud schemes, including but not limited to reverse mortgages and Medicare fraud.
- The top states for elder abuse-related SAR filings included California, Florida, Texas, New York, Washington and Hawaii.

Commonly reported activities included credit card fraud, check fraud, identity theft, wire transfer activity related to advance fee schemes, online dating scams, scams involving individuals posing as friends or family members in need of emergency funds, embezzlement and forgery. According to FinCEN, it is likely that past statistics did not truly reflect the magnitude of the problem of elder financial abuse, as many cases went unreported. After issuing advisories on the rise in elder financial

abuse, the number of SAR filings reporting such abuse increased significantly. Perhaps more importantly, financial institutions were able to prevent some cases of abuse by probing elderly customers during transactions that appeared out of character.

- Of the 1.98 million SAR filings from January 1, 2016 through December 31, 2016, reports of elder financial abuse totalled over 52,000 (3 percent) and were distributed across financial institution types as follows:
    - Money services businesses (MSBs): 30,000 cases (59 percent)
    - Depository institutions: 18,000 cases (36 percent)
    - Securities and futures firms: 1,420 cases (3 percent)
    - Other types of financial institutions (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily): 919 cases (2 percent)
    - Insurance companies: 211 cases (0.4 percent)
    - Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 33 cases (0.1 percent)
    - Casinos and card clubs: 11 cases (less than 0.1 percent)
    - Housing GSEs: 2 cases (less than 0.1 percent)

2527. What resources are available with respect to elder financial abuse?

The following guidance and advisories on elder financial abuse have been provided by FinCEN and other regulatory agencies:

- **Recommendations and Report for Financial Institutions on Preventing and Responding to Elder Financial Exploitation** (2016) by the Consumer Financial Protection Bureau (CFPB)
- **Interagency Guidance on Privacy Laws and Reporting Financial Abuse of Older Adults** (2013) (jointly with the Federal Reserve, the Commodity Futures Trading Commission [CFTC], CFPB, Federal Deposit Insurance Corporation [FDIC], Federal Trade Commission [FTC], National Credit Union Administration [NCUA], Office of the Comptroller of the Currency [OCC], Securities and Exchange Commission [SEC])
- **Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Elder Financial Exploitation** (2011) by FinCEN
- **Advisory to Financial Institutions on Filing Suspicious Activity Reports Regarding Home Equity Conversion Mortgage Fraud Schemes** (2010) by FinCEN
- **FinCEN Supports Efforts to Raise Awareness of Elder Financial Exploitation** (2012) by FinCEN
- **SAR Activity Review – Trends, Tips & Issues provides insight on suspected cases of elder financial abuse** (Various dates) by FinCEN

Other key organisations and initiatives include, but are not limited to, the following:

- The **Elder Justice Coordinating Council** was established in 2009 by the U.S. Department of Health and Human Services (HHS) to coordinate federal activities related to elder abuse, neglect and exploitation.
- Additionally, the **Health Care Fraud Prevention and Enforcement Action Team (HEAT)**, a joint effort between the U.S. Department of Health and Human Services (HHS) and the U.S. Department of Justice (DOJ), was established in 2009 to strengthen existing programs (e.g., Medicare, Medicaid), investigate fraud and invest in new resources to prevent future fraud, waste and abuse.
- The **American Bankers Association (ABA)**, through its Community Engagement Foundation, has partnered with **AARP** to conduct research and create resources to combat elder financial abuse.
- The **Elder Investment Fraud and Financial Exploitation (EIFFE) Prevention Program** was established by the Investor Protection Trust (IPT), a nonprofit organisation devoted to investor education, in partnership with the North American Securities Administrators Association (NASAA), the National Adult Protective Services Association (NAPSA), the American Academy of Family Physicians, the National Area Health Education Center Organisation and the National Association of Geriatric Education Centers. Created by the Baylor College of Medicine and funded by IPT, the EIFFE Prevention Program trains physicians, adult protective service professionals and other caregivers on how to identify and assist elders who are at risk or are victims of investment fraud.
- Another organisation established to address elder abuse in general is the **National Center on Elder Abuse (NCEA)**. Established by the U.S. Administration on Aging (AoA) in 1988, the NCEA serves as a national resource dedicated to the prevention of elder mistreatment. Publications on elder abuse and related issues can be found at the Clearinghouse on Abuse and Neglect of the Elderly (CANE).

Impact on Financial Institutions

2528. What role can financial institutions play with regard to combating elder financial abuse?

Financial institutions may become aware of potential abuse through their regular interactions with customers within their branch locations, through call center activity and via routine transaction monitoring. Branch personnel who are familiar with specific customers may note behavioural changes or other oddities in how the customer conducts business, including the presence of third-party influencers. Call center representatives may receive complaints about missing funds and inquiries about unrecognised transactions. Back-office personnel may note increased activity or activity that deviates from the customer's profile. Financial institutions should have escalation procedures to refer these types of anomalies for further investigation and for initiating reviews of customer activity.

2529. What should a financial institution do if it suspects potential elder financial abuse?

Financial institutions should report suspected elder financial abuse to FinCEN through Suspicious Activity Reports (SARs). Institutions should select the appropriate characterisation of suspicious activity in the Suspicious Activity Information section of the SAR form and specifically use the term "elder financial exploitation" in the SAR narrative. Institutions should also use the narrative to explain why the institution knows, suspects or has reason to suspect that the activity is suspicious. The potential victim of elder financial exploitation should not be reported as the subject of the SAR, but rather information on the victim should be included in the SAR narrative.

Many states have laws against elder financial abuse that may require financial institutions to contact state or local authorities and may impose additional requirements.

For additional guidance on SARs, please refer to the Suspicious Activity Reports section.

2530. What can financial institutions do to help prevent elder financial abuse?

Financial institutions can play an important role in preventing elder financial abuse by establishing programs that increase awareness of the risks and offering account security features that consider the needs of elder customers. Steps that financial institutions can take include, but are not limited to, the following:

- Develop policies that communicate the financial institution's position on elder financial abuse and implement procedures for how it will detect, investigate and report elder financial abuse to the authorities;
- Train employees about elder financial abuse schemes so that they recognise when a customer may be a potential victim and are sensitive to the heightened risk of elder customers;
- Assign responsible persons within the institution to whom employees should refer potential suspected elder financial abuse for further investigation and who will maintain awareness of industry trends and disseminate prevention techniques; and
- Educate customers on how to recognise the signs of elder financial abuse and the availability of resources for victim assistance, including alerting customers to possible scams as they appear.

2531. Are there instances in which a financial institution should notify law enforcement in advance of filing a SAR?

Whenever a violation is ongoing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

Anti-Bribery and Corruption Compliance Programs

Basics

2532. How is "corruption" defined?

Corruption is the abuse of one's official position for personal gain. Most often, corruption is the act of receiving a bribe. Transparency International (TI) classifies corruption into three categories, depending on the amount of money lost and the sector in which it occurred:

- **Grand Corruption** – "Acts committed at a high level of government that distort policies or the central functioning of the state, enabling leaders to benefit at the expense of the public good"; also referred to as kleptocracy;
- **Petty Corruption** – "Everyday abuse of entrusted power by low and mid-level public officials in their interactions with ordinary citizens, who often are trying to access basic goods or services in places like hospitals, schools, police departments and other agencies"; and
- **Political Corruption** – "Manipulation of policies, institutions and rules of procedure in the allocation of resources and financing by political decision makers, who abuse their position to sustain their power, status and wealth."

Columbia Law School administers the website "U.S. Anti-Corruption Oversight: A State-by-State Survey" that details state anti-corruption laws and institutions covering the following types of corruption:

- Influencing a public officer;
- Accepting gratuities or gifts;
- Official misconduct or abuse of public trust;
- Official oppression or official extortion;
- Embezzlement or misuse of public property;
- Misuse of official or confidential information by a public officer; and
- Fraudulent or unlawful interest in a public contract.

2533. How is "bribery" defined?

Bribery is the offering or giving of "something of value" in order to induce the recipient to abuse his or her position in some way for the benefit of the bribe payer or the person or entity on whose behalf the bribe is being offered or paid. Bribes can come in as anything of value (e.g., cash payments, gifts, jobs or internships).

2534. Is corruption/bribery considered a predicate crime for money laundering in the United States?

Yes. Corruption and bribery of a public official are two types of crimes underlying money laundering and terrorist financing activity in the United States. The USA PATRIOT Act, specifically Section 315 – Inclusion of Foreign Corruption Offenses as Money Laundering Crimes, includes the following as money laundering offenses:

- Bribery of a public official or the misappropriation, theft, or embezzlement of public funds by or for the benefit of the public official;
- Smuggling or export control violations related to certain goods (e.g., items on the U.S. Munitions list pursuant to the Arms Export Control Act of 1976 [AECA]);
- Any felony violations of the Foreign Corrupt Practices Act of 1977 (FCPA);
- Any felony violations of Foreign Agents Registration Act of 1938 (FARA);
- An offense with respect to multilateral treaties in which the United States would be obligated to extradite the offender or submit the case for prosecution if the offender were found in the United States.

The proceeds from corruption are often laundered. FinCEN defines "proceeds of foreign corruption" as "any asset of a senior foreign political figure acquired by misappropriation, theft, or embezzlement of public funds, the unlawful conversion of a foreign government's property, or through acts of bribery or extortion, including any other property into which the asset has been transformed or converted."

2535. What is the current scale of global corruption?

Measuring the current scale of corruption is extremely difficult. The Stolen Asset Recovery Initiative (StAR), the World Bank (WB) and the United Nations (UN) estimate between US$20 and US$40 billion in assets linked to foreign government corruption are lost by developing countries annually.

According to Transparency International's (TI) Corruption Perception Index (CPI) in 2016:

- The top five nations with the most corrupt public sectors included Somalia, South Sudan, North Korea, Syria and Yemen.
- Approximately 70 percent of the nearly 180 countries assessed by TI were perceived to have a serious corruption problem.
- The top five nations with the least corrupt public sectors are Denmark, New Zealand, Finland, Sweden and Switzerland.
- The United States ranked as the 18th least corrupt country out of nearly 180 jurisdictions with a corruption score of 74, higher than the global average corruption score of 43.

According to TI's Bribe Payers Index (BPI) in 2011, the top three sectors with companies which were more likely to offer bribes included the following:

- Public works contracts and construction

- Utilities
- Real estate, property, legal and business services

2536. What are the key U.S. anti-corruption laws and regulations?

The following are key U.S. federal laws and regulations addressing corruption and bribery:

- **Foreign Agents Registration Act (FARA)** (1938) – "Requires persons acting as agents of foreign principals in a political or quasi-political capacity to make periodic public disclosure of their relationship with the foreign principal, as well as activities, receipts and disbursements in support of those activities";
- **Foreign Corrupt Practices Act (FCPA)** (1977) – Prohibits the bribery of foreign officials for the purpose of obtaining or retaining business. For organisations with U.S.-listed securities, there are additional requirements regarding reasonable assurance provided by internal controls, as well as maintenance of books and records that accurately reflect transactions and both the nature and quantity of corporate assets and liabilities;
- **Office of Foreign Assets Control (OFAC)** – Administers multiple sanctions programs to address significant acts of corruption (e.g., political corruption, misappropriation of public assets and natural resources). For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section;
- **USA PATRIOT Act – Section 312** – Special Due Diligence for Correspondent Accounts and Private Banking Accounts (and Senior Foreign Political Figures) (2001);
- **USA PATRIOT Act – Section 315** – Inclusion of Foreign Corruption Offenses as Money Laundering Crimes (2001);
- **Kleptocracy Asset Recovery Initiative** (2010) – Established by the DOJ to forfeit the proceeds of foreign official corruption and/or return proceeds to benefit those harmed by the corrupt acts of the foreign officials;
- **Kleptocracy Asset Recovery Rewards Act (KARA)** (2016) – Authorises the Treasury to "pay rewards under an asset recovery rewards program to help identify and recover stolen assets linked to foreign government corruption and the proceeds of such corruption hidden behind complex financial structured in the United States and abroad."

2537. Do U.S. anti-corruption laws only target political figures?

No. The Federal Acquisition Regulation (FAR) – Improper Practices and Personal Conflict of Interest (2005) targets contractors of the U.S. federal government. FAR Part 3 imposes affirmative obligations on U.S. federal government contractors and subcontractors to comply with a wide range of laws including anti-bribery, procurement integrity, adherence to a written company code of business ethics and conduct and requires self-disclosure of violations of anti-corruption laws.

2538. What are "election crimes"? Are they covered under "political corruption"?

The U.S. Election Assistance Commission (EAC) defines "election crimes" as "all crimes related to the voter registration and voting processes and excludes civil wrongs and non-election related crimes."

Separate laws govern activities related to election crimes and campaign financing and fundraising (e.g., Federal Election Campaign Act of 1971 [FECA]). This section on corruption is focused on the activities of public officials after they have been elected to office, and therefore does not address election crimes.

2539. Who is responsible for examining for compliance with anti-corruption laws and regulations?

While the DOJ has primary responsibility for enforcing U.S. anti-corruption laws, regulatory authorities (e.g., Securities and Exchange Commission [SEC] for listed entities) share examination responsibilities.

2540. What key international treaties and conventions have influenced or shaped U.S. anti-corruption laws?

The United States adopted several international treaties, conventions and resolutions including, but not limited to, the following:

- **United States Proposal for an International Agreement on Illicit Payments** (1989) (Organisation for Economic Co-operation and Development [OECD]);
- **Inter-American Convention Against Corruption** (1996) (Organisation of American States [OAS]);
- **Convention on Combating Bribery of Foreign Public Officials in International Business Transactions** (1997) (OECD) including subsequent recommendations; Criminal Law Convention on Corruption (2000) (Council of Europe [COE]);
- **United Nations Convention Against Corruption (UNCAC)** (2006) (United Nations [UN]); and
- **Good Practice Guidance on Internal Controls, Ethics and Compliance** (2010) (OECD).

2541. How does the Financial Action Task Force (FATF) address corruption?

The Financial Action Task Force (FATF) includes corruption and bribery as designated categories of predicate offenses for money laundering. In 2012, FATF published Corruption: A Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight Against Corruption. Most, if not all, of the FATF Recommendations can be applied to an anti-corruption system as they address the following:

- Financial secrecy laws that do not inhibit monitoring and investigation of money laundering, terrorist financing and other financial crimes
- Adequate supervision and monitoring by competent authorities who have been appropriately vetted (e.g., proper screening and training of employees, adequate allocation of resources)

- Transparency in ownership (e.g., customer due diligence, identifying PEPs and beneficial owners of legal entities)
- Transparency in movement of transactions and assets (e.g., recordkeeping and reporting requirements of high-risk and potentially suspicious transactions)
- Asset recovery of proceeds from criminal activity (e.g., confiscation and forfeiture measures)
- International cooperation to assist in transnational criminal activity (e.g., mutual legal assistance)

For further guidance on the FATF Recommendations, please refer to the Financial Action Task Force section.

2542. Should financial institutions also focus on domestic instances of corruption and bribery?

While the primary focus is on cross-border or transnational corruption and bribery, financial institutions should have a risk-based due diligence program that addresses domestic risks of corruption and bribery.

2543. Is a "no bribery" policy sufficient to combat corruption?

No. Even with strong policies and codes of conduct forbidding bribery of foreign government officials, companies are at risk of being investigated and subjected to enforcement actions arising from allegations of improper payments to officials. Therefore, companies should also have, as examples, procedures for vetting any agents or third parties that may represent them and for monitoring financial transactions for possible improper payments.

2544. How did the Customer Due Diligence Requirements for Financial Institutions final rule (Beneficial Ownership Rule) impact the anti-corruption laws and regulations?

The Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule), finalised in July 2016, strengthen anti-corruption efforts by requiring the identification of beneficial owners of legal entity customers for covered institutions. One noted weakness in AML/CFT and anti-corruption laws and regulations was the inability to identify ultimate beneficial owners of accounts and assets. The Beneficial Ownership Rule addresses this gap. For further guidance, please refer to the Beneficial Owners section.

2545. How many instances of corruption have been reported on Suspicious Activity Reports (SARs)?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports of suspected corruption (foreign and domestic) totalled nearly 1,700 (0.08 percent) and were distributed across financial institution types as follows:

- Depository institutions: 1,157 cases (68 percent)
- Money services businesses (MSBs): 154 cases (9 percent)
- Securities and futures firms: 147 cases (9 percent)

- Other types of financial institutions: 142 cases (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily) (8 percent)
- Casinos and card clubs: 66 cases (4 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 24 cases (1 percent)
- Insurance companies: 11 cases (0.6 percent)
- Housing GSEs: 1 cases (0.1 percent)

2546. What are some examples of significant corruption cases and enforcement actions involving the United States and/or U.S. listed companies?

Following are examples of corruption cases and enforcement actions by various U.S. agencies:

- **Panama Papers/Bahamas Leaks**
  - In April 2016, over 11.5 million documents from Mossack Fonseca (MF), a Panama-based law firm specialising in the formation and management of entities in tax havens, were leaked by an anonymous source, identifying the beneficial owners of 214,000 offshore entities, according to the International Consortium of Investigative Journalists (ICIJ). In September 2016, the same source that leaked the Panama Papers also leaked information from the Bahamas corporate registry, linking approximately 140 international and local politicians to offshore companies in the Bahamas. The ICIJ published the leaked information in its Offshore Leaks Database. As a result of the leaks, regulatory and tax authorities have launched investigations in numerous countries (e.g., United States, United Kingdom, Germany, Australia, Sweden, Hong Kong, Chile, Singapore, India). According to media reports, in February 2017, the two founders of Mossack Fonseca were arrested for their alleged involvement in a separate money laundering investigation involving corruption in Latin America. The Panama Papers/Bahama Leaks has corruption, tax evasion and cybersecurity implications. For further guidance, please refer to the sections: Offshore Tax Evasion and Voluntary Tax Compliance Programs and Cyber Events and Cybersecurity.
- **1Malaysia Development Berhad (1MDB)**
  - In July 2016, the DOJ initiated the largest ever kleptocracy-related asset forfeiture action, in which allegations of the misappropriation of approximately US$3.5 billion from Malaysia's sovereign wealth fund, 1Malaysia Development Berhad (1MDB), led to the seizure of US$1 billion of assets in the U.S., the UK and Switzerland. The seized assets included luxury hotels, penthouse apartments, mansions, a private jet and an ownership interest in the production company that produced the movie "The Wolf of Wall Street." Funds were also used to purchase artwork and pay gambling expenses. The alleged offenses took place between 2009 and 2015. Although Malaysia Prime Minister Najib Razak chaired 1MDB, the DOJ lawsuit did not name him. Razak's step-

son Riza Aziz was named as a "relevant individual" along with two government officials and a private businessman. According to media reports, the DOJ investigation into 1MDB was triggered by a data leak by Xavier Justo, a former employee of PetroSaudi, an oil services company, founded by Saudi nationals, Tarek Obaid and Prince Turki bin Abdullah. Multiple businesses and foreign officials have been implicated in these leaks, including PetroSaudi and the United Arab Emirates ambassador to the United States, Yousef al-Otaiba.

- **Petroleo Brasileiro SA (Petrobas)**
  - In 2014, the U.S. Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) initiated an investigation into Petrobas for possible violations of the FCPA by overpaying contractors and funnelling excess funds illegally to political parties totalling US$1.6 billion. More than 150 people have been arrested so far. In recent years, the investigation has expanded to include other companies with ties to Petrobas that have securities that trade in the United States (e.g., Qdebrecht SA, OAS SA, Andrade Gutierrez SA).
- **Fédération Internationale de Football Association (FIFA) and Central American and Caribbean Association Football (CONCACAF)**
  - In 2015, the DOJ unsealed a 47-count indictment charging 14 defendants, many of whom were high-ranking officials in FIFA and CONCACAF with racketeering, wire fraud, money laundering conspiracies and other offenses in connection to a 24-year scheme to enrich themselves through the corruption of international soccer. Over US$150 million in bribes and kickbacks were paid to obtain lucrative media and marketing rights to international soccer tournaments. The DOJ did not file charges pursuant to FCPA as the FCPA narrowly covers bribes of government officials.
- The **DOJ** addresses violations of the anti-bribery provision of the FCPA:
  - Since the passage of the FCPA in 1977, the DOJ has initiated nearly 250 enforcement actions. Details of each enforcement action are provided on the DOJ's website at: http://www.justice.gov/criminal/fraud/fcpa/cases/a.html.
- The **SEC** addresses violations of the accounting provision of the FCPA:
  - The SEC has initiated more than 170 enforcement actions, with five in January 2017 alone. Details of each enforcement action are provided on the SEC's website at https://www.sec.gov/spotlight/fcpa/fcpa-cases.shtml.
- **FinCEN** listed the following cases as examples of corruption-related investigations aided by data provided on BSA reports (e.g., SARs, CTRs):
  - **Casino Currency Transaction Reports Help Track Funds Embezzled from a Public Utility**
  - **Corrupt Official Convicted on Numerous Charges Including Structuring**

  - **Credit Union's Suspicious Activity Reports Lead to Arrest of Corrupt Utilities Employees**
  - **Local Official Sentenced for Tax Evasion and Structuring**
  - **Proactive SAR Review Leads to the Arrest of Army Officer and Recovery of Iraqi War Funds**
  - **SAR Leads to Recovery of Funds Derived from Foreign Corruption**
  - **SARs Help Uncover Bid-Rigging Scandal**
  - **Suspicious Activity Report Leads to Arrest and Conviction of U.S. Government Employee for Embezzlement**
  - **Suspicious Activity Reports Identify Transactions Linked to Embezzlement at a Tribal Authority**

- U.S. Department of Homeland Security's (DHS) **Immigration and Customs Enforcement** (ICE):
  - According to ICE, since the inception of their Foreign Corruption Investigations Group in 2003, nearly 400 investigations have been initiated resulting in nearly 280 indictments and the seizure of over US$150 million in assets associated with foreign corruption. Specific examples of investigations and cases are provided on ICE's website at www.ice.gov/foreign-corruption.

2547. What key groups have provided guidance and resources on corruption and anti-corruption?

The following key groups have provided guidance or resources related to corruption and anti-corruption efforts:

- The SEC and the DOJ are responsible for enforcing the FCPA. In 2012, they released **A Resource Guide to the Foreign Corrupt Practices Act**, providing guidance on an effective anti-corruption compliance program, including third-party risk due diligence and compliance programs.
- The **International Corruption Unit (ICU)** was established in 2008 by the Federal Bureau of Investigation (FBI) to oversee FCPA cases, International Contract Corruption Task Forces and anti-trust cases. ICU investigations involve global fraud and the corruption of foreign federal public officials involving the U.S. government, funds, persons and businesses.
- The Fraud Section of the DOJ published **The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance** (2016) to provide guidance on their enforcement strategy which includes a pilot program that provides a mechanism for companies to voluntarily disclose FCPA-related misconduct.
- The DOJ's **Public Integrity Section** (PIN), established in 1976, oversees federal efforts to combat corruption (e.g., criminal misconduct, election fraud, campaign financing crimes,

patronage crimes) through the prosecution of election and appointed public officials at all levels of government. PIN published the **Federal Prosecution of Election Offenses** (7th Edition) in May 2007 that provides an overview of election crimes, key statutes, investigative considerations, significant cases and other insights into the prosecution of these types of crimes. Annually, PIN publishes Report to Congress on the Activities and Operations of the Public Integrity Section.

- The DOJ's **Money Laundering and Asset Recovery Section (MLARS**) leads the asset forfeiture and AML enforcement efforts and is comprised of seven units and associated teams: Bank Integrity Unit, International Unit, Policy Unit, Program Management and Training Unit, Program Operations Unit and the Special Financial Investigations Unit.
- Immigration and Customs Enforcement's (ICE) **Foreign Corruption Investigations Group** within the U.S. Department of Homeland Security (DHS) investigates cases of corrupt foreign officials who attempt to place their illicit funds into the U.S. financial system.
- **Stolen Asset Recovery Initiative (StAR)** – Established in 2007, a partnership between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC) that works with developing countries and financial centres to prevent the laundering of the proceeds of corruption and to facilitate a systematic and timely method of returning stolen assets. In 2011, StAR published the Asset Recovery Handbook: A Guide for Practitioners.
- **G20 Anti-Corruption Working Group** commits members to international anti-corruption, anti-bribery and asset recovery efforts. The G20 Anti-Corruption Action Plan 2013 – 2014 outlines commitments, including, but not limited to, ratification of the United Nations Convention Against Corruption (UNCAC), implementation and enforcement of anti-bribery legislation, denying entry and safe havens to corrupt officials, asset recovery, whistleblower programs, prevention of corruption in the public sector and international cooperation. Members have also published Asset Recovery Guides by country to assist international efforts to recover illicit proceeds from foreign corruption.
- **Financial Crimes Enforcement Network** (FinCEN)
    - **SAR Activity Review – Trends, Tips and Issues** (Issue 19, 2011) highlighted regulatory requirements, due diligence procedures and frequently asked questions related to senior foreign political figures and corruption.
    - **Guidance to Financial Institutions on Filing Suspicious Activity Reports regarding the Proceeds of Foreign Corruption** (2008)
    - **Interagency Guidance on Accepting Accounts from Foreign Embassies, Consulates and Missions** (2011)
    - **Guidance on Accepting Accounts from Foreign Governments, Foreign Embassies and Foreign Political Figures** (2004)
- Additional guidance by Protiviti related to anti-corruption includes:
    - **Taking the Best Route to Managing Fraud and Corruption Risks** (2016)

  - **Addressing Fraud Effectively Begins with Managing Third-Party Corruption** (2014) (podcast)
  - **Overcoming Roadblocks to Effective Anti-Corruption Measures** (2014) (video)
  - **A Strong Compliance Culture Starts with Managing Third-Party Corruption** (2014)
  - **Viewing Your Anti-Corruption Efforts Through the Lens of the Hallmarks of an Effective Compliance Program** (2013)
  - **Anti-Bribery and Anti-Corruption Compliance: IPO/SOX Readiness** (2013)
  - **Protiviti Flash Report: Is Department of Justice Dismissal of Morgan Stanley Case a Litmus Test for Corruption Risk Compliance?** (2012)
  - **Even Retailers and Consumer Products Manufacturers Must Manage Compliance with the U.S. Foreign Corrupt Practices Act and Other Anti-Bribery Laws** (2012)

- The United Kingdom's Ministry of Justice published **The Bribery Act 2010: Guidance to Help Commercial Organisations Prevent Bribery** and **The Bribery Act 2010: Quick Start Guide** to help organisations comply with the UK Bribery Act of 2010, the U.K.'s counterpart to the FCPA which is broader in scope.
- **Transparency International (TI)**:
  - **Gateway: Corruption Assessment Toolbox –** A database of diagnostic tools and topic guides related to measuring corruption and identifying gaps in anti-corruption programs.
  - Indices, Surveys, Assessments and Publications:
    - The **Corruption Perceptions Index** (CPI), launched in 1995, measures the perceived level of public-sector corruption in 180 countries and territories around the world based on multiple surveys. The CPI shows a country's ranking (score is based on a scale of 1 to 10, with 10 being the least corrupt), the number of surveys used to determine the score, and the confidence range of the scoring. CPI reports are published annually.
    - The **Bribe Payers' Index** (BPI), launched in 1999, assesses the supply side of corruption and ranks corruption by source country and industry sector. BPI reports have been released in 2002, 2006, 2008 and 2011.
    - The **Global Corruption Barometer** (GCB) is a public opinion survey, launched in 2003, that assesses the general public's perception and experience of corruption in more than 100 countries. The latest GCB survey was released in 2013.

- **National Integrity System Assessments** (NIS) country reports present the results of the NIS assessment in the form of a comprehensive analysis of the anti-corruption provisions and capacities in a country, including recommendations for key areas of anti-corruption reform. In 2012, TI published "Money, Politics, Power: Corruption Risks in Europe" which summarised the findings of 25 National Integrity System assessments carried out across Europe in 2011.
- **Business Principles for Countering Bribery: A Multi-Stakeholder Initiative Led by Transparency International** (2013), builds from earlier editions of Business Principles for Countering Bribery (2003, 2009), by providing a framework for anti-bribery programs. Topics covered include conflicts of interest; bribes; political contributions; charitable contributions and sponsorships; facilitation payments; gifts, hospitality and expenses; and requirements for risk-based anti-bribery programs (e.g., code of conduct, policies and procedures, risk management, internal and external communication, training, oversight, reporting and recordkeeping, monitoring and independent assurance/testing).

– **Working Papers and Global Corruption Reports** includes a series of reports on various topics related to corruption and anti-corruption practices including, but not limited to, the following:

- Exporting Corruption: Progress Report 2015: Assessing Enforcement of the OECD Convention on Combating Foreign Bribery (2015)
- Integrity of Public Officials in EU Countries: International Norms and Standards (2015)
- 2015 and Beyond: The Governance Solution for Development (2013)
- Business Principles for Countering Bribery: A Multi-Stakeholder Initiative Led by Transparency International (2013)
- Corporate Responsibility and Anti-Corruption: The Missing Link? (2010)
- Making Government Anti-Corruption Hotlines Effective (2009)
- Corruption and Local Government (2012)
- Corruption in the [Middle East and North Africa] MENA Region: A Declining Trend or More of the Same? (2008)
- Corruption and Sport: Building Integrity and Preventing Abuses (2009)
- Recovering Stolen Assets: A Problem of Scope and Dimension (2011)
- Corruption in the Land Sector (2011)
- Corruption and Human Trafficking (2011)
- Corruption and Public Procurement (2010)

    - Corruption and (In)security (2008)
    - Accountability and Transparency in Political Finance (2008)
    - Education (2013)
    - Climate Change (2011)
    - Corruption and the Private Sector (2009)
    - Corruption in Judicial Systems (2007)
    - Corruption and Health (2006)
    - Political Corruption (2004)
- **Policy Positions** includes a series of publications that provide guidance in developing anti-corruption policies, including, but not limited to, the following:
    - Controlling Corporate Lobbying and Financing of Political Activities (2009)
    - Building Corporate Integrity Systems to Address Corruption Risks (2009)
    - Making Anti-Corruption Regulation Effective for the Private Sector (2009)
    - Countering Cartels to End Corruption and Protect the Consumer (2009)
    - Strengthening Corporate Governance to Combat Corruption (2009)
    - Political Finance Regulations: Bridging the Enforcement Gap (2009)
    - Effectively Monitoring the United Nations Convention against Corruption (UNCAC) (2011)
    - Standards on Political Funding and Favours (2009)
- **Policy Briefs** including, but not limited to, the following:
    - Closing Banks to the Corrupt: The Role of Due Diligence and PEPs (2014)
    - Regulating Luxury Investments: What Dirty Money Can't Buy (2014)
    - Leaving the Corrupt at the Door: From Denial of Entry to Passport Sales (2014)
    - Ending Secrecy to End Impunity: Tracing the Beneficial Owner (2014)
- The **Anti-Corruption Research News** provides users with insights and activities in anti-corruption research on knowledge gaps and emerging risks, curriculum development, jobs, funding opportunities and research events on a quarterly basis.
- The **Anti-Corruption Plain Language Guide** provides standardised definitions for key terms commonly used by the anti-corruption movement.
- **The Anti-Corruption Kit: 15 Ideas for Young Activists** (2014), published by Transparency International, provides a step-by-step guide to help young people raise

awareness and fight corruption using a variety of methods from technology solutions to comics and theatre.

- **United Nations (U.N.)**
  - **Stolen Asset Recovery Initiative (StAR)** – A partnership between the United Nations Office on Drugs and Crime (UNODC) and the World Bank (WB) that provides policy analysis and proposal, case assistance and capacity building in developing countries to build anti-corruption and asset recovery systems.
  - **Tools and Resources for Anti-Corruption Knowledge (TRACK)** – A web-based anti-corruption portal launched in 2011 by the UNODC with tools and resources for the private sector, academia and civil society. Resources include legal libraries, training and analytical tools related to anti-corruption and asset recovery.
  - **Assessment of the Integrity and Capacity of the Justice System in Three Nigerian States** – A publication created in 2006 that presents statistics and data drawn from live interviews held with specific groups within the justice system.
  - **Compendium of International Legal Instruments on Corruption, 2nd Edition** – A publication created in 2005 that contains all the major relevant international and regional treaties, agreements, resolutions and other instruments related to corruption.
  - **Global Action Against Corruption: The Mérida Papers** – A publication highlighting the key topics addressed in the United Nations Office on Drugs and Crime in Mérida, Mexico, in 2003, including, but not limited to, the following:
    - Preventive Measures against Corruption: the Role of the Private and Public Sectors
    - The Role of Civil Society and the Media in Building a Culture against Corruption
    - Legislative Measures to Implement the United Nations Convention against Corruption
    - Measures to Combat Corruption in National and International Financial Systems
    - International Group for Anti-Corruption Coordination: Report of the Fifth Meeting
  - **Technical Guide to the United Nations Convention Against Corruption** – A publication created in 2009 by the UNODC and the United Nations Interregional Crime and Justice Research Institute (UNICRI) to promote the implementation of the United Nations Convention against Corruption (UNCAC), the first global legally binding instrument in the fight against corruption, which was adopted by the United Nations in 2003.

- **Financial Action Task Force (FATF)**
  - **FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22) –** A publication created in June 2013 which details best practices for detecting and conducting due diligence on PEPs in accordance with Recommendation 12 – Politically Exposed Persons and Recommendation 22 – DNFBPs: Customer Due Diligence. Topics covered include foreign and domestic PEPs; beneficial ownership; sources of information used to detect and identify PEPs; red flags for potentially suspicious activity and examples of abuse (e.g., use of corporate vehicles to obscure ownership).
  - **Best Practices Paper: The Use of FATF Recommendations to Combat Corruption** – A publication created in October 2013 that builds on past FATF guidance on corruption and politically exposed persons (PEPs) and summarises anti-corruption best practices identified by AML/CFT and anti-corruption experts in partnership with the G20 Anti-Corruption Working Group (ACWG). Topics covered include relevant AML/CFT measures for combating corruption; key risk factors; best practices for cooperation and examples of successful co-ordination and co-operation efforts.
  - **Corruption: A Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight against Corruption** – A publication created in October 2012 which details how to use the FATF Recommendations to combat corruption. Topics covered include identifying politically exposed persons (PEPs); safeguarding and increasing transparency of the public sector (e.g., law enforcement, regulatory authorities) and financial systems; detecting, investigating and prosecuting corruption and money laundering; and recovering stolen assets.
  - **Specific Risk Factors in Laundering the Proceeds of Corruption – Assistance to Reporting Institutions** – A publication created in June 2012 specifically to help reporting institutions in better analysing and understanding risk factors for corruption-related money laundering, including politically exposed persons (PEPs).
  - **Laundering the Proceeds of Corruption** – A publication created in July 2011 that describes links between corruption and money laundering drawn from publicly available expert resources and identifies key vulnerabilities within the current AML/CFT framework.
- **Organisation for Economic Co-operation and Development (OECD)**
  - **OECD Working Group on Bribery** (2014) – This annual report from the working group gives an update on progress of enforcement actions by several member states, outlines targeted public statements regarding parties that have not yet implemented the key recommendations, while the results of a survey of member states show they

want more focused and less general monitoring of enforcement of the Convention on Bribery.

  - **Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and Related Documents** (2011) - This publication sets out articles of the Convention on Combating Bribery of Foreign Public Officials and provides commentary on the application of the convention in international business transactions as well as recommendations on tax measures for further combating bribery of foreign officials in international business transactions. The paper also provides the council's recommendations on bribery and officially-supported export credits and for the development of cooperation actors on managing the risk of corruption.
  - **Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors** (2013) - This handbook seeks to raise the awareness of tax examiners and auditors of issues concerning bribery and other forms of corruption and provides guidance on how to recognise indicators of possible bribery or corruption in the course of regular tax examinations and audits.
  - **OECD Bribery Awareness Handbook for Tax Examiners** (2009) - This handbook provides tax examiners with information on the various bribery techniques used and the tools to detect and identify bribes. The 2009 edition also includes the Recommendation on Tax Measures for Further Combating Bribery of Foreign Public Officials in International Business Transactions, which requires countries to explicitly prohibit the tax deductibility of bribes to foreign public officials and promotes enhanced co-operation between tax authorities and law enforcement agencies both at home and abroad to counter corruption.

- **Egmont Group of Financial Intelligence Units (Egmont Group)**
  - **The Role of FIUs in Fighting Corruption and Recovering Stolen Assets** – An FIU can be an important element of fighting corruption-related offenses, and preventing the laundering of illicit funds which stem from corruption activities. Published in 2012, this report details the results of a study aimed at increasing awareness of corruption and asset recovery among FIUs, and presents case scenarios and best practices. It also describes the position and the role of the FIU in the asset recovery process.
- **World Bank (WB)**
  - **Left Out of the Bargain: Settlements in Foreign Bribery Cases and Implications for Asset Recovery –** A publication created in 2014 that summarises global settlement practices as they relate to foreign bribery cases by the WB.
  - **Barriers to Asset Recovery: An Analysis of the Key Barriers and Recommendations for Action –** A publication created in 2011 that provides an

overview on the existing difficulties in stolen asset recovery actions and key recommendations by the WB.

- **Wolfsberg Group**
  - **The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption** (2015) - These FAQs provide answers to some of the numerous questions that arise as a result of financial crime risk assessments as well as providing some guidance on how to address them based on the opinion of The Wolfsberg Group. The Group believes that these FAQs will contribute to the promotion of effective risk management and further prevent the use of financial institutions for criminal purposes.
  - **Wolfsberg Anti-Corruption Guidance** (2011) (replaces previous guidance issued in 2007) – This is a revised, expanded and renamed version of the 2007 paper: Wolfsberg Anti-Corruption Guidance, which incorporates new developments such as the UK Bribery & Corruption Act and gives tailored advice to international financial institutions in support of their efforts to develop appropriate anti-corruption programs, to combat and mitigate bribery risks associated with clients or transactions and also to prevent internal bribery. This guidance paper has an entirely new Appendix that sets out the elements for an internal anti-corruption framework, with sections on roles and responsibilities, reporting, policies and the programme framework, including risk assessments and due diligence in relation to third parties, among others.

Senior Foreign Officials and Politically Exposed Persons

2548. Is a "foreign official" the same as a "politically exposed person (PEP)" as defined by Section 312 of the USA PATRIOT Act?

The FCPA defines "foreign official" as "*any officer or employee* [emphasis added] of a foreign government or any department, agency, or instrumentality thereof, or of a public international organisation, or any person acting in an official capacity for or on behalf of any such government or department, agency, or instrumentality, or for or on behalf of any such public international organisation."

The term "politically exposed person (PEP)" focuses on "senior" foreign officials but also includes immediate family members and close associates. PEP is defined by Section 312 of the USA PATRIOT Act as a "senior foreign political figure" which includes:

- A current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not);
- A senior official of a major foreign political party;
- A senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual;

- An immediate family member of such an individual; or
- Any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual.

"Immediate family member" means an individual's spouse, parents, siblings, children and spouse's parents or siblings. "Senior official" or "senior executive" means an individual with substantial authority over policy, operations or the use of government-owned resources.

2549. Has FATF's definition of "politically exposed person" (PEP) evolved?

Yes. FATF has expanded the definition of a PEP by breaking it down into two categories: foreign PEPs and domestic PEPs.

Foreign PEPs are defined as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials). FATF also states that business relationships with family members or close associates of PEPs have similar reputational risks to PEPs themselves, and therefore should be included in the definition of PEP, as well.

FATF advises that the definition of PEP was not meant to include junior- or middle-ranking individuals in the categories mentioned above. FATF also suggests that persons who are or have been entrusted with a prominent function by an international organisation (e.g., deputy directors, and members of the board or equivalent functions) be considered in the definition of PEP.

Domestic PEPs are individuals who are, or have been, entrusted domestically with prominent public functions (e.g., heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).

2550. How does the BSA's definition of beneficial owner compare to that outlined by FATF?

After the implementation of the Beneficial Ownership Rule, the first prong of the BSA's definition of "beneficial owner" parallels that outlined by FATF by applying a 25 percent threshold for determining due diligence measures, with some exceptions. Additionally, the BSA adds a second prong, the "control" prong, which may be a party who does not meet the ownership test.

Prior to the implementation of the Beneficial Ownership Rule, Section 312 of the USA PATRIOT Act required covered institutions (e.g., depository institutions, broker-dealers in securities) to conduct due diligence on beneficial owners defined as "individual[s] who [have] a level of control over [of 10 percent], or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual[s], directly or indirectly, to control, manage or direct the account."

For further guidance, please refer to Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Beneficial Owners.

2551. Should financial institutions "de-risk" by not providing services to PEPs and their close associates?

De-risking often refers to a financial institution's policy to exit from a high-risk activity to reduce its inherent risk profile. To avoid risk, as opposed to managing risk, some financial institutions may opt out of offering services to certain categories of high-risk customers (e.g., foreign correspondents, money transmitters, marijuana-related businesses [MRBs]) or customers located in high-risk geographies. While this may reduce risk and simplify the KYC and suspicious activity monitoring programs of individual financial institutions, it may increase overall money laundering risk as money is moved through less transparent or less regulated financial systems (e.g., hawalas, financial institutions in lax AML/CFT jurisdictions).

Many financial institutions have taken steps to de-risk because of perceived regulatory pressures. U.S. and international authorities, however, have released guidance cautioning against wholesale de-risking while attempting to provide further clarification on regulatory expectations on servicing inherently high-risk customers (e.g., Office of the Comptroller of the Currency [OCC] Risk Management Guidance on Foreign Correspondent Banking, Federal Deposit Insurance Corporation [FDIC] Financial Institution Letter: Statement on Providing Banking Services, Financial Action Task Force [FATF] Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking, International Monetary Fund [IMF] The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action).

For further guidance, please refer to the Risk Assessments section.

Foreign Corrupt Practices Act

2552. What is the Foreign Corrupt Practices Act (FCPA)?

One of the key anti-corruption laws in the United States is the Foreign Corrupt Practices Act of 1977 (FCPA). U.S. organisations and those with U.S.-listed securities must comply with the FCPA, which prohibits the bribery of foreign officials for the purpose of obtaining or retaining business. Bribes (e.g., offers, payments, promises, gifts) must be made with a corrupt intent (e.g., intended to induce the recipient to misuse his official position) in order to be considered a violation of the FCPA.

For organisations with U.S.-listed securities, there are additional requirements regarding reasonable assurance provided by internal controls, as well as maintenance of books and records that accurately reflect transactions and both the nature and quantity of corporate assets and liabilities.

2553. How is the term "third party" defined? Which types of third parties pose the most risk?

The term "third party" often means different things to different organisations but is generally defined as any commercial partner that provides goods and services to, but is not owned by, the organisation. Many organisations distinguish suppliers (e.g., providers of goods and services to the organisation that rarely have direct contact with customers or act on the organisation's behalf) from business intermediaries (e.g., commercial partners that engage with customers, government agencies or other third parties on behalf of the organisation). The latter poses heightened risk for violations of anti-corruption and anti-bribery laws and regulations.

Examples of third parties may include, but are not limited to, the following:

- Accounting firms
- Agents (e.g., sales agents, business development agents)
- Charitable organisations
- Channel partners
- Consultants
- Customs brokers
- Distributors
- Engineering, procurement and construction (EPC)
- Environmental consultants
- Freight forwarders
- General contractors
- Investigative firms
- Joint venture partners
- Law firms
- Lobbyists
- Resellers
- Subcontractors
- Suppliers
- Tax consultants
- Visa expeditors

For further guidance on third-party risk, please refer to Know Your Third Parties and Know Your Customer's Customer section.

2554. What are the components of an effective anti-bribery and corruption compliance program (ABC Compliance Program)?

An effective ABC Compliance Program includes the following 10 components:

- Commitment from senior management and a clearly articulated statement of anti-corruption culture and policy to prevent bribery;
- Code of conduct and compliance policies and procedures, specific to payments (e.g., gifts, hospitality, facilitation payments);
- Oversight, accountability, autonomy and resources;
- Risk assessment;
- Training and continuing advice;
- Incentives to prevent bribery and disciplinary measures for noncompliance and violations of the law;
- Third-party anti-corruption due diligence program (e.g., risk scoring, questionnaires, written agreements, certifications, training);
- Confidential reporting (e.g., whistleblower) and internal investigations of suspected instances of bribery and corruption;
- Continuous improvement: periodic testing and review of the anti-bribery program; and

- Mergers and acquisitions: pre-acquisition due diligence and post-acquisition integration.

2555. What are the components of an effective third-party anti-corruption due diligence program?

A third-party anti-corruption due diligence program that includes the following components will likely reduce exposure to potential bribery and corruption violations over time:

- Determine the scope of the program (e.g., clearly define "third party," limit to "business intermediaries," limit by dollar-volume threshold);
- Use a risk-scoring process that uses more data points than just high-risk geographies (e.g., jurisdiction designated as high risk by Transparency International [TI]) to group third parties quickly into categories (e.g., high, moderate, low) to determine level of due diligence to be performed on third party;
- Utilise publicly available sources (e.g., media-centric) to conduct initial due diligence; and
- Perform enhanced due diligence on an exception basis.

An example workflow process for a third-party anti-corruption due diligence program may include the following steps:

- Business sponsor initiates onboarding or contract renewal of third party;
- Third party completes questionnaire;
- Sponsor reviews questionnaire and submits for risk-scoring;
- Risk score determines level of due diligence to be performed on third party (e.g., publicly available or enhanced);
- Sponsor conducts appropriate level of due diligence;
- Sponsor follows up on action items identified by compliance from due diligence;
- Compliance reviews due diligence reports and changes/updates disposition accordingly (e.g., approve, need additional information, disapprove); and
- Compliance establishes monitoring timetable once the third party is approved (e.g. watchlist monitoring, audits, periodic reviews of disbursements, contracts, gifts, travel, entertainment expenses).

2556. Should third-party anti-corruption due diligence programs be applied to existing third parties in addition to new ones?

While initial efforts should focus on new third parties, existing intermediaries should be subject to the anti-corruption due diligence program as well. Populations of existing third parties can be selected and prioritised by utilising a combination of a risk-based approach (e.g., jurisdiction, relationship type, aggregate dollar volume) and event triggers (e.g., contract renewal, media alert).

2557. What are some examples of due diligence findings that may heighten the corruption risks of third parties?

The following are some examples of findings that may heighten corruption risks of third parties:

- Prior FCPA enforcement actions;
- Undisclosed presence of conflicts of interest or foreign officials in positions of authority;
- Name matches between company owners or executives and debarred persons or government officials;
- A history of export control or environmental violations;
- Affiliated companies or a corporate parent involved in prior or ongoing scandals; and
- Other historical or pending scandals that could negatively affect suitability of a third party as a business partner.

2558. Should financial institutions voluntarily disclose FCPA-related misconduct?

The Fraud Section of the DOJ published "The Fraud Section's Foreign Corrupt Practices Act Enforcement Plan and Guidance" (2016) to provide guidance on their enforcement strategy which includes a pilot program that provides a mechanism for companies to voluntarily disclose FCPA-related misconduct. The pilot program builds on the Individual Accountability for Corporate Wrongdoing memorandum (Yates Memo) published in September 2015 by former Deputy Attorney General Sally Quillian Yates, the Principles of Federal Prosecution of Business Organisations (USAM Principles) and the United States Sentencing Guidelines. Companies will be able to obtain "mitigation credit" for voluntary disclosures dependent upon the following:

- Timely and full disclosure of all relevant facts of the FCPA violation(s);
- Level of cooperation with investigation;
- Timely and appropriate remediation efforts; and
- Disgorgement from all profits resulting from the FCPA violation.

The Fraud Section may also consider the following factors in determining mitigation credit:

- Involvement/lack of involvement of executive management;
- Size of the profit resulting from the FCPA violation;
- Company history of non-compliance; and
- Prior resolutions with the DOJ within the past five years.

Financial institutions should consult with counsel before voluntarily disclosing violations.

2559. Should financial institutions be concerned with corruption-related activities beyond the bribery of foreign officials?

Yes. While the FCPA focuses on the payment of bribes to foreign officials, in some jurisdictions such as the United Kingdom, laws extend beyond foreign officials and also apply to the act of receiving bribes. Financial institutions should be aware of other corruption-related activities as part of their broader anti-corruption and AML/CFT efforts as they can be exposed to corruption in many ways, including, but not limited to, the following:

- Insiders (e.g., employees, directors) who, in addition to paying bribes, receive bribes and/or provide special services to third parties, including corrupt foreign officials
- Corrupt foreign officials as account holders who deposit bribes or stolen, embezzled or misappropriated public funds
- Beneficial owners of accounts or other products and services who may be corrupt foreign officials
- Customers who transfer funds to/from or on behalf of corrupt foreign officials
- Third parties (e.g. agents, consultants, distributors, suppliers) who pay bribes, especially when conducting international business on behalf of the financial institution

Asset Recovery

2560. How are "stolen assets" defined?

The Kleptocracy Asset Recovery Act (KARA) of 2016, which has been proposed in the U.S. House of Representatives, defines "stolen assets" as "financial assets within the jurisdiction of the United States, constituting, derived from or traceable to, any proceeds obtained directly or indirectly from foreign government corruption."

According to KARA, of the US$20 to US$40 billion lost by developing countries annually, the U.S. estimates that approximately US$5 billion has been repatriated in the past 15 years.

2561. What mechanisms are in place to recover stolen assets?

Multiple mechanisms are in place or are proposed to aid in the recovery of stolen assets, including, but not limited to, the following:

- The DOJ's **Money Laundering and Asset Recovery Section (MLARS)** leads the asset forfeiture and AML enforcement efforts and is comprised of seven units and associated teams: Bank Integrity Unit, International Unit, Money Laundering and Forfeiture Unit, Policy Unit, Program Management and Training Unit, Program Operations Unit and the Special Financial Investigations Unit;
- The **Whistleblower Program** – Established in 1867, the IRS rewards individuals who provide specific and credible information that leads to the collection of taxes, penalties, interest or other amounts from noncompliant taxpayers;

- The **Securities Whistleblower Incentives and Protection** program – Established by Section 21F of the Securities and Exchange Act of 1934 and implemented and enhanced by Section 922 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (2010), the SEC rewards individuals who provide original information about a violation of federal securities laws, including violations of the FCPA, that leads to the successful enforcement of a covered judicial or administrative action or related action. Additional provisions prohibit retaliation by employers against whistleblowers. Whistleblowers are not required to be employees to submit information or be eligible to receive rewards. In 2017, the U.S. Supreme Court is expected to rule on whether this provision protects whistleblowers who report violations within their companies and not specifically to the SEC;
- The **Office of Foreign Assets Control (OFAC)** - Administers multiple sanctions programs to address significant acts of corruption (e.g., political corruption, misappropriation of public assets and natural resources), drug trafficking, terrorism and other criminal acts. OFAC has the authority to freeze/block assets of Specially Designated Nationals (SDNs). Under certain conditions pursuant to the Terrorism Risk Insurance Act of 2002 (TRIA), frozen assets can be used to satisfy judgments against terrorist parties. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section;
- **USA PATRIOT Act Section 319 – Forfeiture of Funds in U.S. Interbank Accounts** (2001) **-** Section 319(a) provides for seizure by U.S. authorities of funds in U.S. interbank accounts. If funds are deposited into an account at a foreign bank, and that foreign bank has an interbank account in the United States with a U.S. bank, broker-dealer or branch or agency of that foreign bank, the funds are deemed to have been deposited in the U.S. interbank account and are potentially subject to seizure. There is no requirement that the funds deposited in the U.S. interbank account be traceable to the funds deposited in the foreign bank. For further guidance, please refer to the USA PATRIOT Act section;
- **Stolen Asset Recovery Initiative (StAR)** – Established in 2007, a partnership between the World Bank Group and the United Nations Office on Drugs and Crime (UNODC) that works with developing countries and financial centres to prevent the laundering of the proceeds of corruption and to facilitate a systematic and timely method of returning stolen assets; and
- **Kleptocracy Asset Recovery Initiative** – Established in 2010 by the DOJ to forfeit the proceeds of foreign official corruption and/or return proceeds to benefit those harmed by the corrupt acts of the foreign officials.

Currently, no program exists to reward acts leading to the identification and recovery of stolen assets linked to foreign government corruption. The KARA would authorise the Treasury to "pay rewards under an asset recovery rewards program to help identify and recover stolen assets linked to foreign government corruption and the proceeds of such corruption hidden behind complex financial structures in the United States and abroad."

Impact on Financial Institutions

2562. What are the obligations of financial institutions as it relates to anti-corruption?

Financial institutions are obligated to implement the following anti-corruption measures:

- Develop and implement an anti-bribery and corruption compliance program pursuant to FCPA and equivalent international laws if operating outside of the United States;
- Develop a comprehensive KYC program to detect and collect due diligence on PEPs and close associates;
- Develop a risk-based suspicious activity monitoring program to detect and report potentially suspicious activities of PEPs and close associates;
- Screen customers/transactions against applicable lists administered by OFAC and other applicable lists, including internally managed lists;
- Train employees and compliance personnel on anti-corruption laws and red flags; and
- Develop a process to voluntarily disclose violations of anti-corruption laws and regulations.

2563. Are some financial institutions considering integrating their AML/CFT compliance and ABC Compliance Programs?

Yes. Those financial institutions that are considering integrating AML/CFT compliance and ABC Compliance Programs are motivated by the potential synergies afforded through cross channel alerts, access to broad financial intelligence and the possibility of cost savings by leveraging technology platforms and pooling resources.

Financial regulators, as well as the Director of FinCEN, have also expressed support for a combined approach with other compliance departments (e.g., AML/CFT and anti-fraud) to take advantage of the potential efficiencies.

2564. How do detection methods compare between AML/CFT and ABC Compliance Programs?

Detection methods for all types of financial crimes (e.g., ML/TF, fraud, corruption) continue to get more sophisticated with emerging technology, moving beyond basic rules-based algorithms that focus on transactional data to incorporating artificial intelligence (AI) algorithms that include free text data (e.g., payment instructions, memo fields) providing investigators with more meaningful information to detect potentially suspicious activity. While some AML/CFT rules may be helpful in identifying corruption, there are other approaches that should be deployed, including, but not limited to, the following:

- Dynamic risk assessments that incorporate key risk indicators for corruption and bribery (e.g., Transparency International's Corruption Perception Index [CPI] and Bribe Payers Index [BPI]);
- Suspicious activity monitoring programs that incorporate risk-based rules and data mining beyond the financial transaction to identify bribes and other possible acts of corruption (e.g., purchase

orders, invoices, frequent/unusual changes to payment instructions/banking account information of vendors or other third parties, excessive or unusual activity in the travel and expense accounts of employees); and

- Sanctions and PEP screening that trigger investigations for possible acts of corruption on confirmed matches.

For additional guidance on transaction monitoring, please refer to the Transaction Monitoring, Investigations and Red Flags section.

2565. What are some common challenges to maintaining an effective ABC Compliance Program?

The following include some of the challenges that financial institutions have experienced in implementing an ABC Compliance Program:

- Program does not cover all types of corruption (e.g., limited to foreign acts of corruption);
- Inadequate risk assessment that does not differentiate between foreign PEPs and domestic PEPs;
- Risk assessment that does not use data points beyond high-risk geographies for corruption;
- Poor escalation process for detected acts of potential corruption (e.g., no escalation to senior investigators or appropriate department);
- Lacks whistleblower program to report internal violations or violations by vendors and other third parties of anti-corruption laws and regulations;
- Inadequate use of suspicious activity monitoring software (e.g., lacks rules to detect corruption, overreliance on rules-based monitoring, no inclusion of relationships/related parties, limited to customers and not employees, vendors and other third-party relationships); and
- Poor third-party risk management (e.g., selection, monitoring of agents, vendors, contractors).

Some key challenges for merging AML/CFT and ABC Compliance Programs include, but are not limited to, the following:

- Assuming that merging of reporting lines is the same as integrating separate programs. Organisational alignment without process/technology alignment only guarantees that everyone has a common manager and accomplishes little in reality;
- Leadership from one or the other discipline may lack the knowledge and experience to manage the area effectively when dealing with issues outside of his/her traditional comfort zone;
- Similarly, management may see one program as more important than the other, and, as a result, may not allocate resources effectively;
- Challenges with process redesign;
- Cost of implementing technology solutions; and
- Cultural barriers.

If the integration is done thoughtfully and with purpose, however, these challenges can be overcome.

Cyber Events and Cybersecurity

Basics

2566. What is a "cyber-event"?

A "cyber-event" is defined by the Financial Crimes Enforcement Network (FinCEN) as "an attempt to compromise or gain unauthorised electronic access to electronic systems, services, resources or information."

2567. What is "cybersecurity"?

"Cybersecurity" is defined by the National Institute of Standards and Technology (NIST) as "the ability to protect or defend the use of cyberspace from cyber attacks."

2568. What are some key terms related to "cyber events" and "cybersecurity"?

The following are some of the key terms related to cyber events and cybersecurity defined by various regulatory, federal and law enforcement authorities:

- **Advanced Persistent Threat (APT)** – Defined by NIST as an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organisations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organisation; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.
- **Adversary** – Defined by the National Initiative for Cybersecurity Careers and Studies (NICCS) as "an individual, group, organisation or government that conducts or has the intent to conduct detrimental activities" sometimes referred to as an "**attacker**" or "threat agent";
    - **Hacker** - Defined by the NICCS as "an unauthorised user who attempts to gain access to an information system";
    - **Hacktivist** – A hacker with a political or social cause, unlike a typical hacker's motive for personal financial gain.
- **Asset** – Defined by the NICCS as "a person, structure, facility, information, and records, information technology systems and resources, material, process, relationships, or reputation that has value";
- **Attack Method** - Defined by the NICCS as "the manner or technique and means an adversary may use in an assault on information or an information system;"

  - **Active Attack** – Defined by the NICCS as "an actual assault perpetrated by an intentional threat source that attempts to alter a system, its resources, its data, or its operations";
  - **Passive Attack** – Defined by the NICCS as "an actual assault perpetrated by an intentional threat source that attempts to learn or make use of information from a system, but does not attempt to alter the system, its resources, its data, or its operations";
  - **Threat** – Defined by the NICCS as "a circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact (create adverse consequences for) organisational operations, organisational assets (including information and information systems), individuals, other organisations, or society";
  - **Inside Threat** – Defined by the NICCS as "a person or group of persons within an organisation who pose a potential risk through violating security policies";
  - **Outside Threat** – Defined by the NICCS as "a person or group of persons external to an organisation who are not authorised to access its assets and pose a potential risk to the organisation and its assets."
  - **Attack Signature** – Defined by the NICCS as "a characteristic or distinctive pattern that can be searched for or that can be used in matching to previously identified attacks."

- **Critical Infrastructure** – Defined by the NIST as "system and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters;"
- **Cryptanalysis** – Defined by the NICCS as "the operations performed in defeating or circumventing cryptographic protection of information by applying mathematical techniques and without an initial knowledge of the key employed in providing the protection;"
- **Cryptography** – Defined by the NICCS as "the use of mathematical techniques to provide security services, such as confidentiality, data integrity, entity authentication and data origin authentication";
- **Cyber-Attack** – Defined by NIST as "an attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information";
- **Cyber-Enabled Crime** – Defined by FinCEN as "illegal activities carried out or facilitated [with] electronic systems and devices such as networks and computers" (e.g., fraud, money laundering, identity theft, computer intrusions/hacking, intellectual property rights matters, economic espionage/theft of trade secrets, online extortion);

- **Cyber-Related Information** – Defined by FinCEN as "information that describes technical details of electronic activity and behaviour (e.g., internet protocol [IP] addresses, timestamps, Indicators of Compromise [IOCs]). Includes, but is not limited to, data regarding the digital footprint of individuals and their behaviour;"
- **Cyberspace** – Defined by the NIST as "a global domain within the information environment consisting of the independent network of information systems infrastructures including the internet, telecommunications networks, computer systems and embedded processors and controllers";
- **Data Breach** – Defined by the NICCS as "the unauthorised movement or disclosure of sensitive information to a party, usually outside the organisation, that is not authorised to have or see the information";
- **Denial of Service (DOS)** – Defined by the NICCS as "an attack that prevents or impairs the authorised use of information system resources or services. [A **distributed DOS**] is a denial of service technique that uses numerous systems to perform the attack simultaneously";
- **Identity and Access Management** – Defined by the NICCS as "the methods and processes used to manage subjects and their authentication and authorisations to access specific objects;"
- **Internet of Things (IoT)** – Defined by the Internet Crime Complaint Center (IC3), a subdivision of the Federal Bureau of Investigation (FBI) as "any object or device which connects to the Internet to automatically send and/or receive data" (e.g., computers, printers, smartphones, security systems, medical devices, smart appliances). The NICCS uses the similar term "**information and communication(s) technology (ICT)"** defined as "any information technology, equipment or interconnected system or subsystem of equipment that processes, transmits, receives or interchanges data or information";
- **Incident** – Defined by the NICCS as "an occurrence that actually or potentially results in adverse consequences to (adverse effects on) (poses a threat to) an information system or the information that the system processes, stores, or transmits and that may require a response action to mitigate the consequences";
- **Indicator** – Defined by the NICCS as "an occurrence or a sign that an incident may have occurred or may be in progress";
- **Integrity** – Defined by the NICCS as "the property whereby information, an information system, or a component of a system has not been modified or destroyed in an unauthorised manner";
- **Internet Crime** – Defined by the IC3 as "any illegal activity involving one or more components of the Internet (e.g., websites, chat rooms, email). Internet crime involves the use of the Internet to communicate false or fraudulent representations to consumers (e.g., advance-fee schemes, non-delivery of goods or services, computer hacking, employment/business opportunity schemes)";
- **Intrusion Detection –** Defined by the NICCS as "the process and methods for analysing information from networks and information systems to determine if a security breach or security violation has occurred";

- **Malware** – Defined by the NIST as "a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity or availability of the victim's data, applications or operating system or otherwise annoying or disrupting the victim."
    - **Scareware** – Defined by the FBI as a form of malware that frightens victims into purchasing fake antivirus software through false security warnings through pop-up windows; malware may automatically download without consumers clicking on these ads, also referred to as malvertising.
    - **Ransomware** – Defined by the FBI as "a form of malware [frequently delivered through phishing emails] that targets both human and technical weaknesses in organisations and individual networks in an effort to deny the availability of critical data and/or systems. [After] the rapid encryption of sensitive files… the cyber actor demands the payment of a ransom [in exchange] for an avenue to the victim to regain access to their data."
- **Non-public Information (NPI)** – Defined by the Federal Trade Commission (FTC) as the following:
    - "Any information an individual gives you to get a financial product or service (for example, name, address, income, social security number, or other information on an application);
    - Any information you get about an individual from a transaction involving your financial product(s) or service(s) (for example, the fact that an individual is your consumer or customer, account numbers, payment history, loan or deposit balances, and credit or debit card purchases); or
    - Any information you get about an individual in connection with providing a financial product or service (for example, information from court records or from a consumer report);
    - A subset of NPI, protected health information (PHI), is defined by the Centers for Disease Control (CDC) as "individually identifiable health information that is transmitted or maintained in any form or medium (e.g., electronic, paper, oral) but excludes certain educational records and employment records."
- **Penetration Testing** – Defined by the NICCS as "an evaluation methodology whereby assessors search for vulnerabilities and attempt to circumvent the security features of a network and/or information system" also referred to as a "pen test";
- **Personally Identifiable Information (PII)** – Defined by the NIST as "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual such as date and place of birth, mother's maiden name, etc.";

- **Publicly Available Information** – Defined by the Federal Financial Institutions Examination Council (FFIEC) as "information that a [financial institution] has a reasonable basis to believe is lawfully and publicly available from sources such as public records, widely distributed media and government-required disclosures;"
- **Recovery** – Defined by the NICCS as "the activities after an incident or event to restore essential services and operations in the short and medium term and fully restore all capabilities in the longer term";
- **Resilience** – Defined by the NICCS as "the ability to adapt to changing conditions and prepare for, withstand, and rapidly recover from disruption";
- **Response** – Defined by the NICCS as "the activities that address the short-term, direct effects of an incident and may also support short-term recovery";
- **Social engineering** – Defined by FinCEN as "human interaction tactics used to deceive an individual into revealing information;"
    - **Phishing/Vishing/Smishing –** Phishing is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by masquerading as a legitimate entity in an electronic communication (e.g., email, spyware). For example, an individual may receive an email that appears to be from his or her bank that requests identity and/or password information under the guise of "verification" purposes. Vishing (voice phishing) and smishing are similar to phishing but conducted through the telephone/voicemails and texting (SMS messages) respectively.
    - **Pharming** - A method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by secretly redirecting users from legitimate websites to websites created by scammers.
- **Unauthorised electronic intrusion** – Defined by FinCEN as "gaining access to a computer system of a financial institution to:
    - Remove, steal, procure or otherwise affect funds of the financial institution or the institution's customers;
    - Remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or
    - Damage, disable, disrupt, impair or otherwise affect critical systems of financial institutions."

For additional terms, please refer to the glossary maintained by the National Initiative for Cybersecurity Careers and Studies (NICCS) https://niccs.us-cert.gov/glossary.

2569. What is the scale of cybercrimes?

Estimating the scale of cybercrimes is difficult since the associated costs may include financial losses as well as the costs associated with investigating cyber breaches and implementing protective measures. According to the U.S. Department of Justice (DOJ), the global cost of cybercrime is estimated to exceed US$100 billion. Some estimates are much higher. According to the 2013 report Europol Serious & Organised Threat Assessment, the "total impact of cybercrime" is approximately US$3 trillion, "making it more profitable than the global trade in marijuana, cocaine and heroin combined."

2570. What are the top jurisdictions affected by cybercrimes reported to the IC3?

In 2015, the IC3 reported the top five countries by victim location as:

- United States (80.2 percent)
- United Kingdom (2.47 percent)
- Nigeria (2.2 percent)
- China (1.91 percent)
- India (1.46 percent)

The top five states by victim location included:

- California (14.53 percent)
- Florida (8.47 percent)
- Texas (7.67 percent)
- New York (6.3 percent)
- Illinois (3.51 percent)

2571. What are the most common types of cybercrimes reported to the IC3?

According to the IC3's Internet Crime Report (2015), of the US$1.2 billion reported losses, the top 10 cybercrimes included the following:

- Business Email Compromise (BEC) (20 percent) (US$246 million)
- Confidence Fraud/Romance (16 percent) (US$203 million)
- Non-Payment/Non-Delivery (10 percent) (US$121 million)
- Investment (10 percent) (US$119 million)
- Identity Theft (5 percent) (US$57 million)
- Other (5 percent) (US$56 Million)
- Advanced Fee (4 percent) (US$51 million)
- 419/Overpayment (4 percent) (US$49 million)

- Personal Data Breach (4 percent) (US$43 million)
- Credit Card Fraud (3 percent) (US$42 million)

According to the DOJ's "Financial Fraud Crime Victim (2015)," only 15 percent of fraud victims report crimes to law enforcement. Additional observations included:

- Phishing/vishing/smishing/pharming accounted for approximately 1 percent (US$8 million) of IC3 complaints;
- Malware/scareware/ransomware accounted for approximately 0.4 percent (US$4.5 million);
- Denial of Service (DOS) attacks accounted for approximately 0.2 percent (US$2.8 million);
- Viruses accounted for approximately 0.1 percent (US$1.2 million);
- Terrorism accounted for less than 0.01 percent (US$66,000);
- Over 5 percent involved social media; and
- Less than 1 percent involved virtual/crypto currency (e.g., Bitcoin, Litecoin, Potcoin).

IC3 noted that duplicative information may be tallied as some victims reported multiple cybercrimes per complaint.

2572. What are some recent examples of cybercrimes?

The following are some recent examples of cybercrimes:

- In November 2015, the DOJ announced a 22-count indictment against three defendants that included computer hacking, wire fraud, securities fraud, aggravated identity theft, conspiracy to commit money laundering and securities market manipulation scheme. The computer hacking crimes targeted U.S. financial institutions, brokerage firms and financial news publishers and included the largest theft of customer data from a U.S. financial institution to date. Two defendants were extradited from Israel. The third defendant was residing in Russia but was arrested in a New York airport in December 2016.
- In April 2016, a whistleblower leaked more than 11.5 million documents identifying the beneficial owners of 214,000 offshore entities from Mossack Fonseca (MF), a Panama-based law firm specialising in the formation and management of entities in tax havens, according to the International Consortium of Investigative Journalists (ICIJ). In September 2016, the same source also leaked information from the Bahamas corporate registry, linking approximately 140 international and local politicians to offshore companies in the Bahamas. The ICIJ published the leaked information in its Offshore Leaks Database. As a result of the leaks, regulatory and tax investigations were launched in numerous countries (e.g., United States, United Kingdom, Germany, Australia, Sweden, Hong Kong, Chile, Singapore, India). According to media reports, in February 2017, the two founders of Mossack Fonseca were arrested for their alleged involvement in a separate money laundering investigation involving corruption in Latin America. These leaks had corruption, tax evasion and cybersecurity implications. For further guidance, please refer to

the sections: Anti-Bribery and Corruption Compliance Programs and Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act.

- In December 2016, the DOJ unsealed a 21-count indictment that included wire fraud, aggravated identity theft, conspiracy to commit money laundering and conspiracy to violate the Computer Fraud and Abuse Act against three Romanian nationals operating out of Eastern Europe. The three Romanians allegedly executed a cyber-fraud scheme that infected between 60,000 and 160,000 computers, registered over 100,000 email accounts with public email providers and sent over 11 million emails that resulted in US$4 million in losses. The cyber schemes utilised included installing malware to harvest personally identifiable information (PII) (e.g., credit card information, usernames, passwords), disabling malware protection, redirecting to fictitious web pages and using software to mine for cryptocurrency for the financial benefit of the group.
- In 2016, years after the cyber attacks occurred, Yahoo publicly announced two of the largest massive data breaches in the history of the internet occurring in August 2013 affecting at least 1 billion user accounts and an additional 500 million user accounts compromised in 2014 which may have included names, email addresses, telephone numbers, dates of birth, passwords and security questions and answers but not financial information (e.g., payment cards, bank accounts). Yahoo speculated that the alleged "state-sponsored" hackers were attempting to use code such as "forged cookies" to gain access to a web-based account without a login. Yahoo notified customers and recommended password resets on one incident but required password resets on the other. Both the FTC and the SEC have initiated investigations into the hacks. Congress launched its own investigation, issuing requests for more information on the data breaches (e.g., when did Yahoo first become aware of the breaches) in order to determine if senior executives fulfilled their obligations to disclose to investors and the public about these hacks.
- In May 2017, a global cyber-attack targeted hospitals, companies and government offices, primarily in Russia, Ukraine, Taiwan and the United Kingdom. The cyber attack lead to global disruptions in transportation, banking and medical care, going as far as causing the cancellation of surgical procedures and the diversion of ambulances in the United Kingdom. The cyber scheme utilised included the ransomware, WannaCry, which may have been developed based on leaked tools from the National Security Agency (NSA) of the United States. WannaCry took advantage of a previously disclosed Microsoft vulnerability. Many referred to this cyber-attack as a "wake-up call" for governments, companies, software vendors and policy makers to address the growing threat of cyber-attacks.

2573. What key U.S. federal laws, regulations and actions address cybercrimes and cybersecurity?

The following are key U.S. federal laws, regulations and actions addressing cybercrimes and cybersecurity:

- **Federal Trade Commission Act** (1914) (Section 5 – Unfair or Deceptive Acts or Practices [UDAP] is the primary enforcement tool of FTC with regard to data security)

- **Computer Fraud and Abuse Act** (CFAA) (1986) (an amendment to the existing computer fraud law enacted in the Comprehensive Crime Control Act of 1984)
- **Health Insurance Portability and Accountability Act** (HIPAA) (1996)
- **Gramm-Leach-Bliley Act** (GLBA) (1999)
- **Critical Infrastructures Protection Act of 2001**
- **Homeland Security Act** (2002)
- **Executive Order 13636 – Improving Critical Infrastructure Cybersecurity** (2013)
- **Cybersecurity Act of 2015**, also known as the Cybersecurity Information Sharing Act (CISA)
- **Executive Order 13694 – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities** (2015)
- **Executive Order 13757 – Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities** (2017)
- **Executive Order – Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure** (2017)

The Cyber-Related Sanctions Program, administered by the Office of Foreign Assets Control (OFAC), was created pursuant to Executive Orders 13694 and 13757. For further guidance, please refer to the Cyber-Related Sanctions Program section.

2574. How does the Financial Action Task Force (FATF) address cybersecurity?

In **Recommendation 36 – International Instruments**, FATF encourages countries to implement the Council of Europe Convention on Cybercrime (2001) which outlines an infrastructure to address cybercrimes and cybersecurity, including, but not limited to, the following:

- **Substantive Criminal Law** - Offences against the confidentiality, integrity and availability of computer data and systems; computer-related offences; content-related offences (e.g., illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud, offences related to child pornography, offences related to infringements of copyright and related rights, attempt and aiding or abetting, corporate liability);
- **Procedural Law** – Legislative measures for the purpose of criminal investigations or proceedings (e.g., preservation, disclosure, search and seizure, real-time collection, and interception of stored computer data);
- **International Cooperation** – General principles related to international cooperation; extradition; mutual assistance even in the absence of applicable international agreements; preservation, disclosure and accessing stored computer data including trans-border access.

Additionally, **Recommendation 15 – New Technologies** addresses the need for the identification and assessment of ML/TF risks of new products, delivery mechanisms and technologies. For further guidance on FATF Recommendations, please refer to the Financial Action Task Force section.

2575. What key groups have played an important role in the development and implementation of anti-cybercrime and cybersecurity standards?

Recognising the international focus on cybercrime, many groups are active in issuing guidance and driving international efforts, including, but not limited to, the following:

- **National Institute of Standards and Technology (NIST)** – Founded in 1901, the NIST, formerly known as the National Bureau of Standards (NBS), is a non-regulatory agency of the U.S. Department of Commerce, with a mission to promote innovation and industrial competitiveness.
    - Released in 2014 and updated in 2017, the NIST published the **Cybersecurity Framework (CSF)** which provides a set of standards, methodologies, procedures and processes to reduce cyber-risks to critical infrastructure.
    - The NIST administers the **National Vulnerability Database (NVD)**, a government repository of standards based vulnerability management, security measurement, compliance and data represented using the Security Content Automation Protocol (SCAP). The NVD includes security checklists, security related software flaws, misconfigurations, product names and impact metrics.
- **U.S. Federal Bureau of Investigation (FBI)**
    - **Internet Crime Complaint Center (IC3)** – Established in May 2000 to provide the public with a mechanism to report internet-facilitated criminal activity to the FBI. The IC3 provides law enforcement access to its database of complaints through the Law Enforcement Enterprise Portal (LEEP).
    - **Operation Wellspring Initiative (OWS)** – Launched in August 2013 to build the cyber-investigative capabilities and capacity of federal, state and local law enforcement communities, the OWS developed a national platform to receive, develop and refer internet-facilitated fraud complaints; coordinates with FBI Cyber and Criminal Units; provides internet-fraud statistical reporting through Cyber Task Forces (CTFs); and addresses internet-facilitated criminal cases which do not meet most federal investigative thresholds.
- **Department of Homeland Security (DHS)**
    - **National Cybersecurity and Communications Integration Center (NCCIC)** – The NCCIC serves as a hub for multiple partners (e.g., government agencies, private sector, international partners) involved in cybersecurity and communications protection to collaborate on providing cybersecurity protection, developing and distributing actionable cybersecurity guidance, responding to and analysing cyber incidents and collaborating with foreign governments and international entities to enhance the cybersecurity infrastructure of the United States. The NCCIC is comprised of four branches:

        - **United States Computer Emergency Readiness Team** (US-CERT) – Established in 2000 as the Federal Computer Incident Response Center (FedCIRC) and later transferred to the DHS as the US-CERT;
        - **NCCIC Operations & Integration (NO&I)**;
        - **Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)**; and
        - **National Coordinating Center for Communications (NCC)**.
    - **Automated Indicator Sharing (AIS)** – Launched in March 2016, the AIS enables the exchange of cyber threat indicators between the federal government and the private sector in real time. AIS is free and available to all private sector entities, federal, state, local, tribal and territorial governments, information sharing and analysis centres (ISACs), information sharing and analysis organisations (ISAOs) and foreign partners and companies. Participants can submit and/or receive cyber threat indicators.

- **United States Secret Service (USSS) Electronic Crimes Task Forces (ECTF)** – Under the USA PATRIOT Act, the New York ECTF was the first task force to form in 1995 to assist in the prevention, detection, mitigation and aggressive investigation of attacks on the financial and critical infrastructures of the United States. The network of ECTFs investigates crimes such as computer-generated counterfeit currency, bank fraud, virus and worm proliferation, access device fraud, telecommunications fraud, internet threats, computer system intrusions and cyber-attacks, phishing, identity theft and internet-related child pornography and exploitation.
- **Computer Crime and Intellectual Property Section (CCIPS) Cybersecurity Unit** – A division of the Department of Justice (DOJ), the Cybersecurity Unit serves as a hub for expert advice and legal guidance related to criminal electronic surveillance, computer fraud and cyber-abuses.
- **European Cybercrime Centre (EC3)** – Established in 2013 by Europol, EC3 works with the Joint Cybercrime Action Taskforce (J-CAT) as a central hub for criminal information and intelligence as it relates to cybercrimes affecting European Union (EU) members.

2576. What are some examples of "critical infrastructure sectors"?

Sixteen critical infrastructure sectors were identified in the Presidential Policy Directive – Critical Infrastructure Security and Resilience published in 2013 with the following designated sector-specific agencies (SSA):

- Chemical – SSA: Department of Homeland Security (DHS)
- Commercial Facilities – SSA: DHS
- Communications – SSA: DHS
- Critical Manufacturing – SSA: DHS

- Dams – SSA: Department of Defense (DOD)
- Defense Industrial Base – SSA: DOD
- Emergency Services – SSA: DHS
- Energy – SSA: Department of Energy (DOE)
- Financial Services – SSA: Department of the Treasury (U.S. Treasury)
- Food and Agriculture – SSA: Department of Agriculture (DOA) and Department of Health and Human Services (DHHS)
- Government Facilities – SSA: DHS and General Services Administration (GSA)
- Healthcare and Public Health – SSA: DHHS
- Information Technology – SSA: DHS
- Nuclear Reactors, Materials and Waste – SSA: DHS
- Transportation Systems – DHS and Department of Transportation (DOT)
- Water and Wastewater Systems – SSA: Environmental Protection Agency (EPA)

2577. What are the key parts of the NIST's Cybersecurity Framework (CSF)?

The CSF is organised into three parts:

- Framework Core:
  - **Five Functions** to manage cybersecurity risk:
    - **Identify** – Develop the organisational understanding to manage cybersecurity risk to systems, assets, data and capabilities;
    - **Protect** – Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services;
    - **Detect** – Develop and implement the appropriate activities to identify the occurrence of the cybersecurity event;
    - **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event; and
    - **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.
  - **Categories** – The Functions are then divided into categories of cybersecurity outcomes tied to programmatic needs and activities (e.g., asset management, business environment, governance, risk assessment, awareness and training, data security, protective technology, detection processes).

  - **Subcategories** – The Categories are further divided into Subcategories of specific outcomes of technical and/or management activities (e.g., physical devices and systems within the organisation are inventoried, organisational communication and data flows are mapped, external information systems are catalogued, data-at-rest is protected, notifications from detection systems are investigated); and
  - **Informative References** – Standards, guidelines and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory (e.g., resources from NIST, Control Objectives for Information and Related Technology [COBIT], International Organisation for Standardisation [ISO]/International Electrotechnical Commission [IEC], International Society for Automation [ISA]).

- **Framework Implementation Tiers** – Provides context on how to view cybersecurity risk and the processes in place to manage that risk by considering current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives and organisational constraints. Listed in increasing degree of rigor and sophistication in cybersecurity risk management practices, the tiers are as follows:
  - Tier 1: Partial
  - Tier 2: Risk Informed
  - Tier 3: Repeatable
  - Tier 4: Adaptive
- **Framework Profile** – The alignment of the Functions, Categories and Subcategories with the business requirements, risk tolerance and resources of the organisation that can be used to describe the current and desired target states of specific cybersecurity activities of the organisation, identify gaps and contribute to a road map from the current to the desired state.

Updates to the CSF were published in 2017 including, but not limited to, the following:

- New details on managing cyber supply chain risk management (SCRM);
- Clarification of key terms; and
- Introduction of measurement methods for cybersecurity.

A new version of the CSF is expected to be released in the latter half of 2017. For further guidance on how to use the framework to establish and/or improve a cybersecurity program, key definitions and further examples, please refer to NIST's Framework for Improving Critical Infrastructure Cybersecurity.

2578. Are U.S. businesses required to implement the CSF?

The CSF was developed as a risk-based, non-industry-specific, technology-neutral framework for operators of critical infrastructure to implement voluntarily. There is no requirement that a business implement the framework.

2579. What is FFIEC's Cybersecurity Assessment Tool?

Developed in 2015 by the FFIEC, the Cybersecurity Assessment Tool provides a reasonable and measurable process for institutions to measure their cybersecurity preparedness over time. The Cybersecurity Assessment Tool assists financial institutions to do the following:

- Identify factors contributing to and determining the institution's overall cyber risk;
- Assess the institution's cybersecurity preparedness;
- Evaluate whether the institution's cybersecurity program is aligned with its risks;
- Determine risk management practices and controls that are needed or need enhancement and actions to be taken to achieve the desired state; and
- Inform risk management strategies.

The Cybersecurity Assessment Tool is organised as follows:

- **Inherent Risk Profile –** Assesses the inherent cybersecurity risk (e.g., type, volume) posed to the institution by the following: Technologies and Connection Types:
  - Delivery Channels
  - Online/Mobile Products and Technology Services
  - Organisational Characteristics
  - External Threats

Risks are rated as Least, Minimal, Moderate, Significant or Most.

- **Cybersecurity Maturity –** Designed to assist management measure the institution's level of risk and corresponding controls within the following domains:
  - Cyber Risk Management and Oversight (e.g., Governance, Risk Management, Resources, Training and Culture)
  - Threat Intelligence and Collaboration (e.g., Threat Intelligence, Monitoring and Analysing, Information Sharing)
  - Cybersecurity Controls (e.g., Preventive Controls, Detective Controls, Corrective Controls)
  - External Dependence Management (e.g., Connections, Relationship Management)
  - Cyber Incident Management and Resilience (e.g., Incident Resilience Planning and Strategy, Detection, Response and Mitigation, Escalation and Reporting)

Maturity levels range from Baseline, Evolving, Intermediate, and Advanced to Innovative.

2580. What are some key processes in developing a cybersecurity program based on the CSF and the Cybersecurity Assessment Tool?

Key processes include, but are not limited to, the following:

- **Asset Management –** The purpose of Asset Management is to identify, document and manage assets during their life cycle to ensure sustained productivity to support critical services;
- **Controls Management –** The purpose of Controls Management is to identify, analyse and manage controls in a critical service's operating environment;
- **Configuration and Change Management** – The purpose of Configuration and Change Management is to establish processes to ensure the integrity of assets using change control and change control audits;
- **Vulnerability Management** – The purpose of Vulnerability Management is to identify, analyse and manage vulnerabilities in a critical service's operating environment;
- **Incident Management** – The purpose of Incident Management is to establish processes to identify and analyse events, detect incidents and determine an organisational response;
- **Service Continuity Management** – The purpose of Service Continuity Management is to ensure the continuity of essential operations of services and their associated assets if a disruption occurs as a result of an incident, disaster or other disruptive event;
- **Risk Management** – The purpose of Risk Management is to identify, analyse and mitigate risks to critical service assets that could adversely affect the operation and delivery of services;
- **External Dependencies Management** – The purpose of the External Dependencies Management is to establish processes to manage an appropriate level of controls to ensure the sustainment and protection of services and assets that are dependent on the actions of external parties;
- **Training and Awareness** – The purpose of Training and Awareness is to promote awareness in and develop skills and knowledge of people in support of their roles in attaining and sustaining operational sustainment and protection; and
- **Situational Awareness** – The purpose of Situational Awareness is to actively discover and analyse information related to immediate operational stability and security and to coordinate such information across the enterprise to ensure that all organisational units are performing under a common operating picture.

2581. What information and guidance have been issued with respect to cybercrimes and cybersecurity?

The following key guidance and resources have been provided related to cybercrimes and cybersecurity:

- **Cybersecurity Framework Frequently Asked Questions** by the National Institute of Standards and Technology (NIST)
- **Glossary of Key Information Security Terms** (2013) by the NIST

- **Advanced Notice of Proposed Rulemaking: Enhanced Cyber Risk Management Standards** (2016) by the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC)
- **Cybersecurity Assessment Tool** (2015) by the Federal Financial Institutions Examination Council (FFEIC)
- **Cybersecurity Assessment General Questions** by the FFIEC
- **Protecting Personal Information: A Guide for Business** by the Federal Trade Commission (FTC)
- **Data Breach Response: A Guide for Business** by the FTC
- **Start with Security: A Guide for Business: Lessons Learned from FTC Cases** by the FTC
- **Cyber Criminal Exploitation of Electronic Payment Systems and Virtual Currencies** (2011) by the FBI
- **Cyber Criminal Exploitation of Real-Money Trading** (2011) by the FBI
- **Typology Report: Cybercrime and Money Laundering** (2014) by the Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)
- **The NIST Cybersecurity Framework and the FTC** (2016) by the FTC and Andrea Arias
- **Guidance on Cyber Resilience for Financial Market Infrastructures** (2016) by the Committee on Payments and Market Infrastructures (CPMI) and the International Organisation of Securities Commissions (IOSCO)
- **The National Strategy to Secure Cyberspace** (2003) by the Department of Homeland Security (DHS)
- **Infrastructure Threats - Intrusion Risks** (2000) by the OCC
- **Guidance Concerning Reporting Computer-Related Crimes by Financial Institutions** (1997) by the FRB
- **Guidance for Financial Institutions on Reporting Computer-Related Crimes** (1997) by the National Credit Union Administration (NCUA)
- **Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime** (2016) by FinCEN
- **Frequently Asked Questions (FAQs) Regarding the Reporting of Cyber-Events, Cyber-Enabled Crime and Cyber-Related Information through Suspicious Activity Reports (SARs)** (2016) by FinCEN
- **Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes** (2016) by FinCEN

- **Account Takeover Activity** (2011) by FinCEN
- **Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation and Additional Resources** (2014) by the FFIEC
- **Destructive Malware and Compromised Credentials** (2015) by the FFIEC
- **Cyber Attacks Involving Extortion** (2015) by the FFIEC
- **Presidential Policy Directive – Critical Infrastructure Security and Resilience** (2013) by the White House
- **Best Practices for Victim Response and Reporting of Cyber Incidents** (2015) by the Cybersecurity Unit of the Computer Crime & Intellectual Property Section (CCIPS) of the Department of Justice (DOJ)
- **Ransomware: What Is It and What To Do About It** (2016) by the Cybersecurity Unit
- **How to Protect Your Networks from Ransomware: Interagency Technical Guidance Document** (2016) by the Cybersecurity Unit and other agencies
- **Avoiding Social Engineering and Phishing Attacks** (2017) by the United States Computer Emergency Readiness Team (US-CERT)
- **Fact Sheet: Cybersecurity National Action Plan** (2016) by the White House
- **Cyber Incident Reporting: A Unified Message for Reporting to the Federal Government** by the U.S. Department of Homeland Security (DHS)
- **Reporting Computer, Internet-Related or Intellectual Property Crime** by the U.S. Department of Justice (DOJ) Computer Crime and Intellectual Property Section (CCIPS)
- Public Service Announcements (PSAs) by the **Internet Crime Complaint Center** (IC3) of the Federal Bureau of Investigation (FBI):
  - **Business E-Mail Compromise** (2015 & 2016)
  - **E-Mail Account Compromise** (2015)
  - **E-Mail Extortion Campaigns Threatening Distributed Denial of Service Attacks** (2015)
  - **Criminals Continue to Defraud and Extort Funds from Victims Using Cryptowall Ransomware Schemes** (2015)
  - **Criminals Host Fake Government Services Web Sites to Acquire Personally Identifiable Information and to Collect Fraudulent Fees** (2015)
  - **FBI Warns of Fictitious 'Work-From-Home' Scam Targeting University Students** (2015)
  - **Gift Card Scams** (2015)

  - **Hacktivists Threaten to Target Law Enforcement Personnel and Public Officials** (2015)
  - **Internet of Things Poses Opportunities for Cyber Crime** (2015)
  - **ISIL Defacements Exploiting Wordpress Vulnerabilities** (2015)
  - **New Microchip-Enabled Credit Cards May Still Be Vulnerable to Exploitation by Fraudsters** (2015)
  - **Scammers May Use Paris Terrorist Attack to Solicit Fraudulent Donations** (2015)
  - **Tax Return Fraud** (2015)
  - **University Employee Payroll Scam** (2015)
- **Internet Crime Report** (2015; published annually) by IC3
- **Infrastructure Threats – Intrusion Risks** (2000) by the Office of the Comptroller of the Currency (OCC)
- **Guidance Concerning Reporting of Computer Related Crimes by Financial Institutions** (1997) by the Federal Reserve Board (FRB)
- **Guidance for Financial Institutions on Reporting Computer-Related Crimes** (1997) by the Federal Deposit Insurance Corporation (FDIC)
- **Guidance for Reporting Computer-Related Crimes** (1997) by the National Credit Union Association (NCUA)
- **Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015** by the U.S. Department of Homeland Security (DHS)
- **Start with Security: A Guide for Business: Lessons Learned from FTC Cases** by the Federal Trade Commission (FTC)
- **Framework for Improving Critical Infrastructure Cybersecurity** (2014) by the National Institute of Standards and Technology (NIST)
- **Report on Cybersecurity Practices** (2015) by the Financial Industry Regulatory Authority (FINRA)
- **Principles for Effective Cybersecurity: Insurance Regulatory Guidance** (2015) by the National Association of Insurance Commissioners (NAIC)
- **Cybersecurity Examination Initiative** (2015) by the Office of Compliance Inspections and Examinations (OCIE)
- **Cybersecurity Examination Sweep Summary** (2015) by the OCIE

- **Report on Cyber Security in the Insurance Sector** (2014) by New York State Department of Financial Services (DFS)
- **Report on Cyber Security in the Insurance Sector** (2015) by NYDFS
- **Update on Cyber Security in the Banking Sector: Third Party Service Providers** (2015) by NYDFS
- **Council Framework Decision: Combating Fraud and Counterfeiting of Non-Cash Means of Payment** (2001) by the Council of the European Union
- **Internet Organised Crime Threat Assessment (IOCTA)** (2011, 2014, 2015, 2016) by Europol's European Cybercrime Center (EC3)

Business E-Mail Compromise and E-Mail Account Compromise

2582. What is an "E-mail Compromise Fraud"?

FinCEN defines "E-mail Compromise Fraud" as a "scheme in which criminals compromise the e-mail accounts of victims to send fraudulent wire transfer instructions to financial institutions in order to misappropriate funds." E-mail Compromise Fraud often includes the following types of activities:

- **Business E-mail Compromise (BEC) –** Scheme that targets the commercial customers of a financial institution, often those with foreign suppliers who regularly conduct wire transfer payments, through social engineering or computer intrusion techniques; other methods of payments (e.g., checks) can be used as well; targets range from small businesses to large corporations; schemes can include non-business activity such as romance, lottery and employment; and
- **E-mail Account Compromise (EAC) –** Scheme that targets a victim's personal accounts; victims may overlap with BEC victims as the scheme expands beyond the business activity of companies. Financial services professionals (e.g., attorneys, accountants, realtors) are frequent targets.

2583. How do BEC and EAC schemes work?

According to FinCEN, there are three stages to BEC/EAC schemes:

- **Stage 1 – Compromising Victim Information and Email Accounts**: Through social engineering or computer intrusion, criminals gain access to a victim's email account(s) to obtain information to enable the cybercrime (e.g., financial account information, contacts);
- **Stage 2 – Transmitting Fraudulent Instructions**: With the stolen information, criminals either utilise the victim's email account or a fake email account resembling the victim's email account to submit fraudulent transaction instructions (e.g., wire transfers directed to a fraudulent account); and
- **Stage 3 - Executing Unauthorised Transactions**: Victims are tricked into executing the fraudulent transaction instructions by appearing legitimate and/or urgent.

2584. Are BEC/EAC schemes the same as identity theft/account takeovers?

No. BEC/EAC fraud is distinct from identity theft/account takeover in that the victim retains control over the email account(s). For further guidance on identity theft, please refer to the Identity Theft and Identity Theft Prevention Program section.

2585. What are some common BEC schemes?

The IC3 provided the following five scenarios as common BEC schemes based on complaint data:

- **Data Theft** – Fraudulent email requests sent utilising an executive's hacked/compromised email, typically to an entity responsible for maintaining PII (e.g., human resources, bookkeeping, audit);
- **Business Working with a Foreign Supplier** – Fraudulent request (e.g., made via email, telephone, facsimile) with instructions to wire funds for an invoice to an alternate, fraudulent account; requests closely mimic legitimate requests;
- **Business Executive Receiving or Initiating a Request for a Wire Transfer** – Fraudulent request sent from the hacked/compromised email of a business executive and sent to a second employee within the company with instructions to send funds to a fraudulent account; also referred to as "CEO Fraud," "Business Executive Scam," "Masquerading" and "Financial Industry Wire Frauds."
- **Business Contacts Receiving Fraudulent Correspondence through Compromised Emai**l – Fraudulent requests sent from the hacked/compromised email of an employee/executive and sent to vendors mined from the contacts of the employee/executive requesting payment for invoices; and
- **Business Executive and Attorney Impersonation** – Fraudulent requests sent from persons identifying themselves as lawyers or representatives of law firms; with claims of confidentiality and time-sensitivity, cybercriminals pressure victims to transfer funds, often at the close of business (domestic or international) or at the end of a work week.

FinCEN provided similar scenarios for common BEC schemes:

- Cybercriminal Impersonates a Financial Institution's Commercial Customer
- Cybercriminal Impersonates an Executive
- Cybercriminal Impersonates a Supplier

Some have reported BEC schemes targeting compliance and legal personnel from cybercriminals impersonating regulatory agencies, such as the SEC, in an attempt to acquire insider information.

2586. What are some common EAC schemes?

FinCEN provided the following three scenarios as common EAC schemes:

- **Lending/Brokerage Services** – Cybercriminal hacks into the email account of a financial services professional and sends fraudulent payment instructions to the banks of their clients, requesting transfers to accounts in control by the cybercriminal;

- **Real Estate Services** – Cybercriminal hacks into the email account of a realtor and sends fraudulent payment instructions to other parties (e.g., escrow company) to divert payments (e.g., sale proceeds, loan disbursements, fees) into accounts in control by the cybercriminal; and
- **Legal Services** – Cybercriminal hacks into the email account of an attorney and sends fraudulent payment instructions to either the attorney's financial institution or to trust and escrow accounts managed by the attorney on behalf of his/her clients.

2587. What are some leading practices to guard against BEC schemes?

The IC3 provided the following list of self-protection strategies to guard against BEC schemes, primarily compiled from published Public Service Announcements (PSAs) issued by the FBI in 2015:

- Avoid free web-based email accounts; utilise company domain email accounts;
- Be cautious when sharing information publicly (e.g., company websites, social media), especially information that could enable a cybercrime (e.g., job duties/descriptions, hierarchical information, out-of-office details);
- Be suspicious of requests for secrecy or pressure to take action quickly;
- Consider implementing additional financial security procedures (e.g., 2-step verification/authentication process, out of band communication such as telephone calls, digital signatures, procedures to report and delete unsolicited email/spam, utilisation of forward function as opposed to reply when responding to emails);
- Beware of sudden changes in business practices;
- Create intrusion detection system rules (e.g., flags for emails with extensions similar to company email);
- Register all company domains that are slightly different from the actual company domain (e.g., abc_company.com versus abc-company.com);
- Verify changes in vendor payment locations;
- Confirm requests for transfers of funds; and
- Know your customer (e.g., volume, frequency and types of payments).

2588. What are some common red flags for BEC/EAC schemes?

FinCEN provided the following examples of red flags to detect BEC/EAC schemes:

- Email address used to send transaction instructions has been slightly altered (e.g., addition, deletion, changing of a letter so email address resembles authentic email address);
- Payment instructions include different language, beneficiary, account information, timing and amounts from previously verified and authentic transactions;
- Payment instructions include the same beneficiary as previous instructions, but different account information;

- Payment instructions include transfers to beneficiary with no payment history or documented relationship with the customer;
- Payment instructions include beneficiary/account information previously flagged for fraudulent activity;
- Payment instructions include language such as "Urgent," "Secret" or "Confidential";
- Payment instructions are delivered in a way to limit the time and opportunity for a financial institution to authenticate the transaction (e.g., close-of-business, end of the week);
- Payment instructions originate from a customer's employee who is newly authorised to conduct transactions and/or has no history of conducting transactions;
- Customer's employee or representative cannot verify payment instructions originating from emails from executives, attorneys or designees;
- Multiple payment instructions for additional payments shortly after a successful payment from an account not typically used in this manner (e.g., payments to vendors/suppliers); or
- Beneficiary in wire transfer instructions does not match the name of the account holder.

For further guidance on additional red flags, please refer to the Suspicious Activity Red Flags section.

2589. What information should BEC victims provide to the IC3 if funds are transferred to a fraudulent account?

When filing a complaint, the IC3 recommends identifying the incident as "BEC" with the following information:

- **Description of the incident**:
  - Internet protocol (IP) and/or email address of fraudulent email
  - Date and time of incidents
  - Incorrectly formatted invoices or letterheads
  - Requests for secrecy or immediate action
  - Unusual timing, requests, or wording of the fraudulent phone calls or emails
  - Phone numbers of the fraudulent phone calls
  - Description of any phone contact to include frequency and timing of calls
  - Foreign accents of the callers
  - Poorly worded or grammatically incorrect emails
  - Reports of any previous email phishing activity
- **Financial Information**:
  - Originating Name (where the originator is the victim)

- Originating Location
- Originating Bank Name
- Originating Bank Account Number
- Recipient Name (where the recipient is the beneficiary of the fraud)
- Recipient Bank Name
- Recipient Bank Account Number
- Recipient Bank Location (if available)
- Intermediary Bank Name (if available)
- SWIFT Number
- Date
- Amount of Transaction
- Additional Information (if available) (e.g., "FFC" – For Further Credit, "FAV" – In Favor Of)

The IC3 recommends the filing of complaints regardless of dollar loss or timing of the incident.

2590. What additional steps should victims take beyond reporting a cyber-attack to the IC3 or other federal agency?

In 2015, the Cybersecurity Unit of the DOJ published Best Practices for Victim Response and Reporting of Cyber Incidents that included steps to take before, during and after a cyber intrusion or attack. These steps include, but are not limited to, the following:

- Inventory critical assets and processes;
- Develop an action plan prior to a cyber incident that includes measures to minimise continuing damage;
- Have access and appropriate authorisations in place to technology and services prior to a cyber-incident;
- Familiarise legal counsel with cyber-incident action plan to reduce response time during a cyber-incident;
- Notify people within the affected organisation, law enforcement and other potential victims;
- Avoid using the compromised system to communicate;
- Continue to monitor systems after a cyber-incident; and
- After the victim has recovered from the cyber-incident, reassess cybersecurity infrastructure and take remedial steps as needed.

2591. What information should financial institutions include when filing SARs on BEC/EAC fraud?

When filing a SAR, FinCEN requests that financial institutions include the appropriate key term "BEC Fraud" and/or "EAC Fraud" in the SAR narrative and in the SAR Characterisations field as well as the following information:

- Wire Transfer Details
  - Dates and amounts of suspicious transactions;
  - Sender's identifying information, account number and financial institution;
  - Beneficiary's identifying information, account number and financial institution; and
  - Correspondent and intermediary financial institution's information, if applicable.
- Scheme Details
  - Relevant email addresses and associated Internet Protocol (IP) addressees with their respective timestamps; and
  - Description and timing of suspicious email communications.

For further guidance on SARs, please refer to the Suspicious Activity Reports section.

2592. How many instances of cyber-related activities (i.e., identity theft, account takeover, unauthorised electronic intrusion) have been reported on SARs?

Of the 1.98 million suspicious activity report (SAR) filings from January 1, 2016 through December 31, 2016, reports of cyber-related activities (i.e., identity theft, account takeover, unauthorised electronic intrusion) totalled nearly 200,000 (10 percent) and were distributed across financial institution types as follows:

- Depository institutions: 142,000 cases (72 percent)
- Money services businesses (MSBs): 29,000 cases (15 percent)
- Other types of financial institutions (e.g., institutions outside of the other categories of financial institutions, institutions that file voluntarily): 18,000 cases (9 percent)
- Securities and futures firms: 8,800 cases (4 percent)
- Insurance companies: 350 cases (0.2 percent)
- Nonbank residential mortgage lenders and originators (RMLOs)/loan or finance companies: 209 cases (0.1 percent)
- Casinos and card clubs: 437 cases (0.2 percent)
- Housing GSEs: 28 cases (less than 0.1 percent)

2593. Can victims expect the recovery of stolen funds?

While there are no guarantees, FinCEN has partnered with the FBI and the USSS to help financial institutions recover funds stolen as a result of BEC schemes. FinCEN has a higher rate of recovery when BEC schemes are reported to law enforcement within 24-48 hours of the fraudulent wire transfer as they may be able to freeze funds before everything is lost.

Impact on Financial Institutions

2594. What are the obligations of financial institutions as they relate to reporting cybercrimes and cybersecurity?

Depending on the nature of the incident, financial institutions may need to comply with the following as they relate to cybercrimes and cybersecurity:

- Under **Section 5 of the Federal Trade Commission Act** (1914) disclosures of data breaches of customer information are required under the "unfair or deceptive acts or practices" (UDAP);
- **Office of Foreign Assets Control's (OFAC)** Cyber-Related Sanctions Program – Blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Designees are listed on the Specially Designated Nationals (SDN) List under the program tag [CYBER]. For further guidance, please refer to the Cyber-Related Sanctions Program section.
- The **Financial Enforcement Network (FinCEN)** requires covered financial institutions to report cyber-related events on Suspicious Activity Reports (SARs). For further guidance, please refer to the Suspicious Activity Reports section.
- The **U.S. Securities and Exchange Commission (SEC)** adopted multiple rules to address cybersecurity risks including, but not limited to, the following:
    - Regulation Systems Compliance and Integrity (SCI)
    - Regulation S-P
    - Regulation SDR
    - Regulation S-ID: Subpart C: Identity Theft Red Flags
    - Exchange Act Rule 13n-6
    - Exchange Act Rule 15c3-5
    - Investment Company Act Rule 38-1
    - Investment Advisers Act Rule 206(4)-7
- The SEC published guidelines on cybersecurity preparedness:

- Conducting periodic assessments on vulnerabilities, internal and external threats, controls, impact of threats, effectiveness of cybersecurity governance structure that also addresses identity theft, data protection, fraud and business continuity;
- Developing a strategy designed to prevent, detect and respond to cybersecurity threats;
- Implementing the cybersecurity strategy through written policies and procedures and training.

- While public companies are required to report any incident that causes "material harm," they are not specifically required to disclose cybersecurity failures and risks. In 2011, the SEC published guidance, not rules, on the disclosure obligations relating to cybersecurity risks and cyber incidents. Public companies are expected to disclose cybersecurity risks and cyber incidents that could have a "material adverse effect on the business." With each publicised cyber-attack or data breach, more pressure is being placed on the SEC to provide more clarity on previous guidance and issue rules requiring disclosures of cybersecurity risks and failures.
- The National Association of Insurance Commissioners (NAIC) issued "Principles for Effective Cybersecurity: Insurance Regulatory Guidance" which was derived from "Principles for Effective Cybersecurity Regulatory Guidance" by the Securities Industry and Financial Markets Association (SIFMA). The NAIC guidance lists 12 principles to assist state insurance regulators develop uniform standards. Topics covered include, but are not limited to, the following:
  - Safeguarding of personally identifiable consumer information including by third parties and service providers;
  - Risk-based, flexible, scalable regulatory guidance on cybersecurity consistent with national efforts (e.g., National Institute of Standards and Technology [NIST]);
  - Reporting of audit findings that present a material risk to the insurer to the board of directors or appropriate committee;
  - Participation in information sharing with other insurers to stay informed of emerging risks, threats as well as threat intelligence analysis and sharing; and
  - Periodic training for employees and other third parties on cybersecurity issues.
- Several federal agencies, such as the Department of Homeland Security (DHS), have established a mechanism to report potentially suspicious activity including, but not limited to, the following:
  - **Cyber incidents** – A violation or imminent threat of a computer security/acceptable use/standard security policy (e.g., failed or successful attempts to gain unauthorised access to a system, unauthorised use of a system, unwanted disruption, denial of service [DOS], unwanted changes to system hardware, firmware or software);
  - **Phishing** – Attempts to solicit information through social engineering techniques (e.g., emails appearing to be sent by legitimate organisations or known individuals, with links to fraudulent websites); and

- **Malware** – Software programs designed to damage or perform other unwanted actions on a computer system (e.g., viruses, worms, Trojan horses, spyware).

- Some states have enacted laws and regulations requiring financial institutions to establish cybersecurity programs and report cyber incidents to financial supervisors/regulatory authorities. Proposed in 2016 and finalised in 2017, the New York State Department of Financial Services (DFS) issued "Part 500 – Cybersecurity Requirements for Financial Services Companies" that requires the adoption of a cybersecurity program that, at a minimum, addresses the following core functions:
  - Identification of internal and external cyber risks (e.g., identification of stored Non-public Information [NPI] and how it can be accessed);
  - Use of defensive infrastructure to protect information systems and NPI from attacks and unauthorised access;
  - Detection of cybersecurity events;
  - Response to identified or detected cybersecurity events to mitigate negative impact;
  - Recovery from cybersecurity events and restoration to normal operations; and
  - Fulfilment of regulatory reporting obligations.

2595. Is the obligation to file SARs on cyber-incidents a new obligation?

No. Covered financial institutions were already obligated to file SARs on reportable transactions related to cybercrimes such as identity theft, account takeover and unauthorised electronic intrusions (UEI). The Cybersecurity Act of 2015, also known as the Cybersecurity Sharing Act (CISA) did not change the SAR reporting obligations of financial institutions.

2596. What obligations does the Advanced Notice of Proposed Rulemaking (ANPR) Enhanced Cyber Risk Management Standards impose on covered financial institutions?

The ANPR: Enhanced Cyber Risk Management Standards, published in October 2016, by the Federal Reserve Board (FRB), the Office of the Comptroller of the Currency (OCC) and the Federal Deposit Insurance Corporation (FDIC) targets financial institutions that are critical to the functioning of the financial sector. This may include the following types of entities with consolidated assets greater than or equal to US$50 billion:

- Banks and bank holding companies (BHCs)
- U.S. operations of foreign banking organisations
- Savings and loans
- Select nonbank financial institutions (NBFIs)
- Financial market utilities (FMUs)

- Select financial market infrastructures (FMIs)
- Third-party service providers (TPSPs) of the aforementioned entities

Covered entities would be required to demonstrate the following:

- **Cyber Risk Governance** - Effective cyber risk governance;
- **Cyber Risk Management** - Continuous monitoring and management of cyber risk within the risk appetite and tolerance levels approved by board of directors;
- **Internal Dependency Management** - Establishment and implementation of strategies for cyber resiliency and business continuity for business assets (e.g., workforce, data, technology, facilities) in the event of a disruption;
- **External Dependency Management** - Establishment of protocols for secure, immutable, transferable storage of critical records with third parties external to the organisation (e.g., outside vendors, service providers, suppliers, customers); and
- **Incident Response, Cyber Resilience and Situational Awareness** - Continuous situational awareness of operational status and cybersecurity posture on an enterprisewide basis.

The ANPR seeks comments on the scope, the proposed requirements of each of the aforementioned categories of cyber risk management standards, the proposal to implement the rule in a tiered approach (e.g., requiring enhanced standards for sector-critical institutions versus remaining covered institutions with consolidated assets greater than or equal to US$50 billion) and approaches to quantifying cyber risk.

In March 2017, the New York State Department of Financial Services (DFS) finalised Part 500 – Cybersecurity Requirements for Financial Services Companies, subjecting financial institutions operating in New York to additional cybersecurity requirements.

2597. Does the filing of a report with the IC3 or other federal agency obviate the need for a financial institution to file a SAR on a cyber-incident?

No. Reporting a cyber-incident to the IC3 or other federal agency does not obviate the need to file a SAR or notify law enforcement, if warranted. For further guidance on reporting potentially suspicious activity, please refer to the Suspicious Activity Reports section.

2598. Should financial institutions automatically file a SAR on detected cyber-incident?

No. A financial institution should not automatically file a SAR upon detection of a cyber-incident. The decision to file a SAR should be based on the institution's own investigation into the activity of the party that/who is involved in the cyber-incident. For further guidance on reporting potentially suspicious activity, please refer to the Suspicious Activity Reports section.

2599. Should financial institutions file SARs on otherwise reportable unsuccessful cyber-incident (e.g., no financial loss incurred by the customer)?

Yes. The obligation to file a SAR is not dependent on the success of the cyber-incident or if a financial loss occurred.

2600. Should the amount reported on SARs be limited only to losses due to cybercrimes?

No. Financial institutions should include losses as well as transactions that were at risk due to the cybercrime.

Cyber events can also take place with no transactions occurring. If the reportable threshold of US$5,000 is not met, the cyber-event will still need to be reported to the appropriate federal agency or law enforcement authority, even if a SAR is not warranted.

2601. Should financial institutions voluntarily report cyber-incidents that otherwise do not require the filing of a SAR?

FinCEN encourages financial institutions to file SARs on otherwise non-reportable cyber-incidents as these SARs are invaluable to law enforcement investigations.

2602. What information should financial institutions include when filing SARs on cyber-related events or cyber-enabled crimes?

When filing a SAR, FinCEN requests financial institutions to include cyber-related information and identifiers including, but not limited to, the following:

- Source and Destination Information:
  - IP address and port information with respective date timestamps in UTC (Coordinated Universal Time)
  - Uniform Resource Locator (URL)
  - Attack vectors
  - Command-and-control nodes
- File Information:
  - Suspected malware filenames
  - MD5, SHA-1 or SHA-256 hash information
  - Email content
- Subject User Names:
  - Email addresses
  - Social media account/screen names
- System Modifications:

  - Registry modifications
  - Indicators of compromise (IOCs)
  - Common vulnerabilities and exposures (CVEs)
- Involved Account Information:
  - Affected account information
  - Involved virtual currency accounts

2603. Should financial institutions share cyber events and cyber-enabled crimes with other financial institutions?

Yes. FinCEN encourages financial institutions to share cyber-event and cyber-enabled crime information with other financial institutions through Section 314(b) – Cooperation Among Financial Institutions of the USA PATRIOT Act. For further guidance on information sharing, please refer to Section 314 – Cooperative Efforts to Deter Money Laundering.

2604. Should financial institutions integrate cybersecurity programs into AML/CFT Compliance Programs?

FinCEN does not expect AML/CFT personnel to be knowledgeable on cyber events and cybersecurity; however, financial institutions are expected to collaborate with cybersecurity personnel to meet their AML/CFT obligations to report potentially suspicious activity. AML/CFT compliance personnel may want to incorporate cybersecurity considerations into their AML/CFT risk assessments.

2605. Should financial institutions address cybersecurity incidents even when there is no financial loss to the client?

Yes. In 2015, the SEC settled charges with a St. Louis-based investment adviser due to the failure to prepare an adequate cybersecurity program in advance of a breach that compromised the PII of approximately 100,000 individuals. The SEC advised that even though financial losses were not incurred by clients, charges would still be issued against the investment adviser for its lack of preparedness.

In addition to potential financial losses to clients and the institution (e.g., through activity related to the cyber-incident or through fines levied by regulatory authorities), financial institutions can face other damages such as loss of reputation.

For further guidance, please refer to the Cyber-Related Sanctions Program section.

2606. What are some of the common challenges to maintaining an effective cybersecurity program?

The following include some of the challenges that financial institutions have experienced in implementing a cybersecurity program:

- Inadequate/incomplete understanding of cyber threats;

- Critical assets remain vulnerable because they are not identified and/or not included in the cybersecurity program;
- Cybersecurity programs slow to address newest threats or inadequately address emerging threats;
- Inadequate response to sophisticated cyber-attacks such as advanced persistent threats (APTs);
- Companies fail to implement timely software patches that would reduce the risk of cyber intrusion;
- Vendors and partners not included in the cybersecurity program;
- Out-of-date training of employees and compliance personnel;
- Difficulty in hiring and/or retaining qualified cybersecurity professionals; and
- Lack of support demonstrated by senior management.

Alternative Value Transfer Systems

Basics

2607. What are alternative value transfer systems?

Alternative value transfer systems refer to nontraditional value transfer systems outside of the conventional financial services system (e.g., banking) which can include, but are not limited to, the following:

- Informal value transfer systems (IVTSs)
- Black Market Peso Exchange (BMPE)
- Reintegro
- Virtual Currency Systems
- Crowdfunding

For additional guidance on these aforementioned systems, please refer to the respective questions below.

2608. What key AML/CFT laws, regulations and actions have been passed related to alternative value transfer systems?

As new technologies and new methods to abuse these technologies emerge, the U.S. and individual states have passed various legislation and published guidance to address ML/TF risks including, but not limited to, the following:

- While included in the definition of "financial institutions" under the USA PATRIOT Act, money services businesses (MSBs) and providers and sellers of prepaid access are often considered to be alternative value transfer systems. For further guidance on their AML/CFT obligations, please refer to the sections: Money Services Businesses and Providers and Sellers of Prepaid Access.

- Section 373 - Illegal Money Transmitting Businesses of the USA PATRIOT Act specifically criminalises the operation of an unlicensed money transmitting business.
- The Financial Enforcement Network (FinCEN) has issued multiple guidance on virtual currencies, particularly on under which circumstances the existing AML/CFT requirements for MSBs would apply to certain virtual currency participants (e.g., administrators, exchangers).
- Initially proposed in 2014, New York finalised its "BitLicense" regulatory framework, Title 23, Chapter I, Part 200: Virtual Currencies in 2015, which includes AML/CFT, cybersecurity and consumer protection rules for virtual currency businesses operating in New York or with customers residing in New York.
- In October 2015, the Securities and Exchange Commission (SEC) finalised its Regulation Crowdfunding rule (Title III of the Jumpstart Our Business Startups [JOBS] Act of 2012), permitting companies to offer and sell securities through crowdfunding to raise capital up to an aggregate amount of US$1 million in a 12-month period under specific conditions without having to register the securities with the SEC or state securities regulators by providing a framework for the regulation of funding portals and broker-dealers.

For guidance on cybersecurity obligations of financial institutions, please refer to the Cyber-Related Events and Cybersecurity Preparedness section.

Informal Value Transfer Systems

Definitions

2609. What is an informal value transfer system (IVTS)?

An informal value transfer system (IVTS) refers to any system, mechanism or network of people that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, regardless of whether it is in the same form. They are networks that facilitate the transfer of value (e.g., cash, commodities) domestically or internationally outside the conventional financial systems. IVTS activities often do not involve traditional banking transactions or services, such as deposit or lending products, although they may sometimes use banking systems.

IVTSs are also known as informal money transfer systems (IMTSs), underground banking systems and alternative remittance systems. FATF uses the term "hawalas and other similar service providers (HOSSPs)" to describe IVTSs.

As they are informal, IVTSs are not licensed to operate as a value transfer system. Section 373 - Illegal Money Transmitting Businesses of the USA PATRIOT Act specifically criminalises the operation of an unlicensed money transmitting business.

2610. What are some examples of IVTSs?

FinCEN's "The Hawala Alternative Remittance System and its Role in Money Laundering" and the International Monetary Fund's (IMF) "The Hawala System" provide the following more common examples of IVTS:

- Hawala is an Arabic word that means “a bill of exchange or promissory note.”
- Hundi, a word that originated in India, means “trust” and “reference.”
- Fei-ch’ien, a Mandarin word, translates into “flying money” or “fast money.”

Other IVTSs including, but not limited to, phoe kuan (Thai), hui k’uan (Mandarin), ch’iao hui (Mandarin), nging sing kek (Cantonese), hui kuan (Vietnamese), stash house (South American) and chit house (British).

2611. What characteristics of an IVTS make it a preferred method of transferring funds by criminals?

All users benefit from the speed, cost-effectiveness and convenience of IVTSs; however, the following characteristics of an IVTS make this system a preferred method of transferring funds for illicit purposes:

- Many transactions do not involve the physical or electronic transfer of funds but instead are an exchange of debt.
- There are no official receipts of deposited funds and very limited or no paperwork.
- Due to the complex variations that can be used to conduct these transactions, they can be very difficult to detect.

2612. How do IVTSs work?

The various informal money transfer systems often provide paperless banking transactions and enable individuals to transfer large sums of cash from one country to another without the funds ever crossing borders or being recorded. The IVTS makes minimal use of any sort of negotiable instrument; the system is simply based on trust and “recordless” systems of transactions.

Transfers of money take place based on communications between members of a network of dealers. For example, when an individual wishes to send money to relatives in another country, he or she may contact local IVTS agents, who communicate payment instructions to their counterparts in the relatives’ country. The counterparts complete the transaction(s) and balance their accounts with future payments in the opposite direction. In some cases, IVTS agents utilise the traditional banking system and wire payments or funds transfers or other financial transactions on behalf of their customers. It is this latter type of IVTS that can be detected by a financial institution as an unlicensed money transmitter.

2613. Are IVTSs used only to transfer money?

No. Commodities can be transferred through this system as well.

2614. Are IVTSs illegal in the United States?

Yes. IVTSs are unlicensed money transmitters. Operating an unlicensed MSB, unless otherwise exempt from licensure by law, is deemed to be engaging in money laundering.

2615. Are IVTS operators required to establish AML Programs pursuant to Section 352 of the USA PATRIOT Act?

All money transmitters, licensed or not, are required to establish AML Programs and comply with other applicable AML/CFT requirements. As a practical matter, however, an unlicensed money transmitter is unlikely to be in compliance with AML/CFT requirements.

2616. What actions should a financial institution take if a customer is suspected of being an IVTS operator?

A financial institution that suspects or knows a customer is operating as an illegal money transmitter should file a SAR with FinCEN and then determine if it should close the account(s).

2617. Are there any penalties for unlicensed money transmitters/IVTS operators?

Yes. Penalties for operating an illegal money transmitting business include civil and criminal fines, imprisonment, or both.

Black Market Peso Exchange

2618. What is the Black Market Peso Exchange (BMPE)?

Generally, the Black Market Peso Exchange (BMPE) is an intricate trade-based money laundering (TBML) system in which transnational criminal organisations (TCOs) (e.g. Colombian drug cartels) sell drug-related U.S.-based currency to money brokers (e.g., peso broker) in a foreign country (e.g., Colombia) who, in turn, "exchange" the illicit U.S. currency for a foreign currency (e.g., Colombian peso) through a series of transactions involving multiple financial institutions that support legitimate international trade between foreign importers and U.S. exporters.

For example, once Colombian drug cartels deliver drug-related U.S. currency to peso brokers (directly or indirectly through the use of couriers or other transportation operators), peso brokers then may do the following:

- Place the illicit currency into U.S. bank accounts by structuring or smurfing transactions to evade BSA reporting requirements; and
- Sell monetary instruments drawn on their U.S. bank accounts to Colombian importers who use them to purchase U.S. goods; or
- Pay for U.S. goods directly (e.g., by delivering the illicit currency directly to U.S. exporters) on behalf of Colombian importers with reimbursement upon delivery of the goods in Colombia; or
- Smuggle drug-related U.S. currency out of the country for deposit into foreign financial institutions (FFIs) for repatriation to the peso broker or directly to a U.S. exporter through various methods (e.g., wire transfers, bulk shipments of currency), often involving correspondent banking relationships and/or *casas de cambio*; and
- Pay the Colombian drug cartels in pesos, less a fee, thereby completing the "foreign exchange" transaction, and effectively laundering drug-related currency.

The BMPE not only allows drug cartels to launder funds, it assists importers/exporters in evading trade controls and taxes. Peso brokers often fail to file required reports on reportable currency transactions and increasingly use new methods to launder illicit funds (e.g., funnel accounts, prepaid cards, mobile payments, digital currencies, internet gambling sites). Due to the complex nature of the transactions and the involvement of multiple third parties, BMPE activity is difficult to detect.

Although the BMPE in Colombia is one of the more widely known informal value transfer systems (IVTSs), BMPEs operate in other countries, too (e.g., Mexico, Panama).

2619. What is an example of a recent BMPE case?

In September 2014, U.S. federal agencies conducted "Operation Fashion Police," a raid busting a multi-million dollar BMPE scheme based out of Los Angeles' fashion district. Approximately US$65 million in cash and bank accounts were seized. Officials posed as cash couriers to catch participating businesses attempting to launder proceeds from narcotics sales by the Sinaloa drug cartel through legitimate trade in garment and clothing products. In September and October 2014, FinCEN issued a Geographic Targeting Order (GTO) imposing additional reporting and recordkeeping requirements on certain businesses located within the fashion district of Los Angeles.

Per U.S. federal agencies, Operation Fashion Police is part of a larger effort to crackdown on Mexican organised crime rings.

2620. How can financial institutions incorporate the detection of the BMPE within their suspicious activity monitoring programs?

Detecting BMPE activity is very difficult due not only to the complexity of the scheme but also to the lack of any one participant having access to all of the underlying transaction details necessary to detect such activity. Whether a broker, a *casa de cambio* or a bank, it is the responsibility of each participant to conduct adequate due diligence into the source and purpose of funds. Common red flags include, but are not limited to, the following:

- Structured currency deposits to individual checking accounts, often well below the typical levels for reporting, with multiple daily deposits to multiple accounts at different branches of the same bank on the same day
- Consumer checking accounts used for a period of time and then becoming dormant, and in some cases, overdrawn
- Personal checking accounts opened by foreign nationals who come to the bank together
- Multiple accounts opened on the same day or held by the same foreign nationals at various banks
- Frequent structured cash purchases of monetary instruments, including money orders or bank checks made payable to the same individuals or entities

For additional guidance on how to detect BMPE activity, please refer to sections: Informal Value Transfer System (IVTS) Red Flags and Trade Finance Red Flags.

Reintegro

2621. What does the term "reintegro" mean?

"Reintegro" refers to a trade-based, reverse-BMPE laundering scheme that hinges on trade document manipulation and often includes the corruption of a bank employee or customs official. Unlike traditional BMPE activities that operate with goods (not funds) crossing the border, in reintegro transactions, peso exchange brokers repatriate illicit proceeds, often from the sale of narcotics, by disguising them as payments for non-existent or overvalued goods using purchased export papers, similar to letters of credit, to make the payments appear legitimate. This is known as "reintegro" or "reintegrate papers."

2622. What is an example of a reintegro scheme?

The following is an example of a reintegro scheme:

- A Colombia-based peso broker purchases legitimate export forms from a corrupt bank employee and establishes a shell company, National Fruit. The Colombian peso broker's U.S.-based partner also establishes a shell company, Worldwide Fruit. Both companies share the same names with legitimate fruit companies as detailed on the purchased export forms. Both open business accounts at financial institutions in their respective countries. Cash derived from the selling of narcotics in the United States is then structured/smurfed into Worldwide Fruit's business account. The Colombia-based broker, under the pretense of shipping fruit to the United States, presents the purchased export forms to his financial institution to create the appearance that National Fruit has a legitimate reason to receive funds from Worldwide Fruit (i.e., payment for shipment of fruit). The funds are sent to National Fruit and deposited at the official exchange rate, which is more profitable than the traditional BMPE, where peso brokers sell pesos to Colombian businesses at a discounted rate.

2623. How many times can export papers be used to "reintegrate" illicit funds?

In the United States, purchased export papers or reintegro papers can remain valid for up to one year, so criminals are able to sell their use multiple times within that year.

2624. What is a "reverse hawala"?

"Hawalas" are typically used to transfer funds to countries in the Gulf and Pacific region from countries such as the United States. A "reverse hawala" is similar to the reintegro scheme that has been used by criminals to smuggle goods, such as gold, out of developing countries to avoid regulations, taxes and tariffs. Payment for the smuggled goods is made through the hawala either as a direct transfer or through the complex use of fraudulent export forms as described above.

Virtual Currency Systems and Participants

Definitions

2625. How is the term "virtual currency" defined?

FinCEN defines "**virtual currency**" as "a medium of exchange that operates like currency in some environments, but does not have all the attributes of real or fiat currency."

"**Currency**" is defined as the coin and paper money (including Federal Reserve notes and circulating notes of Federal Reserve banks and national banks) of the United States or of any other country that:

- Is designated as legal tender (i.e., form of payment defined by law which must be accepted by creditors as payment for debts);
- Circulates; and
- Is customarily used and accepted as a medium of exchange in the country of issuance.

"**Fiat currency**" is another term used to describe "real" currency that is government-issued.

Similarly, in its report "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," FATF defines "virtual currency" as a "digital representation of value that can be digitally traded and functions as:

- A medium of exchange; and/or
- A unit of account; and/or
- A store of value that does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction."

2626. Who are the typical participants of a virtual currency system?

FinCEN identifies three types of participants in a virtual currency system:

- A "**user**" is defined as "a person that obtains virtual currency to purchase [real or virtual] goods or services on the user's own behalf;" in other words, a consumer.
- An "**exchanger"** is defined as "a person engaged as a business in the exchange of virtual currency for real currency, funds or other virtual currency."
- An "**administrator**" is defined as "a person engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency."

FATF highlights other third parties that participate and support virtual currency systems, including, but not limited to, "**merchants**" that accept virtual currency in exchange for goods and services, "**wallet providers"** that provide a virtual currency wallet (e.g., software application, data file) for holding, storing and transferring virtual currency, "**third party payment senders**" that facilitate merchant acceptance, and "**software developers**" which provide applications to facilitate merchant

payment processing. Collectively, FATF refers to these products as virtual currency payments products and services (VCPPS).

2627. What is a "convertible virtual currency"? Is it a type of e-cash?

Both virtual currencies and e-cash are digital representations of value, but they are not the same.

FinCEN defines "convertible virtual currency," also known as open virtual currency, as a type of virtual currency that has "an equivalent value in real currency or acts as a substitute for real currency." It is not a form of e-cash.

"E-cash," also known as e-wallets or e-money, is a digital representation of fiat currency that can be stored and retrieved in several forms, including computer-based, mobile telephone-based and prepaid cards.

For further guidance on e-cash, please refer to the Electronic Banking and Digital Value section.

2628. Are convertible virtual currencies a type of prepaid access?

No. Prepaid access is defined as "access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number."

Per FinCEN, the term "funds or the value of funds" is limited to fiat currency, not virtual currency.

2629. How is virtual currency "converted" into fiat currency or vice versa?

Convertible virtual currency can be "converted" into fiat currency based on rules agreed upon by the community of users of a particular virtual currency system. This is distinct from a traditional currency "exchange" which is governed by the laws of fiat currency of each issuing jurisdiction (e.g., legal tender from one country "converted" into legal tender of another country based on foreign currency exchange rates).

Fiat currency is "converted" into virtual currency by a user's purchase of units of virtual currency.

2630. Is there agreement on whether virtual currency should be treated as fiat currency as it relates to financial crimes (e.g., money laundering)?

There are conflicting cases on whether virtual currency should be treated as fiat currency and therefore be used as evidence in criminal prosecutions. Examples include:

- Ross William Ulbricht, founder of Silk Road, a web-based criminal marketplace that enabled users to conduct illegal activity anonymously, operated his website from 2011 through 2013. Silk Road attempted to anonymise its users by using techniques such as an onion router (i.e., encrypted messages passed through a network of servers where each intermediary is only aware of the preceding and following nodes) to disguise IP addresses and utilising a bitcoin-based payment system. Despite efforts to stay hidden, the FBI was able to locate Silk Road's servers, identify users and ultimately build a case against Ulbricht. Though transactions were conducted in bitcoins, in

February 2015, the Manhattan court was able to successfully prosecute Ulbricht on charges of Narcotics Trafficking Conspiracy, Continuing Criminal Enterprise, Computer Hacking Conspiracy and Money Laundering Conspiracy.

- In July 2016, a Miami-Dade Circuit judge ruled that, under Florida law, virtual currency (e.g., bitcoin) is not a fiat currency and dismissed money laundering charges against a defendant who sold bitcoins to undercover detectives who stated their intent to use the bitcoins to purchase stolen credit card numbers.
- In early 2017, the Netherlands suggested proposing laws and regulations to recognise the use of a virtual currency mixer (a mechanism that "mixes" bitcoins to obscure the digital trail/ownership of bitcoins) as money laundering without having to prove a reasonable suspicion of an underlying crime. The Netherlands ultimately decided not to ban the use of virtual currency mixers but to include their use as a high-risk indicator for potentially suspicious activity.

2631. What are the heightened money laundering and terrorist financing risks of virtual currencies and virtual currency systems?

Virtual currencies and virtual currency systems pose heightened ML/TF risk due to the following factors:

- Rise in use in financial crimes (e.g., fraud, identity theft/account takeover, money laundering), especially by transnational criminal organisations
- Rise in use to finance illicit activities, purchase illicit goods and services and receive donations from anonymous donors
- Use of fraudulent methods to "mine" (generate) virtual currencies (e.g., botnets)
- Ease of funds movement across borders
- Lack of transparency (e.g., facilitation of anonymous virtual currency transfers through the use of avatars with fake identities)
- Inadequate screening against applicable sanctions listings (e.g., Office of Foreign Assets Control [OFAC] Sanctions Listings) due to limited or inaccurate user information
- Lack of historical regulatory oversight
- Lack of depth in AML/CFT compliance experience of operators/employees of virtual currency systems, especially those operating in multiple jurisdictions with varying regulatory requirements
- System weaknesses in technological infrastructure of virtual currency systems
- Lack of familiarity/understanding of financial/technical infrastructure and roles of participants of virtual currency systems
- In decentralised systems, the lack of a single administrator inhibits obtaining user and transaction information for further investigation by law enforcement authorities

- Use of third-party service providers (e.g., exchangers, wallet providers) further obscures the money trail

2632. Do all virtual currency systems pose the same degree of risk?

No. According to the European Central Bank's report issued in October 2012, "Virtual Currency Schemes," there are generally three types of virtual currency systems, each posing varying levels of ML/TF risk:

- **Closed virtual currency systems –** Allows users to buy virtual currency (e.g., units, credits) with fiat currency for the purpose of purchasing virtual goods and services within that closed system (e.g., gaming systems in which users can "purchase" virtual items created by the game developers). Virtual currency in this closed system cannot be used in the real economy.
- **Unidirectional virtual currency systems** – Allows users to buy virtual currency with fiat currency for the purpose of purchasing both virtual and real goods and services (e.g., participating merchants accept virtual currency payments in exchange for virtual or real products such as a frequent flyer program).
- **Bidirectional virtual currency systems** – In addition to the activities in the unidirectional virtual currency system, users can convert virtual currency into real currency (known as convertible virtual currency) and transfer value to other users or to other locations.

Both FinCEN and FATF add another key distinction that impacts ML/TF risk:

- **Centralised virtual currency systems** – A single administrator (issuer) controls a centralised repository (e.g., establishes and enforces rules [e.g., creation, allocation, exchange rates], maintains a ledger).
- **Decentralised virtual currency systems** – No single administrator (e.g., tasks are executed by users); no centralised repository, also referred to as peer-to-peer systems or cryptocurrencies (e.g., bitcoin).

The decentralised bidirectional virtual currency system poses the most ML/TF risk as it facilitates third-party transfers and lacks a single authority responsible for providing oversight.

It is important to note that these classifications may change as the virtual currency industry evolves.

2633. Are internet-based payment systems a type of virtual currency system?

Internet-based payment systems allow users to purchase goods and services and transfer funds to/from each other. The digital payments and transfers represent fiat currency. Unless the internet-based payment system begins using virtual currencies, they do not fall under the definition of a virtual currency system; however, they are considered money transmitters and thus are subject to the AML/CFT requirements of MSBs.

2634. Other than buying virtual currency with fiat currency, how can users "obtain" virtual currency?

In addition to purchasing virtual currency with fiat currency, users can "obtain" virtual currency by completing certain activities (e.g. lending computer processing power to the virtual currency system, executing certain tasks on behalf of the administrator of the virtual currency system) in exchange for "payment" in virtual currency. The type of activities and the "virtual currency pay rate" is determined by the users of a particular virtual currency system. Terms used to describe these activities include, but are not limited to, mining, harvesting, earning, manufacturing and self-generating.

FATF defines a miner as "an individual or entity that participates in a decentralised virtual currency network by running special software to solve complex algorithms in a distributed proof-of-work or other distributed proof system used to validate transactions in the virtual currency system."

Tech-savvy users can create their own virtual currencies as well.

2635. Is virtual currency typically stored within the virtual currency system?

Virtual currency can be stored within the virtual currency system, with a third-party service provider (e.g., wallet provider) or locally on the computers of users.

2636. What are "botnets"?

Botnets are a type of malware that can be used to conduct online criminal behaviour (e.g., send spam email, perform denial of service attacks, illegally mine virtual currency).

2637. What are some examples of money laundering cases involving virtual currencies?

In May 2013, Liberty Reserve, an unlicensed money transmitter of virtual currency based out of Costa Rica, was designated as a financial institution of primary money laundering concern by the U.S. Department of the Treasury under Section 311 – Special Measures of the USA PATRIOT Act.

Liberty Reserve allegedly facilitated the laundering of approximately US$6 billion derived primarily from narcotics trafficking, fraud (e.g., credit card, investment, identity theft), computer hacking and child pornography. Liberty Reserve allowed its users to deposit and withdraw funds through designated exchange houses located in jurisdictions with lax AML/CFT controls and transfer funds to/from other users in virtual currency (e.g., "Liberty Reserve Dollars," "Liberty Reserve Euros"), often anonymously.

As a result, the fifth level of Special Measures was imposed against Liberty Reserve:

- Prohibition on the provision of correspondent accounts on behalf of Liberty Reserve and implementation of special due diligence on other correspondent accounts to prohibit the facilitation of transaction(s) on behalf of Liberty Reserve.

For further guidance on Special Measures, please refer to Section 311 – Special Measures.

Recently, vulnerabilities within virtual massively multiplayer online games (MMOGs) (e.g., Second Life, EverQuest, Worlds of Warcraft) have been exploited by criminals for financial gain (e.g., account takeover, fraud, theft, money laundering). For example, many virtual MMOGs allow users to purchase

virtual items that can be sold/exchanged and ultimately transfer value anonymously to other users or criminals posing as multiple users with the purpose of obscuring the origins/ownership of the assets/funds. Many virtual MMOGs lacked customer verification procedures, thereby reducing the investigative trail to a debit/credit card/prepaid card transaction used at the placement or withdrawal phase. Additionally, illegal acts such as internet gambling were permitted in some virtual MMOGs. While some have moved to ban simulated activities of acts that are illegal in real life, the virtual MMOGs remain vulnerable to abuse without proper oversight by regulatory authorities.

2638. What factors should be considered to assess the ML/TF risks of virtual currency systems?

The following factors can be used to assess ML/TF risks of virtual currency systems:

- Type of virtual currency system (e.g., closed, unidirectional, bidirectional, centralised, decentralised)
- Volume and amount of transactions
- Types of underlying customers serviced by the virtual currency system provider
- Geographic considerations (e.g., location of business operations, location of customers, origination/destination of transactions)
- Strength of AML/CFT, anti-fraud and privacy programs, policies and procedures of the virtual currency provider (e.g., type and validity of customer information, sanctions screening, monitoring for potentially suspicious activity, protection of sensitive customer information)

For further guidance on risk assessments, please refer to the Customer Risk Assessments section.

2639. How do the FATF Recommendations address virtual currencies?

FATF Recommendation 15 – New Technologies advises countries and financial institutions to conduct risk assessments to identify and evaluate the ML/TF risks and vulnerabilities of new technologies. FATF uses the term new payment products and services (NPPS) to describe some of the new product offerings (e.g., prepaid cards, mobile payments, electronic money, digital currencies).

FATF published three reports addressing new technologies, including virtual currencies, "Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Systems" (2013), "Virtual Currencies: Key Definitions and Potential AML/CFT Risks" (2014) and "Guidance for a Risk-Based Approach to Virtual Currencies" (2015).

FATF refers to virtual currency products as virtual currency payments products and services (VCPPS) and focuses its latest guidance on convertible virtual currency exchangers. FATF suggests countries develop de minimis thresholds on virtual currency transactions equal to or less than the wire transfer thresholds of US$15,000 outlined in **FATF Recommendation 16 – Wire Transfers,** which will trigger due diligence measures.

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

2640. How is the term "cryptocurrency" defined?

"Cryptocurrency" is defined by FATF as "... a math-based, decentralised convertible virtual currency that is protected by cryptography.—i.e., it incorporates principles of cryptography to implement a distributed, decentralised, secure information economy. Cryptocurrency relies on public and private keys to transfer value from one person (individual or entity) to another, and must be cryptographically signed each time it is transferred. The safety, integrity and balance of cryptocurrency ledgers is ensured by a network of mutually distrustful parties (in Bitcoin, referred to as miners) who protect the network in exchange for the opportunity to obtain a randomly distributed fee (in Bitcoin, a small number of newly created bitcoins, called the 'block reward' and in some cases, also transaction fees paid by users as an incentive for miners to include their transactions in the next block). Hundreds of cryptocurrency specifications have been defined, mostly derived from Bitcoin, which uses a proof-of-work system to validate transactions and maintain the block chain. While Bitcoin provided the first fully implemented cryptocurrency protocol, there is growing interest in developing alternative, potentially more efficient proof methods, such as systems based on proof-of-stake."

2641. What is blockchain technology?

Blockchain technology, also known as distributed ledger technology (DLT), is generally defined as the secure distributed ledger of digital events that uses consensus and cryptography to validate each transaction while also protecting the identities of all participating parties. Blockchain technology expedites the payment process securely and with transparency by grouping transactions to form encrypted blocks that are confirmed through digital signatures and network consensus. There are many applications of this technology that can be used to support AML/CFT compliance. For further guidance, please refer to The Future of AML/CFT Technology section.

2642. Is blockchain technology only used in cryptocurrency?

No. While blockchain technology is commonly associated with cryptocurrency, it has applications in the following areas:

- Settling of electronic payments in the broader financial services industry, with a particular impact on cross-border wire transfers, Automated Clearing House (ACH) transactions and peer-to-peer payments;
- Facilitating digital documentation transfer of legal documents and property titles; and
- Providing electronic sign-offs using smart contracts (e.g., digital documentation of management approvals in a compliance setting).

For further guidance on technology, please refer to the AML/CFT Technology section.

2643. Of what risks related to blockchain technology should financial institutions be aware?

Blockchain technology is not an additive technology that will supplement legacy payment systems. It will likely replace legacy systems causing a significant disruption to existing payment systems.

With respect to AML/CFT processes, the most significant adjustments may need to occur in suspicious activity transaction monitoring (e.g., new or modified rules to detect irregularities). Some suggest transaction monitoring may need to occur on a state or global level, not an institutional level, to properly monitor all the participants in blockchain transactions by changing the role of financial institutions from monitor to provider of data to regulatory authorities for their analysis.

R3 is a financial innovation firm leading over 75 of the world's leading financial institutions in researching the use and development of blockchain technology, so the adoption of blockchain technology in broader applications will likely continue to gain momentum. While some financial institutions may remain reluctant to adopt blockchain technology due to having to partner or share information with competitors, the advantages may ultimately outweigh any perceived disadvantages.

2644. What is a "bitcoin mixer"?

A "bitcoin mixer," "bitcoin blender" or a "bitcoin tumbler" mixes received bitcoins with other bitcoins sent by other parties and returns an equal amount of different bitcoins to the sender to obscure any electronic trails that could trace the bitcoins to the original sender/wallet. Examples include, but are not limited to, Onion Wallet, BitMixer and Bitcoin Boost. Some countries (e.g., Netherlands) are proposing laws and regulations to recognise the use of a bitcoin mixer as money laundering without having to prove a reasonable suspicion of an underlying crime.

2645. What key guidance has been published on virtual currencies?

Key guidance issued on virtual currencies includes, but is not limited to, the following:

- **Virtual Currencies: Key Definitions and Potential AML/CFT Risks** (2014) by the Financial Action Task Force (FATF)
- **Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Systems** (2013) by FATF
- **Virtual Currency Schemes** (2012) by the European Central Bank (ECB)
- **BitLicense Framework** (proposed regulation Title 23, Chapter I, Part 200: Virtual Currencies) (2014) by the New York State Department of Financial Services (DFS)
- **Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies** (FIN-2013-G001) (2013) by FinCEN
- **Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity** (FIN-2014-R002) (2014) by FinCEN
- **Application of FinCEN's Regulations to Virtual Currency Mining Operations** (FIN-2014-R001) (2014) by FinCEN
- **Application of Money Services Business Regulations to the Rental of Computer Systems for Mining Virtual Currency** (FIN-2014-R007) (2014) by FinCEN
- **Emerging Regulatory, Law Enforcement and Consumer Protection Challenges** (2014) by the U.S. Government Accountability Office (GAO)

- **Bitcoin Virtual Currency: Unique Features Present Distinct Challenges for Deterring Illicit Activity** (2012) by the Federal Bureau of Investigation (FBI)
- **Cyber Criminal Exploitation of Electronic Payment Systems and Virtual Currencies** (2011) by the FBI
- **Cyber Criminal Exploitation of Real-Money Trading** (2011) by the FBI
- **The Digital Economy: Potential, Perils, and Promises: A Report of the Digital Economy Task Force** (2014) by Thomson Reuters and the International Centre for Missing & Exploited Children

Key groups tasked with addressing the risks of virtual currencies and the virtual economy include, but are not limited to, the following:

- The **Digital Economy Task Force** lead by Thomson Reuters and the International Centre for Missing & Exploited Children in partnership with the FBI, Immigrations and Customs Enforcement (ICE) of the U.S. Department of Homeland Security (DHS), the U.S. Department of State, the United States Agency for International Development (USAID) and leaders from academia, financial and web services and the nonprofit sector
- **Virtual Currencies Emerging Threats Working Group** within the U.S. Department of Justice
- **Electronic Crimes Task Forces (ECTF) and Working Groups** lead by the Secret Service in partnership with ICE-HSI (Homeland Security Investigations), academia, law enforcement and the private sector

Current and Pending AML/CFT and Sanctions Requirements

2646. What regulatory guidance or regulations govern virtual currency activities?

In the United States, at the federal level, FinCEN issued guidance in March 2013 applying existing AML/CFT requirements for money services businesses (MSBs) to certain businesses that conduct activities with convertible virtual currencies (e.g., administrators, exchangers).

In July 2014, the New York State Department of Financial Services (NYDFS) proposed a regulatory framework for virtual currency businesses under Title 23, Chapter I, Part 200: Virtual Currencies, referred to as the "BitLicense Framework," which was finalised in 2015. The BitLicense Framework exempts merchants and consumers of virtual currencies and requires covered businesses to establish an AML Program that includes customer identification, recordkeeping, suspicious activity reporting procedures and other cybersecurity and consumer protection requirements. All virtual currency transactions in excess of US$10,000 would be required to be reported to the NYDFS as well as potentially suspicious virtual currency transactions in any amount.

Internationally, in October 2014, Europol called on the European Union to legislate the use of virtual currencies by applying the existing AML/CFT framework for fiat currencies to virtual currencies. The Council of the European Union published the Council Framework Decision: Combating Fraud and

Counterfeiting of Non-Cash Means of Payment in 2001 and have developed multiple initiatives to address ML/TF with virtual currencies, including, but not limited to, workshop and the formation of a working group of Europol, INTERPOL and the Basel Institute on Governance to gather information, organise workshops and meetings to exchange collected information and create a network of experts to provide assistance and recommendations to those inside and outside of the working group.

2647. Are virtual currency exchangers and administrators required to establish an AML Program pursuant to Section 352 of the USA PATRIOT Act?

Yes. FinCEN has issued multiple rulings on the application of the definition of "money transmitters" and "money transmission services" to virtual currency activities.

A money transmitter is defined as the following:

- Any person engaged in the transfer of funds
- A person who provides money transmission services

"Money transmission services" is defined as "the acceptance of currency, funds or other value that substitutes for currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."

"By any means" includes money transmission through the following:

- A financial agency or institution;
- A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both;
- An electronic funds transfer network; or
- An informal value transfer system (IVTS).

Exchangers and administrators of convertible virtual currencies transfer "value that substitutes for currency to another location or person," and, therefore, fall under the regulatory definition of a money transmitter. As money transmitters, exchangers and administrators of convertible virtual currencies are required to establish AML Programs and comply with other AML/CFT reporting and recordkeeping requirements (e.g., currency transaction reports [CTRs], suspicious activity reports [SARs]).

Other participants using/engaging virtual currencies (e.g., miners, investors, software developers, businesses that rent computer systems for mining) did not fall under the definition of money transmitter. For further guidance, please refer to the FinCEN rulings provided below.

2648. Do exchangers of convertible virtual currency fall under the definition of dealers in foreign exchange?

No. Dealers in foreign exchange are defined as "a person that accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds or other instruments denominated in

the currency, of one or more countries in an amount greater than US$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery."

Virtual currencies are not fiat currencies and therefore do not fall under the definition of dealers in foreign exchange.

2649. Are e-currencies and e-precious metals examples of virtual currencies? Would broker-dealers trading in e-currencies and e-precious metals fall under the definition of a money transmitter as an administrator or exchanger of convertible virtual currencies?

According to FinCEN, trading in e-currencies and e-precious metals typically involves a broker-dealer "electronically distributing digital certificates of ownership of real currencies or precious metals, with the digital certificate being the virtual currency." The digital certificate acts as a substitute for the underlying fiat currency and precious metal.

However, the activity of trading in digital certificates would not subject broker-dealers of e-currencies and e-precious metals to the definition of a money transmitter as an administrator or exchanger of convertible virtual currencies. Like broker-dealers in real currency and other commodities, if a broker-dealer "accepts and transmits funds solely for the purpose of effecting a bona fide purchase or sale of the real currency [or e-currency or e-precious metal] or other commodities for or with a customer, such a person is not acting as a money transmitter."

For further guidance on FinCEN's ruling, please refer to Application of the Definition of Money Transmitter to Brokers and Dealers in Currency and Other Commodities (FIN-2008-G008) (2008).

2650. Are decentralised virtual currency systems subject to AML/CFT requirements of money transmitters?

According to FinCEN, a decentralised convertible virtual currency system that "has no central repository and no single administrator [in which] persons may obtain [virtual currency] by their own computing or manufacturing effort" is not subject to the AML/CFT requirements of money transmitters, if the person uses "earned" units of convertible virtual currency solely for personal use (e.g., purchase of virtual or real goods and services). If the person transfers earned units of convertible currency from one person to another (or to a different location), then the person would be subject to the AML/CFT requirements of a money transmitter.

2651. Have additional regulations been proposed for virtual currency?

Yes. Section 13 of the proposed bill Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017, introduced by the U.S. Senate in May 2017, proposed amending the definition of monetary instrument to include funds stored in a digital format (e.g., prepaid access devices, virtual currency). Whether this bill will ever be passed into law is unclear.

2652. What steps can a financial institution take to mitigate the risks of customers who are administrators and exchangers of convertible virtual currencies?

Financial institutions should perform initial and ongoing due diligence on administrators and exchangers of convertible virtual currencies. They also should consider including contractual commitments advising of the financial institution's expectations with respect to preventing the use of the machines for illicit activities, requiring notification of a change in ownership and monitoring shipments for unusual activity.

Following are examples of the types of due diligence that may be performed on these customers:

- Review corporate documentation, licenses, permits, contracts or references.
- Review public databases to identify potential problems or concerns with principal owners or advertisements affiliated with high-risk activities (e.g., escort services, get-rich-quick investment schemes).
- Review existing relationships with other financial services providers (e.g., financial institutions who accept deposits and transfer funds on behalf of the virtual currency system operator).
- Review expected volumes.
- Review and/or visit locations of operations of virtual currency system operators.

Additionally, financial institutions should monitor administrators and exchangers of convertible virtual currencies for suspicious activity by comparing expected versus actual virtual currency transaction activity levels, and also compare the level of activity to other virtual currency exchangers in comparable geographic and demographic locations. Some examples of red flags include, but are not limited to, the following:

- Customer is unlicensed or unregulated, where licensing/regulation is required.
- Customer is not affiliated or backed by a traditional financial institution.
- Customer is linked to nonbanking financial institutions (e.g., *casas de cambio*) in high-risk jurisdictions for criminal activity and financial crimes or lax AML/CFT systems.
- Customer has lax customer identification and monitoring policies and procedures and/or does not enforce AML/CFT policies, thus facilitating anonymous transactions.
- Customer is linked to advertisements of businesses involved in potentially illicit activities (e.g., illegal internet gambling, unregulated pharmaceutical companies, escort services, get-rich-quick investment schemes).

For additional guidance on red flags for potentially suspicious activity, please refer to the Suspicious Activity Red Flags section.

Crowdfunding

2653. What is "crowdfunding" and what are its heightened ML/TF risks?

Crowdfunding is an internet-based method of raising funds from individual contributions from a large number of people (a crowd) to support various businesses, projects or causes. Popular platforms include Kickstarter and IndieGoGo. Social media coupled with a payment service (e.g., PayPal) has also been used as a form of crowdfunding.

The following characteristics, which may apply in varying degrees, heighten the money laundering and terrorist financing risks of crowdfunding platforms:

- High volume of transactions
- High-risk nature of customer/donor/investor base (e.g., anonymous, geographically dispersed; financially sophisticated; increased use of corporate structures, such as offshore private investment companies; lack of ongoing relationships with customers)
- Ability to transfer funds domestically and internationally, particularly to jurisdictions with weak AML/CFT requirements
- Historically less regulated, less stringently regulated or less uniformly regulated than traditional financial institutions, such as depository institutions
- Potentially weaker controls than traditional financial institutions due to fewer regulatory pressures
- Possibility of operating without proper registration or licensing

2654. What is a recent ML/TF case involving crowdfunding?

The US$28,500 loan allegedly used by Syed Farook and Tashfeen Malik, the couple who allegedly killed 14 and injured 22 people in a 2015 terrorist attack in San Bernardino, California, originated from Prosper Funding LLC, a peer-to-peer crowdfunding platform enabled by WebBank, a state-chartered industrial bank that provides private-label and bank card financing programs. Although Prosper Funding LLC had AML/CFT measures in place to validate identity and screen against Specially Designated Nationals (SDN) lists provided by the Office of Foreign Assets Control (OFAC), because the couple had not engaged in a documented history of terrorist or potentially suspicious activity, they were not flagged by Prosper for further investigation.

After the attack, various crowdfunding platforms were also utilised to raise funds for the victims and their family members.

2655. What is a "funding portal"?

The SEC defines "funding portal," also known as an equity crowdfunding platform, as "any person acting as an intermediary in a transaction involving the offer or sale of securities for the account of others that does not:

- Offer investment advice or recommendations;
- Solicit purchases, sales or offers to buy the securities offered or displayed on its website or portal;

- Compensate employees, agents or other persons for such solicitation or based on the sale of securities displayed or referenced on its website or portal;
- Hold, manage, possess or otherwise handle investor funds or securities; or
- Engage in such other activities as the SEC, by rule, determines appropriate."

2656. Are funding portals subject to AML/CFT laws and regulations?

Unless also acting as a covered financial institution as defined by the USA PATRIOT Act, a funding portal is not independently subject to AML/CFT laws and regulations, as funding portals were exempted from registering securities with the SEC under the Regulation Crowdfunding rule (Title III of the Jumpstart Our Business Startups [JOBS] Act of 2012). Under the Regulation Crowdfunding rule, companies are permitted to offer and sell securities through crowdfunding to raise capital up to an aggregate amount of US$1 million in a 12-month period under specific conditions without having to register the securities with the SEC or state securities regulators by providing a framework for the regulation of funding portals and broker-dealers.

To address this gap, in April 2016 FinCEN issued a notice of proposed rulemaking (NPRM) 81 FR 19086 seeking to amend the definition of "broker or dealer in securities" to include funding portals that are involved in the offering or selling of crowdfunding securities pursuant to the Securities Act of 1933. The NPRM only addresses funding portals that offer or sell securities. Additional proposals would need to be published to address other types of funding portals (e.g., person to person, charities). If finalised, funding portals would be subject to the AML/CFT requirements of broker-dealers. For further guidance, please refer to the Broker-Dealer section.

2657. What can financial institutions do to mitigate the risks of crowdfunding?

Financial institutions can implement the following to mitigate the risks of crowdfunding:

- Update Know Your Customer (KYC) procedures to detect and obtain due diligence from crowdfunding customers;
- Update suspicious transaction monitoring procedures to detect use of crowdfunding platforms within customer activity; and
- Update training to reflect the AML/CFT risks of crowdfunding platforms and measures to mitigate these risks.

Human Trafficking and Migrant Smuggling

Basics

2658. What is human trafficking?

FinCEN defines human trafficking, which is also known as modern slavery, as the "act of recruiting, harbouring, transporting, providing or obtaining a person for forced labour or commercial sex acts through the use of force, fraud or coercion."

2659. What is migrant smuggling?

Migrant smuggling, which is also known as human smuggling or alien smuggling, is defined by FinCEN as "acts or attempts to bring unauthorised aliens to or into the United States, transport them within the U.S., harbour unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status."

2660. What are the stages of human trafficking and migrant smuggling?

Human trafficking generally involves three stages:

- **Recruitment/Abduction**: This initial stage involves the recruitment of a person from his/her community or country, often by coercion, deception or bondage (e.g., fake job offers, arranged marriages, educational opportunities).
- **Transportation**: This stage involves the movement of people, whether within the same geographic location (e.g., country) or across international borders, often by planes, boats or trains.
- **Exploitation**: This is the final stage of human trafficking, where victims are sold for various exploitative reasons including, but not limited to, the following:
    - Bride trafficking
    - Child trafficking
    - Debt bondage
    - Forced labour
    - Illegal adoption
    - Removal of organs
    - Servitude
    - Sex tourism
    - Sexual labour
    - Slavery

The physical transportation of victims from one location to another is not required for the crime to fall within the definition of human trafficking.

Migrant smuggling, similarly, involves three stages:

- **Solicitation**: Victim seeks services of a facilitator/smuggler (also known as "coyotes" in some regions).
- **Transportation**: Same as human trafficking; involves the movement of people, whether within the same geographic location (e.g., country) or across international borders, often by planes, boats or trains.

- **Payment**: Migrants pay the smuggler (in advance, partially or upon arrival) and live in the "receiving" country, often as undocumented aliens.

As a vulnerable and isolated group, it is not uncommon for migrants to be sold for the same exploitative reasons as individuals who are victims of human trafficking during the final stage.

2661. How is migrant smuggling different from human trafficking?

According to FinCEN, the differences are as follows:

- Human trafficking involves the use of force or coercion; whereas migrant smuggling involves persons choosing to immigrate illegally. Human trafficking may involve individuals of any legal status, whereas migrant smuggling involves foreign nationals.
- Human trafficking involves exploitation of victims (e.g., forced labour) and does not need to involve illegal border crossing; whereas the crimes in migrant smuggling are generally limited to illegal border crossings or the harbouring of undocumented aliens.

2662. What is the scale of human trafficking and migrant smuggling?

According to multiple U.S. officials, human trafficking and migrant smuggling are the fastest growing crimes in the world: While many of the victims are from developing nations, the victims end up in highly industrialised nations.

The International Labour Office (ILO) estimates that more than US$150 billion in illegal profits are generated annually from 21 million victims of human trafficking and migrant smuggling, with approximately two-thirds of that amount related to sexual exploitation and one-third in forced labour exploitation.

The following are select statistics and trends related to human trafficking and migrant smuggling:

- According to the ILO, domestic work, agriculture, construction, manufacturing and entertainment are high-risk sectors for human trafficking and migrant smuggling.
- Although not an official number, the U.S. Department of State estimates 600,000-800,000 people are trafficked across international borders annually with approximately 50,000 individuals entering the United States.
- According to the National Center for Missing and Exploited Children (NCMEC), one in six runaways reported to their center in 2016 were likely sex trafficking victims, of which 86 percent were in the care of social services or foster care when they went missing.
- Of the nearly 190 countries evaluated by the U.S. State Department in the Trafficking in Persons Report of 2016, approximately 19 percent were fully compliant with minimum standards for anti-human trafficking, 41 percent were partially compliant, 23 percent were placed on watch and 14 percent were noncompliant.
- According to the last Polaris Project Annual State Ratings published in 2014, 39 states had strong anti-human trafficking laws in 2014, an increase of 18 from 2012; and two states (North Dakota and South Dakota) needed active improvement.

- According to the U.S. Department of State, the number of global trafficking prosecutions grew from over 5,800 (with over 3,100 convictions) in 2006 to nearly 19,000 (with over 6,600 convictions) in 2015. More than 77,000 trafficking victims were identified in 2015.

The fact that very little information related to human trafficking has been reported on SARs is indicative of how underreported this crime is and how difficult it is for financial institutions to detect.

2663. What are the key U.S. laws that address human trafficking and migrant smuggling?

The following U.S. laws establish key definitions and guidelines to combating human trafficking and migrant smuggling:

- The Trafficking Victims Protection Act (TVPA) of 2000
- Trafficking Victims Protection Reauthorisation Act of 2003
- Trafficking Victims Protection Reauthorisation Act of 2005
- Trafficking Victims Protection Reauthorisation Act of 2008
- Trafficking Victims Protection Reauthorisation Act of 2013
- Justice for Victims of Trafficking Act (JVTA) of 2015

The TVPA laws define "severe forms of trafficking in persons" as:

- Sex trafficking in which a commercial sex act is induced by force, fraud or coercion, or in which the person induced to perform such an act has not attained 18 years of age; or,
- The recruitment, harbouring, transportation, provision or obtaining of a person for labour or services, through the use of force, fraud or coercion, for the purpose of subjection to involuntary servitude, peonage, debt bondage or slavery.

The JVTA made amendments to the TVPA including, but not limited to, the following:

- Expands or amends key definitions and classifications of certain crimes (e.g., child abuse, child pornography) to fall within the trafficking offense;
- Imposes additional assessments and asset forfeiture penalties;
- Makes traffickers and buyers equally culpable for sex trafficking offenses;
- Extends the statute of limitation for civil actions against perpetrators until 10 years after the victim reaches age 18;
- Expands the authority of the DOJ to intercept wire, oral or electronic communications to include investigations of trafficking offenses;
- Establishes a fund to award grants to states and localities to assist in expanding capabilities to combat trafficking and assist victims;
- Amends and expands treatment programs for victims (e.g., replaced the original residential treatment programs for victims to renewable grant-based programs administered by the DOJ);

- Requires the notification of victims of plea bargains or deferred prosecution agreements consistent with the Victims' Rights and Restitution Act of 1990;
- Requires expanded training (e.g., online, briefings, annual reminders) related to trafficking for federal personnel (e.g., threats, methods, warning signs);
- Additional expansions and amendments to existing legislation addressing the various phases of anti-trafficking efforts and responses (e.g., prevention, survivor services, awareness, training) were made by the following JVTA provisions:
    - Combat Human Trafficking Act of 2015
    - Survivors of Human Trafficking Empowerment Act of 2015
    - Bringing Missing Children Home Act of 2015
    - Stop Advertising Victims of Exploitation Act (SAVE) of 2015
    - Human Exploitation Rescue Operations Act (HERO) of 2015
    - Rape Survivor Child Custody Act of 2015
    - Military Sex Offender Reporting Act of 2015
    - Trafficking Awareness Training for Health Care Act of 2015
    - Ensuring a Better Response for Victims of Child Sex Trafficking of 2015
    - Human Trafficking Survivors Relief and Empowerment Act of 2015

The JVTA of 2015 also established a National Strategy to Combat Human Trafficking (National Strategy) which requires the DOJ to report annually on the anti-trafficking efforts of key federal agencies (e.g., Federal Bureau of Investigation [FBI], Civil Rights Division Human Trafficking Prosecution Unit [HTPU], Criminal Division's Child Exploitation and Obscenity Section [CEOS], U.S. Attorney's Offices [USAO], Office of Justice Programs [OJP]) as well as efforts executed by state, local and tribal authorities. The National Strategy also includes the following:

- Assessment of the threat presented by human trafficking based on FBI cases and experience;
- District-specific anti-trafficking strategies developed by each USAO;
- Analysis of human trafficking and anti-trafficking efforts in the American Indian (AI) and Alaskan Native (AN) communities (e.g., high-risk Native communities in Montana, Alaska, North Dakota);
- Annual spending dedicated to prevent and combat human trafficking; and
- Plans to encourage cooperation, coordination and mutual support of anti-trafficking efforts between federal agencies, the private sector and the nonprofit sector.

Pursuant to the JVTA, in 2015, the United States appointed eleven trafficking survivors to the U.S. Advisory Council on Human Trafficking to provide recommendations on federal anti-trafficking policies. In October 2016, the council released its first report, "United States Advisory Council on Human Trafficking: Annual Report."

In March 2017, the U.S. Congress introduced Targeted Rewards for the Global Eradication of Human Trafficking to offer financial rewards leading to the arrest or conviction of international human traffickers. Additional bills have been introduced in 2017, including the Enhancing Detection of Human Trafficking Act, Protecting Young Victims from Sexual Abuse Act and Child Soldier Prevention Act.

The Office of Foreign Assets Control (OFAC) has established country-based sanctions programs that include identifying persons involved in the recruitment and use of child soldiers. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2664. Are there any other anti-human trafficking or migrant smuggling laws that have been enacted at the state or federal level?

Yes. The State of Washington, as an example, enacted an anti-human trafficking statute in 2002, becoming the first state to do so. The California Transparency in Supply Chains Act (CTSC Act) was enacted in January 2012. The CTSC Act requires retailers and manufacturers operating in California with annual revenues of more than US$100 million to disclose their efforts to ensure their supply chains are free of slavery and human trafficking. Other states are expected to follow suit.

According to the Polaris Project, a nonprofit, non-governmental organisation established in 2002 to combat human trafficking, the number of states with basic anti-human trafficking criminal statutes grew from 28 in 2007 to all 50 plus the District of Columbia in 2014.

Other enacted or proposed laws and requirements include:

- Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (PROTECT Act), increased sanctions and/or eliminated statutes of limitations for exploitative acts against children (e.g., murder, sexual abuse, kidnapping, child pornography); increased coordination and support for public outreach efforts (e.g., AMBER Alerts, National Center for Missing and Exploited Children [NCMEC], sex offender apprehension program); and amended existing “truth in domain names” laws prohibiting the use of misleading domain names to deceive a person (e.g., minor) into viewing material considered obscene or harmful to minors.
- Section 1502 of the Dodd-Frank Wall Street Reform and Consumer Protection Act (2010) (Dodd-Frank Act) requires that companies disclose the source of any conflict minerals they use in their products (e.g., minerals mined in conditions of armed conflict and human rights abuses).
- In September 2012, President Barack Obama issued Executive Order 13627 - Strengthening Protections Against Trafficking in Persons in Federal Contracts, mandating that government contractors implement compliance programs throughout the supply chain to prevent human trafficking.
- Section 1702 through 1707 of the National Defense Authorisation Act (NDAA) seeks to end human trafficking in government contracting by amending the TVPA of 2000 to expand the authority of federal agencies to terminate a grant, contract or cooperative agreement involving grantees or contractors who engage in severe forms of trafficking in persons; and requiring certification from grantees and contractors that anti-trafficking procedures have been established; requires reporting

of detected trafficking activities to an appropriate government authority (e.g., agency's inspector general) for further monitoring and investigation.

- The Business Supply Chain Transparency on Trafficking and Slavery Act of 2014, modelled after the conflict mineral rule of the Dodd-Frank Act (2010) and the California Transparency in Supply Chains Act (2012), was introduced in Congress initially in 2011, and again in June 2014 and July 2015. If passed, it would require publicly traded companies with more than US$100 million in global gross receipts to disclose in their annual reports to the U.S. Securities and Exchange Commission (SEC) all measures taken to counter forced labour, human slavery, trafficking and child labour within companies' supply chains (e.g., mitigating policies, audits of suppliers, training of employees and management, responsible labour recruitment practices, remedial actions). Disclosures would be made available to the public on the websites of each company and by the SEC.

2665. What are the key international laws and treaties that address human trafficking and migrant smuggling?

The United Nations' Palermo Protocol addresses human trafficking and migrant smuggling:

- The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children (2000);
- The Protocol against the Smuggling of Migrants by Land, Sea and Air (2000); and
- The Protocol against the Illicit Manufacturing and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime (2001).

The Global Action against Trafficking in Persons and the Smuggling of Migrants (Glo Act) is a joint initiative by the European Union (EU) and the UNODC focused on developing counter-trafficking and counter-smuggling responses in 15 countries across Africa, Asia, Eastern Europe and Latin America. The Glo Act has six key objectives over four years (2015-2019):

- Strategy and policy development;
- Legislative assistance;
- Capacity building;
- Regional and trans-regional cooperation;
- Protection and assistance to victims of trafficking and smuggled migrants; and
- Assistance and support to children among victims of trafficking and smuggled migrants.

2666. What roles can individuals play in a human trafficking and migrant smuggling operation?

According to the United Nations Office on Drugs and Crime (UNODC), a human trafficking operation involves many individuals with multiple roles, including:

- Coordinator or organiser
- Recruiter
- Transporter or guide
- Spotter
- Driver
- Messenger
- Enforcer
- Service provider or supplier

According to EUROPOL, it is also not uncommon for former victims to assume some of these roles as they age.

2667. How are transnational criminal organisations involved with human trafficking and migrant smuggling operations?

Human trafficking and migrant smuggling operations are increasingly being run by organised crime. According to FATF's "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants" (2011), many trafficking and smuggling activities along the U.S.-Mexico border are supervised by the Mexican drug cartel, Los Zetas; in addition, Russian and Albanian gangs and the Italian mafia control a large portion of trafficking in Europe, while Chinese criminal groups and the Japanese Yakuza control trafficking in Asia.

Los Zetas and the Yakuza are designated under the Transnational Criminal Organisations (TCO) Sanctions Program administered by the Office of Foreign Assets Control (OFAC). Los Zetas is also designated under the Counter Narcotics Trafficking Program as a Specially Designated Narcotics Trafficker – Kingpin (SDNTK). Many designees are also listed under other country-based programs for the recruitment and use of child soldiers (e.g., Central African Republic [CAR], South Sudan). A full list of designees under the various OFAC Sanctions Programs can be found on the Specially Designated Nationals and Blocked Persons List (SDN List). For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.

2668. How are fees generated in a human trafficking and migrant smuggling operation?

Fees can be generated through disparate activities with multiple parties during each stage of human trafficking and migrant smuggling: recruitment, transportation and exploitation.

Smugglers often require payment for transportation of individuals across international borders, which generally includes the cost of transportation, bribery and fraudulent immigration documents. According to the International Organisation for Migration (IMO), estimated fees for smuggling vary by country:

- Mexico: US$1,000 – US$3,500
- South America: US$5,000 – US$7,000

- Eastern Europe: US$18,000 – US$25,000
- China: US$40,000 – US$70,000

Payments can be made in advance, partially or upon arrival.

2669. Which countries are at higher risk for human trafficking-related activities?

Various factors contribute to the higher occurrence of human trafficking and migrant smuggling, including but not limited to war, corruption, economic and political instability, natural disasters, high rates of poverty and lack of education, gender discrimination, population pressure, lack of human rights and inadequate legal infrastructure to enforce laws related to human trafficking, smuggling and money laundering.

Victims of human trafficking and migrant smuggling are trafficked from many countries. According to FATF's typology report on human trafficking and migrant smuggling, the most common "sending" regions include:

- The Commonwealth of Independent States (former Soviet Republics)
- Central and Southeast Europe
- Western Africa
- Southeast Asia

The top "receiving" regions include:

- Western Europe
- North America
- Western Asia

Top "transit regions" include:

- Western, Central, Southeast Europe
- Southeast Asia
- Central America
- Western Africa

2670. Which states are at higher risk for human trafficking-related activities?

Statistics for domestic cases of human trafficking at the state level are difficult to obtain since most studies track these activities on a country level and it is generally difficult to identify human trafficking activities. Generally, states with strong tourism and agricultural industries are at higher risk for sex and labour trafficking.

According to the National Human Trafficking Resource Center (NHTRC), the top 5 states with the highest number of reports of potential trafficking cases and victims located within their state in recent years were:

- California
- Texas
- Florida
- Ohio
- New York

According to the Polaris Project Annual State Ratings of July 2014, these five states had strong anti-human trafficking state laws.

2671. What are some examples of human trafficking and smuggling cases?

The United Nations administers a Human Trafficking Case Law Database that provides summaries of cases, including key information, such as:

- Victim information (e.g., nationality, age)
- Defendants
- Form of trafficking
- Purpose of exploitation
- Sector in which exploitation took place
- Charges/claims/decisions
- Commentary

FATF's "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants," published in July 2011, provides details on 15 human trafficking and smuggling case studies. Case studies detail methods of recruitment, retention and exploitation of victims and methods of money transmission and laundering, including, but not limited to, the following:

- Frequent use of money service businesses (MSBs), informal value transfer systems (IVTS) and casinos;
- Commingling of illicit proceeds with funds of legitimate cash-intensive businesses, including takeovers of existing companies;
- Use of front companies, shell companies and straw persons;
- Purchasing of real estate abroad and luxury items (e.g., foreign cars); and
- Use of multiple bank accounts and credit cards in the names of associates and extended family members of traffickers.

FATF's report also provides a list of red flags by industry to assist banks, MSBs, dealers in high-value goods and casinos in detecting potential human trafficking schemes. In addition, the U.S. Immigration and Customs Enforcement (ICE) periodically provides on its website summaries of cases in which they have successfully rescued victims and prosecuted traffickers.

2672. What are the components of an effective anti-human trafficking and anti-migrant smuggling program?

Key components to an effective anti-human trafficking and anti-smuggling program include:

- Implementation and enforcement of victim-friendly laws and regulations with criminal penalties for traffickers and smugglers;
- Monitoring of adherence to existing legislation and activities contributing to human trafficking and migrant smuggling and analysis of successful prosecutions;
- Awareness and training programs for community members and law enforcement;
- Process to identify victims;
- Provision of support services to victims (e.g., protection, transportation, medicine, counselling, shelter, legal assistance);
- Process to reintegrate or voluntarily repatriate victims;
- Prosecution of traffickers and smugglers;
- Forfeiture and confiscation of assets of traffickers and smugglers; and
- Civil actions and monetary restitution for victims.

The president's Executive Order 13627 - Strengthening Protections Against Trafficking in Persons in Federal Contracts, calls for the following:

- Employee awareness program
- Process to report violations without retaliation
- Certification that subcontractors/suppliers have not engaged in human trafficking-related activities (e.g., misleading recruitment, charging recruitment fees, destroying employees' identification documents)

Due to the fragmented and complex system of human trafficking and migrant smuggling, collaboration among community members, service providers and law enforcement, domestically and internationally, is key to developing an effective anti-human trafficking and anti-migrant smuggling program.

2673. What challenges exist to combating human trafficking and migrant smuggling?

Challenges to combating human trafficking and smuggling include, but are not limited to, the following:

- Lack of comprehensive anti-human trafficking and anti-migrant smuggling laws or poor enforcement of existing laws;
- Lack of awareness of existing anti-human trafficking and anti-migrant smuggling laws and perception that human trafficking is a problem limited to a few countries;

- Insufficient training of local law enforcement on indicators for human trafficking and migrant smuggling and identifying and securing key evidence to assist in the successful prosecution of traffickers;
- Lack of cooperation, internationally and among federal, state and local organisations, leading to fragmented investigation processes;
- Lack of comprehensive data due to gaps, discrepancies and inconsistent methodologies in the collection of information on human trafficking and migrant smuggling cases (e.g., victims, traffickers, geographies, profits); and
- Lack of self-identification due to fear and/or shame of victims, particularly those who have been isolated for long periods of time.

Language and cultural barriers and lack of victim cooperation and testimony, often due to fear and distrust, lead to difficulties in prosecuting traffickers.

2674. What key groups have played an important role in the development and implementation of anti-human trafficking and anti-human smuggling standards?

Recognising the international focus on anti-human trafficking and anti-human smuggling, many groups are active in issuing guidance and driving international efforts, including, but not limited to, the following:

- The United Nations (U.N.) issued the Palermo Control, including the Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children; the Protocol against the Smuggling of Migrants by Land, Sea and Air; and the Protocol against the Illicit Manufacturing and Trafficking in Firearms, Their Parts and Components and Ammunition, supplementing the United Nations Convention against Transnational Organised Crime. The United Nations Office on Drugs and Crime (UNODC) also produced "Toolkits to Combat Trafficking in Persons and Smuggling of Migrants" and the "Global Report on Trafficking in Persons," a publication created in 2012 with scheduled updates every two years that provides an overview of human trafficking and the worldwide response at global, regional and national levels.
- The International Labour Office (ILO) holds multiple conventions on forced labour, the abolition of forced labour and child labour. The ILO published Profits and Poverty: The Economics of Forced Labor (2014) and the Data Initiative on Modern Slavery: Better Data for Better Policies (2015).
- The Financial Action Task Force (FATF) issued the typology report "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants" in 2011.
- Other international, regional and sub-regional organisations that have issued laws and guidance for anti-human trafficking and anti-human smuggling include:
    - African Union (AU)
    - Association of Southeast Asian Nations (ASEAN)

- Commonwealth of Independent States (CIS)
- Coordinated Mekong Ministerial Initiative against Trafficking (COMMIT)
- Council of Europe (COE)
- Economic Community of Central African States (ECCAS)
- Economic Community of West African States (ECOWAS)
- League of Arab States (LAS)
- Organisation for Security and Cooperation in Europe (OSCE)
- Organisation of American States (OAS)
- Regional Conference on Migration Plan of Action by the Puebla Group
- South Asian Association for Regional Cooperation (SAARC)
- Southern African Development Community (SADC)

For an extensive list of organisations and their anti-human trafficking efforts, please refer to Annex E of FATF's "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants."

Within the United States, the federal response to combating human trafficking involves multiple federal agencies tasked with the following key responsibilities:

- The **President's Interagency Task Force to Monitor and Combat Trafficking** (PITF) – Coordinate federal efforts to combat human trafficking.
- **U.S. Department of State** (DOS) – Coordinate international anti-human trafficking programs and efforts.
- **U.S. Department of Health and Human Services** (HHS) – Identify, certify and assist victims of human trafficking.
- **U.S. Department of Justice** (DOJ) – Investigate cases of human trafficking and prosecute traffickers. The Human Trafficking Prosecution Unit (HTPU), created in 2007 by the Civil Rights Division, partners with the Assistant United States Attorneys (AUSAs) to coordinate expertise on human trafficking investigations and prosecutions. The DOJ funds more than 40 Human Trafficking Task Forces to coordinate federal, state and local law enforcement anti-human trafficking efforts.
- **U.S. Department of Defense** (DOD) – As one of the largest buyers in the world, ensure that the U.S. military, its civilian employees and its contractors are aware of and adopt a zero-tolerance policy on human trafficking within its organisation and supply chain.
- **U.S. Department of Homeland Security** (DHS) (U.S. Immigration and Customs Enforcement [ICE], U.S. Customs and Border Protection [CBP], U.S. Citizenship and Immigration Services [USCIS]) – Raise awareness, identify and protect victims, grant immigration relief to victims, disrupt human trafficking rings and investigate cases of human trafficking.

- **U.S. Department of Labor** (DOL) – Detect exploitative labour practices and provide assistance to victims of human trafficking, including job search, education and training services, transportation, childcare and housing.
- **U.S. Department of Agriculture** (USDA) – Reduce the likelihood that agricultural products produced with the use of child or forced labour are imported into the United States.
- **U.S. Department of Education** (ED) – Raise awareness to prevent human trafficking and increase victim identification of trafficked children in schools.
- **U.S. Agency for International Development** (USAID) – Fund international programs that prevent trafficking, protect and assist victims, and support prosecutions through training for police and criminal justice personnel.
- **U.S. Equal Employment Opportunity Commission** (EEOC) – Identify labour trafficking cases in addition to discriminatory cases based on race, colour, national origin, sex, religion, age, disability and genetic information.
- **U.S. Department of the Treasury** – The Financial Crimes and Enforcement Network (FinCEN), the U.S. financial intelligence unit (FIU), within the Treasury Department, has a mission to safeguard the financial system from abuses of financial crime. In 2014, FinCEN published "**Guidance on Recognising Activity that May be Associated with Human Smuggling and Human Trafficking**" providing basic definitions and red flags for human trafficking and smuggling.

Some key initiatives by the U.S. federal government include, but are not limited to, the following:

- Together with the Office of Refugee Settlement (ORS), the HHS established the **Anti-Trafficking in Persons** (ATIP) program, which supports the following initiatives:
  - **Victim Identification and Public Awareness** through the "Rescue and Restore" campaigns, which establish state, local and regional coalitions composed of non-government organisations, law enforcement and other community members to address the problem of human trafficking.
  - **Assistance for Victims of Human Trafficking** through certification and eligibility letters that identify and verify victims of human trafficking who are eligible for federal benefits and services; service grants through the National Human Trafficking Victim Assistance Program; and the National Human Trafficking Resource Center (NHTRC), a national hotline that offers resources and tools for victims as well as service providers and community members who are attempting to identify and prevent human trafficking and assist victims of this crime.
- The **Office to Monitor and Combat Trafficking in Persons** (J/TIP) within the U.S. Department of State issues an annual "**Trafficking in Persons Report**" (TIP Report), similar to the Financial Action Task Force (FATF) Mutual Evaluation Reports (MERs), that evaluates each country on its compliance with the minimum standards of the Trafficking Victims Protection Act (TVPA). Countries are monitored for progress in adhering to TVPA minimum standards based on

a "3P" paradigm: prosecution, protection and prevention. Topics covered in the most recent TIP (2014), included vulnerable and marginalised communities (e.g., lesbian, gay, bisexual and transgender [LGBT] individuals, indigenous persons, child soldiers), methods of coercion (e.g., use of forced criminality) and opportunities and reasons for exploitation (e.g., major sporting events, demand for organs). Additional publications issued by J/TIP include, numerous Fact Sheets covering topics including but not limited to, the following:

  - Identifying common victims and at-risk populations (e.g., children, Lesbian, Gay, Bisexual, Transgender [LGBT], Indigenous Persons, people fleeing conflict zones);
  - Common practices of human traffickers (e.g., forced criminality, high-risk industries);
  - Common misperceptions of human trafficking;
  - Non-criminalisation and protection of victims;
  - Methods to prevent human trafficking (e.g., public awareness and outreach, overcoming harmful cultural norms, international efforts, media best practices).

- Within the U.S. Department of State, the **Human Smuggling and Trafficking Center** (HSTC) gathers information on illicit travel, including that of trafficking, and coordinates with foreign agencies and diplomats to monitor and fight trafficking on an international basis.
- The Bureau of Justice Assistance (BJA) and the Office for Victims of Crime (OVC) within the DOJ funds the establishment of **Anti-Human Trafficking Task Forces** and released an "**Anti-Human Trafficking Task Force Strategy and Operations e-Guide**." The DOJ issues periodic Bureau of Justice Statistics (BJS) reports titled "**Characteristics of Suspected Human Trafficking Incidents,**" which summarise data captured in the **Human Trafficking Reporting System** (HTRS) based on information collected from local and federal law enforcement cases involving human trafficking within the United States. Additionally, the DOJ also produces the "**Attorney General's Annual Report to Congress on U.S. Government Activities to Combat Trafficking in Persons**."
- The U.S. Department of Labor's "**List of Goods Produced by Child Labor or Forced Labor**" cites goods from countries that the agency believes are produced by child or forced labour in violation of international standards.
- Together with the Federal Law Enforcement Training Center (FLETC), the DHS developed web-based human trafficking training modules under the "**Blue Campaign**" to teach law enforcement how to recognise human trafficking, protect victims and initiate human trafficking investigations. The DHS also initiated Project STAMP (Smugglers' and Traffickers' Assets, Monies and Proceeds), an effort to attack and seize the assets of human trafficking organisations and identify and disseminate typologies and red flags related to money laundering by these organisations.
- The U.S. Department of Agriculture established the **"Consultative Group to Eliminate the Use of Child Labor and Forced Labor in Imported Agricultural Products**," representing government, private sector, academic and non-government entities charged with developing

recommendations to reduce the likelihood of importing agricultural products produced with the use of child or forced labour.

The Polaris Project is a nonprofit, non-governmental organisation established in 2002 to combat human trafficking. It has been involved in the following initiatives:

- Administration of the **National Human Trafficking Resource Center** (NHTRC) in partnership with the Office of Refugee Settlement (ORS).
- Founding member of the **Alliance to End Slavery and Trafficking** (ATEST), launched by Humanity United, to strengthen U.S. laws and federal resources to fight human trafficking.
- Administration of the Polaris Project Annual State Ratings, an annual assessment of state trafficking legislation in the United States.

Examples of other organisations involved in anti-human trafficking and anti-smuggling efforts include the following:

- **The Nexus Institute** is an independent international human rights research and policy center.
- **Safe Horizon** is a victim assistance organisation that provides services to victims and families affected by crime and abuse, including, but not limited to, child abuse, domestic violence and human trafficking.
- **The Global Alliance Against Traffic in Women** is an alliance of more than 100 non-governmental organisations founded to promote the rights of women migrant workers and trafficked persons.
- **The Pillars of Hope: Attorneys General Unite Against Human Trafficking** is an initiative by the National Association of Attorneys General focused on nationwide efforts to fight labour and sex trafficking.
- **The Human Trafficking Clinic** at the University of Michigan Law School is a clinical law program committed to advancing anti-human trafficking policy through interdisciplinary collaboration at the local, national and international levels.

Impact on Financial Institutions

2675. What obligations do financial institutions have related to human trafficking and migrant smuggling?

Financial institutions have an obligation to identify and report potential cases of human trafficking and smuggling of their customers through routine suspicious activity monitoring processes. In addition, financial institutions may be subject to other requirements that require them to ensure their supply chains are free of human trafficking and smuggling activities.

In September 2014, FinCEN issued Guidance on Recognising Activity that May be Associated with Human Smuggling and Human Trafficking – Financial Red Flags to assist financial institutions detect and report activities related to human trafficking and migrant smuggling.

2676. How do the FATF Recommendations address human trafficking and migrant smuggling?

The FATF Recommendations includes "trafficking in human beings and migrant smuggling" as a designated category of offense for money laundering. In 2011, FATF issued the typology report "Money Laundering Risks Arising from Trafficking in Human Beings and Smuggling of Migrants."

For further guidance on international AML/CFT standards, please refer to the Financial Action Task Force section.

2677. What other resources can a financial institution use to assess country risk related to human trafficking?

The Office to Monitor and Combat Trafficking in Persons within the U.S. State Department issues an annual "Trafficking in Persons Report" (TIP Report), similar to the Financial Action Task Force (FATF) Mutual Evaluation Reports (MERs), that evaluates each country on its compliance with the minimum standards of the Trafficking Victims Protection Act (TVPA) based on the following:

- Enactment and implementation of anti-human trafficking laws
- Criminal penalties for trafficking offenses
- Victim identification measures
- Victim protection and assistance efforts (e.g., legal assistance, primary healthcare, counselling, shelter)
- Victim repatriation and/or reintegration efforts

Each country is assigned a ranking of one of four tiers:

- Tier One: Fully compliant
- Tier Two: Partially compliant with progress in areas of noncompliance
- Tier Two Watch List: Partial compliance but significant occurrences of human trafficking violations continue to exist or there is a lack of evidence on progress in areas of noncompliance
- Tier Three: Noncompliant with lack of evidence of efforts to progress in areas of noncompliance

Of the nearly 190 countries evaluated by the U.S. State Department in 2016, approximately 19 percent were fully compliant with minimum standards for anti-human trafficking, 41 percent were partially compliant, 23 percent were placed on watch and 14 percent were noncompliant. Noncompliant countries included the following:

- Algeria
- Belarus
- Belize
- Burma
- Burundi
- Central African Republic
- Comoros
- Djibouti
- Equatorial Guinea
- Eritrea
- The Gambia
- Guinea-Bissau
- Haiti
- Iran
- North Korea
- Marshall Islands
- Mauritania
- Papua New Guinea
- Russia
- South Sudan
- Sudan
- Suriname
- Syria
- Turkmenistan
- Uzbekistan
- Venezuela
- Zimbabwe

Libya, Somalia and Yemen were not rated but listed as "special cases" due to incomplete or inadequate reporting because of instability in the region.

Financial institutions can consider utilising these tiered rankings as part of their risk assessment methodology. For additional guidance on risk assessments, please refer to the Customer Risk Assessment and Geographic Risk Assessment sections.

2678. Are there penalties for noncompliance with human trafficking and migrant smuggling laws?

Yes. Governments of countries that receive a Tier Three ranking by the U.S. State Department may be subject to certain sanctions, including, but not limited to:

- The withholding or withdrawal of non-humanitarian, non-trade-related foreign assistance;
- Withholding of funding for government employees' participation in educational and cultural exchange programs; or
- Withdrawal of support to receive assistance from international financial institutions (e.g., International Monetary Fund [IMF], World Bank [WB]).

2679. What resources can a financial institution use to assess domestic risk as it relates to human trafficking?

From 2011 to 2014, the Polaris Project released a state ratings map that assessed the strengths of human trafficking laws based on the following 10 categories:

- Sex trafficking provision
- Labor trafficking provision
- Asset forfeiture and/or investigative tools for law enforcement
- Training requirement and/or human trafficking task force
- Posting a human trafficking hotline
- Safe harbour: protecting trafficked minors
- Lower burden of proof for sex trafficking of minors
- Victim assistance
- Access to civil damages
- Vacating convictions for sex trafficking victims

States were assigned a ranking of one of four tiers:

- Tier One: Highest ranking indicating state has passed significant anti-human trafficking laws
- Tier Two: State has passed numerous anti-human trafficking laws but needs to improve and implement its laws
- Tier Three: State has made nominal efforts to pass anti-human trafficking laws
- Tier Four: State has not made minimal efforts to pass anti-human trafficking laws

The Polaris Project Annual State Ratings reported the following results of its assessment in July 2014:

- Tier One: 39 states, an increase of 18 states since 2012
- Tier Two: 9 states and Washington, D.C.
- Tier Three: 2 states (North Dakota and South Dakota)
- Tier Four: 0 states

Financial institutions can consider utilising these results and tiered ranking methodology as part of their risk assessment methodology. For additional guidance on risk assessments, please refer to the Customer Risk Assessment and Geographic Risk Assessment sections.

2680. Which types of businesses are considered potentially high risk for human trafficking and migrant smuggling?

Certain types of businesses are more easily used and abused by human traffickers and smugglers. Such businesses include those that are cash-intensive, lack transparency, involve international transactions/customers, require seasonal labour, and have less stringent regulatory requirements.

The Polaris Project distinguishes "perpetrators" from "facilitators" of human trafficking. Some of these businesses are directly involved in human trafficking, while others knowingly or unknowingly facilitate human trafficking by providing advertising, transportation, financial services and spaces to operate.

High-risk businesses and industries include, but are not limited to, the following:

- Adult film industry
- Advertisers (e.g., online websites, phone books, newspapers)
- Agriculture and farms
- Attorneys (e.g., immigration)
- Beauty salons (e.g., hair, nail)
- Brothels and prostitution rings
- Car washes
- Domestic work service providers (e.g., cleaning and janitorial services)
- Diplomats or government officials
- Escort service providers
- Factories
- Fishing
- Hostess and strip clubs
- Hotel and hospitality services
- Import/export companies
- Labor brokers
- Landlords
- Logging
- Manufacturers (e.g., textile)
- Massage parlours
- Mining

- Non-banking financial institutions (e.g., currency exchange houses, money transmitters, check cashing facilities) and informal value transfer systems (IVTS) (e.g., hawala, hundi, fei ch'ien, black market peso exchange [BMPE])
- Recruitment agencies (e.g., for domestic employment and education opportunities targeting foreign persons)
- Restaurants
- Sales crews (e.g., peddling and begging rings)
- Shelters (e.g., homeless, domestic violence, child abuse)
- Ship, bus or plane operators
- Taxi services
- Travel agencies
- Truck stops

Executive Order 13627 – Strengthening Protections Against Trafficking in Persons in Federal Contracts, directs federal agencies to establish processes to identify industries and sectors with a history of human trafficking.

For additional guidance on high-risk customers, please refer to the sections: Customer Risk Assessment and Know Your Customer Types.

2681. What are some common red flags for suspicious activity related to human trafficking and migrant smuggling?

Red flags that can be used by financial institutions to better identify and report potentially suspicious activity related to human trafficking and migrant smuggling include, but are not limited to, the following:

- Customer with an excessive number of individual accounts
- Customer who conducts transactions on behalf of customers whose accounts were recently closed due to suspicious activity
- Customer's telephone numbers linked to personal advertisements for potentially illicit activity (e.g., escort services) that have been verified through public sources
- Customer's address linked to residence and/or hotel with suspected ties to trafficking (e.g., named in previous investigations and busts, offer hourly rates)
- A common mobile number, address and/or employment references that are used to open multiple accounts under different names
- Households with an unusually high number of residents who also appear unrelated, but share accounts, addresses and mobile numbers
- Accounts opened in the name of unqualified minors, foreign workers or foreign students

- Accounts opened by an employer or recruitment agency on behalf of foreign workers and students (e.g., custodial arrangement)
- Accounts reported for identity theft
- Accounts opened with fraudulent or missing/incomplete documentation
- Accounts lacking commercial activity (e.g., payroll taxes) or activity inconsistent with the stated nature of business/expected activity
- Account activity beyond the living standard of the account holder
- Account activity conducted by a third party (e.g., employer) who always accompanies the account holder (may direct the transaction, possess the identification of the account holder and act as an interpreter)
- Account activity with beneficiaries/originators in high-risk countries known for human trafficking or with significant migrant populations (e.g., El Salvador, Guatemala, Honduras, Mexico) or along the southwest border of the United States
- High number of cash deposits structured to avoid reporting requirements
- Cash deposits into one account from multiple locations throughout all states, often followed by multiple wire transfers to high-risk countries (also known as funnel accounts)
- Frequent deposits and withdrawals from multiple branches and ATMs
- Frequent use of cash couriers
- Frequent exchanges of small dollar denominations for large dollar denominations by customers involved in non-cash intensive businesses
- Frequent transfers to common recipients often in high-risk countries; often under the US$3,000 reporting threshold
- Frequent transfers or checks payable to casinos or money transmitters
- Frequent small-dollar international funds transfers for “repayment of debt”
- Frequent deposits of payroll checks from multiple parties, seemingly unrelated
- Frequent payments for rent, hotels, rental cars, airline tickets or other travel-related accommodations
- Repeat payments to advertisers (e.g., websites, newspapers) that promote the sex industry (e.g., escort services)
- Frequent payments to unlicensed or noncompliant recruitment agencies (e.g., employment, students) with a history of labour violations
- Bill payments using money orders as opposed to paying with personal checks
- High volume of payments for multiple mobile phones

- High volume of payments for large food purchases
- High volume of deposits of government benefits for multiple beneficiaries followed immediately by cash withdrawals
- Purchases of luxury items or assets in high-risk countries

The fragmented and complex system of human trafficking and migrant smuggling contributes to the difficulty in detecting potentially suspicious financial transactions related to human trafficking. Data mining may be a more effective method of detecting these types of activities than traditional suspicious transaction monitoring.

For additional examples of red flags, please refer to the Suspicious Activity Red Flags section.

2682. What phrases should financial institutions include in their SAR narratives when reporting suspicious activities related to human trafficking and migrant smuggling?

Financial institutions should include the phrase "Advisory Human Trafficking" or "Advisory Human Smuggling" within the narrative of SARs when reporting suspicious transactions that include suspicious activities related to human trafficking and migrant smuggling.

The phrases enable FinCEN to identify and report on trends in SAR filings related to these criminal activities.

In February 2017, FinCEN, among other technical updates, proposed adding a field to identify human trafficking/migrant smuggling in SARs. For further guidance, please refer to the Suspicious Activity Reports section.

2683. Are there instances in which a financial institution should notify law enforcement in advance of filing a SAR?

Whenever a violation is ongoing, financial institutions should immediately notify law enforcement, even before the SAR is filed.

U.S. Immigration and Customs Enforcement (ICE) has established a hotline at 1.866.DHS.2ICE to report instances of suspected human trafficking and migrant smuggling.

2684. Does notifying law enforcement of suspicious activity serve as a replacement or in any way relieve a financial institution's obligation to file a SAR?

No. Notifying law enforcement does not remove or in any way affect a financial institution's obligation to file a SAR if it detects suspicious activity.

For additional guidance on the reporting of potentially suspicious activity, please refer to the Suspicious Activity Reports section.

Illegal Internet Gambling and Fantasy Sports Wagering

Basics

2685. How is a "bet or wager" defined?

The Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA) defines a "bet or wager" as follows:

- "The staking or risking by any person of something of value upon the outcome of a contest of others, a sporting event, or a game subject to chance, upon an agreement or understanding that the person or another person will receive something of value in the event of a certain outcome;
- Includes the purchase of a chance or opportunity to win a lottery or other prize (which opportunity to win is predominantly subject to chance);
- Includes any scheme of a type described in Section 3702 of Title 28 [Professional and Amateur Sports Protection Act (PASPA) (1992)]; and
- Includes any instructions or information pertaining to the establishment or movement of funds by the bettor or customer in, to, or from an account with the business of betting or wagering."

2686. What is internet gambling?

Simply put, internet gambling is the online wagering of money or other value. Other terms used include online gambling and the more comprehensive term, remote gambling, which includes gambling through the use of remote communications such as the internet, smartphone, telephone, radio and television. Much of the legislation on gambling was enacted prior to the invention of the internet.

In the United States, there is no common definition of internet gambling, so the legality or illegality of some activities must be determined based on the particular facts. Examples of activities considered as a type of internet gambling include, but are not limited to, the following:

- Online poker;
- Internet lottery; and
- Simulated gambling in virtual multiplayer online games (MMOGs).

2687. What is "sports betting" and "fantasy sports wagering"? Are they illegal?

Sports betting is generally defined as placing a bet or wager on the outcome of an actual sporting event. The federal law PASPA made land-based or live-action sports betting illegal with exceptions for grandfathered states.

Fantasy sports wagering is generally defined as placing a bet or wager on the outcome of a simulated sporting event based on virtual teams created by various participants. While some may consider fantasy sports wagering an illegal form of internet gambling, the activity has been granted an exception by federal laws. For further guidance, please refer to the Fantasy Sports Wagering section.

2688. How big is the U.S. internet gambling market?

Internet gambling, including online betting and internet lotteries, could generate US$4 billion in revenues in the United States by 2020 according to Technavio, a market research company.

2689. Since various forms of gambling are permitted in the United States, why is internet gambling a concern?

Those concerned about internet gambling cite the following reasons:

- Potential for fraud, such as identity theft, over the internet
- Children's access to gambling sites
- 24/7 access, which facilitates "problem gambling"
- Money laundering and terrorist financing risks

2690. What is "problem gambling" and "responsible gambling"?

The Diagnostic and Statistical Manual of Mental Disorders (DSM) defines "problem gambling" as an individual exhibiting four or more of the following:

- Preoccupied with gambling
- Unable to cut back or control
- Irritable or restless when attempting to cut down or stop gambling
- Risks more money to reach desired level of excitement
- Gambles to escape problems or depressed mood
- "Chases" losses
- Lies to family and others about gambling
- Risks or loses relationships or job because of gambling
- Relies on others for financial needs caused by gambling

Responsible gambling generally refers to the enablement of a fair and safe gaming experience. For example, the National Council on Problem Gambling (NCPG) published the Consumer Protection, Age & Identity Verification, Responsible Play Guidelines and Exclusion (CARE) Amendments for Fantasy Sports Legislation that includes guidelines for the following:

- **Consumer Protection** (e.g., resources on problem gambling, restrictions on advertisements);
- **Age and Identity Verification** (e.g., verification that participants are of legal age);
- **Responsible Play Guidelines** (e.g., game instructions, tips on safe spending and time limits); and
- **Exclusion** (e.g., self-exclusion initiated by the customer).

2691. What is "third-party betting"?

The Financial Crimes Enforcement Network (FinCEN) issued guidance in 2014 defining "third-party betting" as "using intermediaries to place bets on behalf of unidentified third parties." FinCEN advised casinos and card clubs currently subject to AML/CFT laws and regulations to inquire if patrons are betting on behalf of third-parties, similar to guidance on the proper filing of Currency Transaction Reports (CTRs) (e.g., inquiring if reportable currency transactions are conducted by or on behalf of a third party). Third-party betting could be abused to disguise underlying third-parties or obscure the source of funds used to bet.

For additional guidance on CTRs, please refer to the Currency Transaction Reports section. For further guidance on the AML/CFT requirements for casinos, please refer to the Casino and Card Clubs section.

2692. What U.S. laws address internet gambling?

On a federal level, the Interstate Wire Act of 1961 (Wire Act), also referred to as the Federal Wire Act, prohibits the use of a wire communication facility (e.g., internet) for the transmission of sports bets or wagers or information assisting in the placement of such bets or wagers. However, in 2011, the U.S. Department of Justice indicated that the scope of the Wire Act's prohibition was limited to sports betting.

The Professional and Amateur Sports Protection Act of 1992 (PASPA), also known as the Bradley Act, prohibits sports wagering in all states except those with pre-existing operations (i.e., Delaware, Montana, Nevada, Oregon). Some states have enacted laws that specifically prohibit certain internet gambling activities.

Broader key gambling regulations and statutory provisions include, but are not limited to, the following:

- The Travel Act of 1961
- Interstate Transportation of Wagering Paraphernalia Act of 1961
- Illegal Gambling Business Act of 1970
- Racketeer Influenced and Corrupt Organisations Act of 1970 (RICO)
- The Indian Gaming Regulatory Act of 1988 (IGRA)
- Interstate Wagering Amendment of 1994
- Amendment to Interstate Horseracing Act
- Illegal Money Transmitting Business Act of 1992
- Gambling Ship Act
- Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA).

2693. Have any U.S. states legalised internet gambling?

While the United States has enacted federal legislation to prohibit "unlawful Internet gambling," the U.S. Department of Justice indicated in a 2011 ruling that, with exception to sports wagering, individual states have the authority to determine whether to legalise intrastate online gambling.

Delaware, Nevada and New Jersey became the first states to legalise certain forms of internet gambling. A number of states have since begun the process of attempting to legalise online gambling, including, but not limited to, California, Illinois, Mississippi, New York, Pennsylvania and Texas.

State lawmakers face a number of obstacles in attempting to pass legislation, including the potential difficulties in enforcing and monitoring appropriate compliance with online gambling regulations as well as possible interference with gambling conducted across state borders with varying legalities.

2694. What key guidance and resources have been provided related to internet gambling and fantasy sports?

The following key guidance and resources have been provided related to internet gambling and fantasy sports:

- **Report to Congressional Requesters: Internet Gambling: An Overview of the Issues** (2002) by the United States General Accounting Office (GAO)
- **Internet Gambling: An Emerging Field of Research** (2013) by the National Center for Responsible Gambling (NCRG)
- Founded in 1972 as a national advocate for problem gamblers and their families, the **National Council on Problem Gambling (NCPG)** has published key resources including, but not limited to, the following:
    - Internet Responsible Gambling Standards (2012)
    - U.S. Online Responsible Gaming Regulations: Delaware, Nevada and New Jersey (2014)
    - Fantasy Sports Consumer Protection Guidelines (2015)
    - Responsible Gaming Verification (RGV) Program for Lottery Organisations (2016) (jointly with the North American State and Provincial Lotteries [NASPL])
    - Consumer Protection, Age & Identity Verification, Responsible Play Guidelines and Exclusion (CARE) Amendments for Fantasy Sports Legislation
    - Internet Compliance Assessment Program (ICAP)
- Founded in 1998, the **Fantasy Sports Trade Association (FSTA)** provides resources for its members that includes, but is not limited to, the following:
    - Resource Center
        - Demographic Research
        - Market Size Research

        - Lawsuits, Laws, Briefs, Rulings
        - Newsletters
        - Webinars
    - State Regulations
    - State Monitoring

For additional guidance related to casinos and card clubs, please refer to the Casinos and Card Clubs section.

Unlawful internet Gambling Enforcement Act

2695. How is "unlawful Internet gambling" defined under the UIGEA?

Under the U.S. Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA), unlawful internet gambling includes placing, receiving or otherwise knowingly transmitting a bet or wager by any means that involves the use, at least in part, of the internet, where such bet or wager is unlawful under any applicable federal or state law in the state or tribal land in which the bet or wager is initiated, received or otherwise made.

The term does not include certain bets or wagers that are excluded under the UIGEA as an intrastate transaction or an intra-tribal transaction, and does not include any activity that is allowed under the Interstate Horseracing Act of 1928. The intermediate routing of electronic data does not determine the location or locations in which a bet or wager is initiated, received or otherwise made.

The UIGEA requirement is implemented under regulation 12 C.F.R. 233 – Prohibition on Funding of Unlawful Internet Gambling (Regulation GG).

2696. Are there any exemptions to "unlawful Internet gambling" under the UIGEA?

The UIGEA exempts participation in any game or contest in which participants do not stake or risk anything of value other than personal efforts of the participants in playing the game or contest or obtaining access to the internet, or points or credits that the sponsor of the game or contest provides to participants free of charge and that can be used or redeemed only for participation in games or contests offered by the sponsor.

The UIGEA also exempts participation in any fantasy or simulation sports game or educational game or contest in which (if the game or contest involves a team or teams) no fantasy or simulation sports team is based on current membership of an actual team that is a member of an amateur or professional sports organisation and meets each of the following conditions:

- All prizes and awards offered to winning participants are established and made known to the participants in advance of the game or contest and their value is not determined by the number of participants or the amount of any fees paid by those participants;

- All winning outcomes reflect the relative knowledge and skill of the participants and are determined predominantly by accumulated statistical results of the performance of individuals (athletes in the case of sports events) in multiple real-world sporting or other events; and
- No winning outcome is based on the score, point spread or any performance(s) of any single real-world team or any combination of teams, or solely on any single performance of an individual athlete in any single real-world sporting or other event.

The law also exempts the following:

- Deposits or transactions with insured depository institutions
- Contracts for insurance, indemnity or guarantee
- Certain other transactions governed by securities or commodity laws

2697. How does the UIGEA aim to prevent illegal internet gambling?

The UIGEA of 2006 made it a criminal offense for persons engaged in the business of betting or wagering to knowingly accept payments in connection with the participation of another person in unlawful internet gambling. It required the U.S. Treasury Department and the Federal Reserve Board to promulgate regulations requiring certain participants in the payment systems and financial transaction providers participating in such systems to have policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions.

Since the UIGEA was enacted in October 2006, and the U.S. Treasury Department and Federal Reserve Board published a proposed rule in October 2007 and a final rule in November 2008, the effective date for compliance for designated participants within specified payment systems was deferred until June 1, 2010, under the Prohibition on Funding of Unlawful Internet Gambling (Regulation GG).

2698. What is the relationship of the UIGEA to the AML/CFT compliance?

UIGEA compliance is separate and distinct from AML/CFT compliance, though customer due diligence (CDD) is a tenet of both. Compliance with the UIGEA does not fulfil any other AML/CFT requirement, such as the requirement to file SARs. For further guidance on AML/CFT requirements, please refer to the sections: Bank Secrecy Act, the USA PATRIOT Act and Casinos and Card Clubs.

2699. Which payment system participants are required to have policies and procedures to prohibit the processing of prohibited transactions?

Under the joint rule issued by the U.S. Treasury Department and the Federal Reserve Board, Regulation GG, the following payment systems are designated participants:

- **Automated clearing house (ACH) systems**. However, the participants processing a particular transaction through an automated clearing house system are exempt from the Act's requirements for establishing written policies and procedures, except for:

  - The receiving depository financial institution and any third-party processor receiving the transaction on behalf of the receiver in an ACH credit transaction;
  - The originating depository financial institution and any third-party processor initiating the transaction on behalf of the originator in an ACH debit transaction; and
  - The receiving gateway operator and any third-party processor that receives instructions for an ACH debit transaction directly from a foreign sender (which could include a foreign banking office, a foreign third-party processor, or a foreign originating gateway operator).

- **Card systems**, which are defined as a system for authorising, clearing and settling transactions in which credit cards, debit cards, prepaid cards or stored-value cards (such cards being issued or authorised by the operator of the system) are used to purchase goods or services or to obtain a cash advance. The term includes systems both in which the merchant acquirer, card issuer and system operator are separate entities and in which more than one of these roles are performed by the same entity.
- **Check collection systems**. However, the participants in a particular check collection transaction through a check collection system are exempt from the Act's requirements for establishing written policies and procedures, except for the depository bank.
- **Money transmitting businesses**, solely to the extent they: (1) engage in the transmission of funds, which does not include check cashing, currency exchange, or the issuance or redemption of money orders, traveller's checks and other similar instruments; and (2) permit customers to initiate transmission of funds transactions remotely from a location other than a physical office of the money transmitting business. The participants in a money transmitting business are exempt from the Act's requirement to establish written policies and procedures, except for the operator.
- **Wire transfer systems**. However, the participants in a particular wire transfer through such a system are exempt from the Act's requirement to establish written policies and procedures, except for the beneficiary bank.

These designated participants in the aforementioned payment systems are collectively referred to herein as "covered participants." For additional guidance on payment processors, please refer to the Third-Party Payment Processors section.

2700. Do casinos and card clubs have additional obligations to comply with the UIGEA?

No. While casinos and card clubs may pose a higher risk for processing prohibited transactions due to the nature of their business, like any other financial institution or payment processor, they will have to evaluate their business lines for risk and establish appropriate internal controls to mitigate those risks in accordance with UIGEA.

For additional guidance on the AML/CFT requirements of casinos, please refer to the Casinos and Card Clubs section.

2701. Are any covered participants exempt from the requirement to have policies and procedures?

Yes, as detailed above, certain types of participants are exempt from establishing written policies and procedures, depending on their roles in the processing of transactions.

2702. Are customers of covered participants also subject to Regulation GG?

No. Regulation GG imposes the obligations to establish and implement written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions on non-exempt participants in designated payment systems, not the customers of designated participants.

However, UIGEA prohibits any person engaged in the business of betting or wagering from knowingly accepting payments in connection with the participation of another person in unlawful internet gambling. Other federal and state laws prohibiting illegal internet gambling can apply directly to customers, and other parties to the transaction.

2703. What types of policies and procedures does Regulation GG require covered payment systems participants to develop and maintain?

Under Regulation GG, the implementing regulation to the Act, participants are required to develop and maintain written policies and procedures reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions. They may be customised to their businesses, and it is likely such policies and procedures may differ across different business lines. The focus of the policies and procedures is intended to be on the due diligence that financial institutions and third-party payment processors should conduct when deciding to establish and maintain commercial customer accounts.

A covered participant can be considered to be in compliance with the requirement to have such policies and procedures if it relies on and complies with the written policies and procedures of the designated payment system that are reasonably designed to identify and block restricted transactions, or otherwise prevent or prohibit the acceptance of the products or services of the designated payment system or participant in connection with restricted transactions, and such policies and procedures of the designated payment system comply with the law's requirements.

A covered party's procedures will meet the standard of being reasonably designed if they include:

- Specified due diligence of its commercial customer accounts or commercial customer relationships including, but not limited to, the conducting of due diligence of a commercial customer and its activities at the time of establishment of the account or relationship commensurate with the participant's judgment of the risk of restricted transactions presented by the customer's business;
- Specified notice be given to all commercial customers;
- The participant (on the basis of its due diligence) is able to make a determination that the customer presents a minimal risk of engaging in an internet gambling business; or
- If it is not able to reach such a determination through its due diligence, it obtains specified documentation, such as evidence of legal authority to engage in such business.

2704. What are card systems expected to do?

The policies and procedures of a card system operator, a merchant acquirer, third-party processor or a card issuer are deemed to be reasonably designed to identify and block or otherwise prevent or prohibit restricted transactions if the policies and procedures provide for specified methods to conduct due diligence or implement a code system (e.g., transaction codes and merchant/business category codes) that are required to accompany the authorisation request for a transaction (that must include specified functionality).

Additionally, the card system operator, merchant acquirer or third-party processor needs to have procedures to be followed when the participant has actual knowledge that a merchant has received restricted transactions through the card system, including but not limited to:

- Circumstances under which the merchant account should be closed; and
- Circumstances under which the access to the card system for the merchant, merchant acquirer or third-party processor should be denied.

2705. What are sufficient policies for money transmitters?

Money transmitters have reasonably designed policies and procedures if they:

- Address methods for the operator to conduct due diligence in established commercial customer relationships as set forth in the regulations;
- Address due diligence methods to be used where there is actual knowledge that an existing commercial customer engages in an internet gambling business (as set forth in the regulations);
- Include procedures regarding ongoing monitoring or testing by the operator to detect potential restricted transactions, such as monitoring and analysing payment patterns to detect suspicious payment volumes to any recipient; and
- Include procedures to be followed when the operator has actual knowledge that a commercial customer of the operator has received restricted transactions through the money transmitting business, that address the circumstances under which the money transmitting services should be denied to the commercial customer and the circumstances under which the account should be closed.

2706. What types of policies and procedures does Regulation GG expect covered participants to develop and implement?

Regulation GG contemplates that covered participants will develop and maintain policies and procedures addressing the following:

- Notices to new and existing commercial account holders that restricted transactions are prohibited from being processed through the account or relationship.
- Due diligence procedures designed to determine the following:
    - Whether a commercial customer poses minimal risk.

- In the event the participant is unable to determine that the commercial customer poses only minimal risk, the financial institution must require:
    - A certification from the customer stating that it does not engage in internet gambling or, if it does, a commercial license from a state or tribal authority authorising the customer to engage in the business or a reasoned legal opinion (as defined in the regulation) that such activity does not involve restricted transactions;
    - A written commitment to report any change in its legal authority to engage in internet gambling; and
    - A third-party certification that the customer's systems for engaging in internet gambling are reasonably designed to ensure the customer will remain within legal limits.

2707. What if a covered participant has actual knowledge that a commercial customer is engaging in internet gambling?

If a covered participant has actual knowledge that a commercial customer is engaging in internet gambling, then the participant should obtain the documentation outlined in its policies and procedures:

- Evidence of legal authority to engage in such business (e.g., commercial license);
- Legal opinion that such activity does not involve restricted transactions;
- Written commitment to report any change in its legal authority; or
- Third-party certification that the customer's systems for engaging in internet gambling are reasonably designed to ensure the customer will remain within legal limits.

The purpose of obtaining this documentation is to assist the covered participant in distinguishing between customers who engage in internet gambling and those who conduct restricted transactions in violation of the UIGEA.

2708. What if a covered participant has actual knowledge that a commercial customer is conducting restricted transactions?

Where it has knowledge that the commercial customer is conducting restricted transactions, covered participants are expected to have policies and procedures to address the following:

- Continued transaction processing;
- Account review;
- Suspicious activity report (SAR) filing; and
- Account closure.

2709. Since most covered participants are not expected to collect information proactively to identify restricted activities, how would participants acquire actual knowledge?

A participant may receive information about the transactions and their illegality from a source such as a government agency or may identify such transactions during the course of its usual business and compliance practices.

2710. Does Regulation GG provide any safe harbour to covered participants?

Yes, the rule gives examples of policies and procedures that constitute a safe harbour for compliance for each type of payment system. Also, a person who identifies and blocks a transaction, prevents or prohibits the acceptance of its products or services in connection with a transaction, or otherwise refuses to honour a transaction, shall not be liable to any party if:

- The transaction is a restricted transaction;
- Such person reasonably believes the transaction to be a restricted transaction; or
- The person is a participant in a designated payment system and blocks or otherwise prevents the transaction in reliance on the policies and procedures of the designated payment system in an effort to comply with the regulation.

2711. If an operator-driven system, such as a card system, has policies and procedures in place to comply with the UIGEA regulation, can participants in those systems leverage these policies and procedures?

The rule provides that participants in operator-driven systems may develop their own policies and procedures or may rely on and comply with conforming policies and procedures of the system operator. The participant may rely on a written statement or notice from the operator-driven system that its policies and procedures are designed to comply with the rule and may rely on these policies and procedures until and unless it is notified by its regulator that the policies and procedures are noncompliant.

2712. Which regulators are responsible for enforcing Regulation GG?

Enforcement is the responsibility of designated federal functional regulators; if no such regulator exists, the Federal Trade Commission (FTC) is responsible for enforcement.

2713. What are the consequences for not complying with the UIGEA?

A violation of the UIGEA can result in fines, up to five years imprisonment, or both, and a permanent injunction preventing the person from making or receiving bets or wagers. Additional other penalties and fines (including civil or criminal) may be imposed under other federal or state laws. Financial institution regulators may impose additional sanctions.

2714. Have any companies been indicted for violations of the UIGEA?

Yes. In 2007, the first indictment for a violation of the UIGEA was against NETeller, an international money transmitter that offers online payment services to businesses and individuals. Several million

dollars in customer funds were seized by the U.S. Department of Justice (DOJ) and returned to customers only after NETeller agreed to forfeit US$136 million as part of a deferred prosecution agreement. Since then, NETeller has exited the U.S. market.

In 2011, three of the largest online poker companies were charged with violations of the UIGEA. The federal government shut down approximately 76 bank accounts in more than 14 countries totalling over US$500 million in assets. These cases included Full Tilt Poker (Ireland), PokerStars (Isle of Man) and Absolute Poker (Costa Rica). All three companies were charged with fraud and money laundering. At the time of the bust, the domain names were seized but have since been returned.

In 2012, Full Tilt Poker and PokerStars reached a US$731 million settlement with the DOJ, of which US$547 million was made available for compensation to U.S. and foreign fraud victims. Full Tilt Poker, PokerStars and Absolute Poker have also exited the U.S. market.

In 2016, a judge ruled that Iipay Nation of Santa Ysabel was in violation of the UIGEA with its online poker and bingo games launched from their reservation in 2014. Even though the IGRA permits sovereign Native tribes to run certain gaming operations without special dispensation from the state, they were found in violation because it could not be verified that patrons who participated in Iipay Nation's online poker and bingo games were on "Indian lands."

2715. How were companies able to circumvent controls established by the UIGEA?

The following is one example of how poker companies allegedly circumvented the controls established by the UIGEA:

- Poker companies began using third-party payment processors (TPPPs) to deceive covered financial institutions by disguising internet gambling payments as those made by phony businesses and websites.
- Specifically, the poker companies began to make unlawful payments to the TPPPs in order to compensate and persuade them to lie to financial institutions with regard to the nature of these payments.
- Poker companies worked with TPPPs to apply incorrect transaction codes to the internet gambling transactions.
- Poker companies not only utilised credit cards, but also stored value cards and ACH transactions:
  - **Credit cards** – Phony companies established Visa and merchant processing accounts with offshore banks.
  - **Stored value cards** – Customers would purchase stored value cards from the phony companies.
  - **ACH** – Poker processors opened accounts in the name of the phony companies and processed fraudulent e-checking transactions.
- Small regional banks facing financial hardships were also allegedly bribed to participate in these schemes.

2716. Does the UIGEA have any applicability outside of the United States?

Foreign-located internet gambling providers are prohibited from providing illegal internet gambling services to U.S. customers if transactions are processed through a domestic payment processor.

The UIGEA encourages the cooperation of foreign governments and the Financial Action Task Force (FATF) in sharing information on internet gambling and related abuses. Many countries have begun to implement internet gambling laws of their own, ranging from restricting activities similar to the UIGEA to regulating the industry.

Certain foreign countries have challenged whether the United States can prevent internet gambling.

2717. What challenges have been made to the UIGEA?

Challenges to the UIGEA have been made both domestically and internationally. Since the passage of the UIGEA, several members of the U.S. Congress have pushed for a regulated U.S. gaming environment, as have many countries that license and permit certain types of online gambling, or a full repeal of the UIGEA. iMEGA, the Interactive Media Entertainment and Gaming Association, challenged the law in U.S. federal court, stating that the UIGEA was unconstitutional. iMEGA lost their case in 2009.

In 2005, Antigua accused the United States of protectionism and filed a complaint with the World Trade Organisation (WTO). In 2006, the WTO ruled that the United States was in violation of the 1995 General Agreement on Trade and Services (GATS) Treaty, which committed to allowing foreign entrants into the online gaming market. After the passage of the UIGEA in 2006, the WTO maintained that this law continued to violate the GATS Treaty.

The Restoration of America's Wire Act (RAWA), originally introduced in 2014 and again in 2015, attempts to extend the federal Interstate Wire Act of 1961, which does not address the internet as a wagering medium, to ban most forms of online gambling, with some exemptions (e.g., online horse wagering, fantasy sports wagering), regardless of state, local and tribal laws and regulations (e.g., existing state-regulated online gambling in New Jersey, Delaware and Nevada).

2718. What are some of the common challenges to complying with the UIGEA/Regulation GG?

The following include some of the challenges that financial institutions and/or payment processors have experienced in complying with the UIGEA/Regulation GG:

- Lack of awareness by business units or departments of applicability to their specific job duties.
- Lack of or inadequate communication and implementation of effective internal policies and procedures in coordination with existing business processes (e.g., correspondent banking monitoring).
- Overreliance on relationship managers' knowledge about the activities of their commercial account holders, thereby leading to inadequate due diligence on commercial customers.

- Lack of incorporation into new or existing risk assessment methodologies for both customers and TPPPs.

Fantasy Sports Wagering

2719. What are "fantasy sports contests" and how big is the fantasy sports market?

Fantasy sports contests generally refers to games of simulated sports with virtual teams that are not based on actual live-action sports teams. Participants create their own virtual teams and compete against other virtual teams utilising player statistics, sometimes for cash prizes. While the most popular is football, fantasy sports contests includes many sports (e.g., baseball, basketball, hockey, boxing, golf, auto racing). Examples of fantasy sports contests include, but are not limited to, the following:

- Major professional sports leagues (e.g., National Football League [NFL], Major League Baseball [MLB], National Basketball Association [NBA]);
- Major media companies (e.g., Yahoo!, ESPN, NBC, Sports Illustrated); and
- Other businesses (e.g., DraftKings, FanDuel, FantasyDraft, Star Fantasy Leagues).

According to the Fantasy Sports Trade Association (FSTA), the first fantasy sports contests occurred when Wilfred Winkenbach devised fantasy golf in the 1950s. The number of players has increased from 500,000 in 1988 to 56.8 million in 2013 with the average player spending US$111 annually or US$3.6 billion cumulatively in spending.

2720. Are fantasy sports contests the same as sports betting?

Not necessarily. Some fantasy sports contests are free, do not accept real money to play and do not reward winners with cash prizes.

2721. What are the heightened ML/TF risks of daily fantasy sports (DFS)?

Fantasy sports contests can run in various lengths (e.g., daily, weekly, seasonally). Some believe daily fantasy sports (DFS) are higher risk for problem gambling than season-long contests, as there are more opportunities to "lose," assuming games are paid contests. In terms of ML/TF risk, DFS is high risk due to it being a largely unregulated industry without a mature understanding of inherent risks. ML/TF risks increase if the DFS operators enable the transferring of funds to third-parties or allow users to place funds into the system anonymously or with an unknown source of funds. Though some states are enacting a regulatory framework to supervise DFS operators, operators may elect to self-regulate and implement AML/CFT controls to mitigate inherent risks.

2722. Is fantasy sports wagering legal in the United States?

Fantasy sports wagering is considered to be a game of skill by some and not a game of chance as with other types of gambling. Fantasy sports wagering was exempted from the definition of a "bet or wager" under the UIGEA. The specific UIGEA exemption reads as follows:

- "Participation in any fantasy or simulation sports game or educational game or contest in which (if the game or contest involves a team or teams) no fantasy or simulation sports team is based on the current membership of an actual team that is a member of an amateur or professional sports organisation (as those terms are defined in section 3701 of title 28) and that meets the following conditions:
    - All prizes and awards offered to winning participants are established and made known to the participants in advance of the game or contest and their value is not determined by the number of participants or the amount of any fees paid by those participants.
    - All winning outcomes reflect the relative knowledge and skill of the participants and are determined predominantly by accumulated statistical results of the performance of individuals (athletes in the case of sports events) in multiple real-world sporting or other events.
    - No winning outcome is based:
        - On the score, point-spread, or any performance or performances of any single real-world team or any combination of such teams; or
        - Solely on any single performance of an individual athlete in any single real-world sporting or other event."

2723. Is fantasy sports wagering legal in all states?

While fantasy sports wagering is legal under Federal law, each state defines legal and illegal internet gambling activities. Some states are pressuring the U.S. Congress to repeal prohibitive gambling laws while others are legalising specific gambling activities under their state law.

New York State is one example of a state electing to legalise and regulate fantasy sports:

- In November, 2015, New York's attorney general issued cease-and-desist letters to two of the largest daily fantasy sports operators, FanDuel and DraftKings, arguing that their daily fantasy sports operations were games of chance which were illegal under New York state law. Many smaller DFS operators pulled out of the New York market as a result;
- In December 2015, a court ruled against FanDuel's and DraftKings' appeal of the cease-and-desist orders, requiring them to cease operations in New York. However, later in the same day, an appeals court stayed the injunction;
- In March 2016, FanDuel and DraftKings signed provisional settlement agreements that, at a minimum, prohibited them from allowing New York state residents (and residents of other states that prohibit fantasy sports wagering) to participate in paid contests.
- In August 2016, New York legalised the operation of fantasy sports contests referenced as "interactive fantasy sports" under S8153 – Interactive Fantasy Sports – "An act to amend the racing, pari-mutuel wagering and breeding law, in relation to the registration and regulation of interactive fantasy sports contests." New York's law includes the following components:

- Registration and oversight for fantasy sports operators by the New York State Gaming Commission (NYSGC);
- 15 percent tax on gross revenues; and
- Consumer protection (e.g., minimum age of 18 years for participants, advertisement restrictions, self-exclusion).

2724. Are fantasy sports operators considered casinos and therefore subject to AML/CFT laws and regulations?

Fantasy sports wagering is not included in the definition of a "bet or wager" therefore operators do not fall within the definition of a casino and thus are not subject to AML/CFT laws and regulations of casinos and card clubs.

Impact on Financial Institutions

2725. What are the obligations of financial institutions as they relate to internet gambling and fantasy sports?

Financial institutions are obligated to implement the following as it relates to internet gambling and fantasy sports:

- Develop policies and procedures to prohibit the processing of prohibited transactions pursuant to the UIGEA if operating a covered payment system;
- File Suspicious Activity Reports (SARs) on potentially suspicious activity (e.g., minimal gaming with large transactions, transactions with no apparent economic, business or lawful purpose);
- Conduct enhanced due diligence on customers who provide internet gambling and fantasy sports services

For further guidance on the AML/CFT obligations of casinos and card clubs, please refer to the Casinos and Card Clubs section.

Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act

Basics

2726. What are "tax evasion," "tax avoidance" and "tax fraud"?

The Internal Revenue Service (IRS) defines these terms as follows:

- Tax evasion is the illegal reduction or nonpayment of taxes.
- Tax avoidance is the legal reduction or nonpayment of taxes.
- Tax fraud is the intentional wrongdoing by the taxpayer with the specific purpose of evading taxes owed or believed to be owed and can result in both civil and criminal penalties.

2727. What are some common methods used to evade taxes?

The IRS provides the following common methods used by taxpayers to evade taxes:

- Intentional understatement or omission of income;
- Claiming fictitious or improper deductions;
- False allocation of income;
- Improper claims, credits or exemptions; and
- Concealment of assets.

Sometimes it is difficult to distinguish between tax evasion and tax avoidance schemes. Corporations can report profits, sales, employees and assets in a manner intended to evade and/or avoid paying taxes. The Organisation for Economic Co-operation and Development (OECD) refers to these tactics as base erosion and profit shifting (BEPS), "tax avoidance strategies that exploit gaps and mismatches in tax rules to artificially shift profits to low or no-tax locations."

2728. What are some common methods used to exploit secrecy laws to reduce tax liabilities?

The IRS provides the following types of entities and schemes used to exploit secrecy laws to reduce tax liabilities:

- Foreign trusts;
- Foreign corporations;
- Foreign (offshore) partnerships, LLCs and LLPs;
- International business companies (IBCs);
- Offshore private annuities;
- Private banking (U.S. and offshore);
- Personal investment companies (PICs);
- Captive insurance companies;
- Offshore bank accounts and credit cards; and
- Related-party loans.

For further guidance on high-risk business entities, please refer to the section Business Entities: Shell Companies, Private Investment Companies.

2729. Is tax evasion considered a predicate crime for money laundering in the United States?

Tax evasion designed to hide illicit funds is considered a predicate crime for money laundering in the United States. If intent to violate federal law can be proven, even tax evasion with legitimate funds is a predicate crime. For further guidance on tax-related disclosures, please refer to the Report of Foreign Bank and Financial Accounts section.

2730. What are "tax havens"?

The IRS defines "tax havens" as "foreign jurisdictions offering financial secrecy laws in an effort to attract investment from outside their borders. They impose little or no tax on income from sources outside their jurisdiction." According to the Tax Justice Network (TJN), some of the top tax havens, according to its Financial Secrecy Index, include but are not limited to, the following:

- Cayman Islands
- Germany
- Hong Kong
- Ireland
- Isle of Man
- Jersey
- Lebanon
- Luxembourg
- Mauritius
- Singapore
- Switzerland
- United States

According to a European Parliament Report, EU-US Trade and Investment Relations: Effects on Tax Evasion, Money Laundering and Tax Transparency, published in March 2017, the United States is an "emerging leading tax and secrecy haven for rich foreigners" because of its resistance to "new global tax disclosure standards" and provision of "tax free facilities available for non-residents."

2731. What is the scale of offshore tax evasion?

Measuring the current scale of offshore tax evasion is extremely difficult. Some estimate the United States loses US$100 billion in tax revenues annually.

2732. What is "offshore finance"?

The International Monetary Fund defines "offshore finance" as the "provision of financial services by banks and other agents to non-residents" (e.g., borrowing from non-residents and lending to residents, investing deposits in foreign financial markets).

2733. What is an "offshore financial center (OFC)"?

The IMF poses a broad definition that would capture most major financial centres in the world, "any financial center where offshore activity takes place." IMF's narrower definition of OFC is "a center where the bulk of financial sector activity is offshore on both sides of the balance sheet (that is the counterparties of the majority of financial institutions' liabilities and assets are non-residents), where the transactions are initiated elsewhere, and where the majority of the institutions involved are controlled by non-residents. OFCs are usually referred to as:

- Jurisdictions that have relatively large numbers of financial institutions engaged primarily in business with non-residents;
- Financial systems with external assets and liabilities out of proportion to domestic financial intermediation designed to finance domestic entities; and

- More popularly, centres which provide some or all of the following services: low or zero taxation; moderate or light financial regulation; banking secrecy and anonymity."

OFCs can offer services for both legitimate and nefarious purposes. The Financial Stability Forum (FSF) outlined the following examples of uses of OFCs, including but not limited to, the following:

- Offshore banking licenses;
- Offshore corporations or international business corporations (IBCs);
- Special purpose vehicles (SPEs);
- Tax planning;
- Tax evasion and money laundering; and
- Asset management and protection.

2734. What are some examples of OFCs and what is being done to mitigate the potential ML/TF risks of these centres?

The IMF identified 44 OFCs for review in 2000 including, but not limited to, the following:

- Andorra
- Aruba
- Cyprus
- Gibraltar
- Guernsey
- Isle of Man (dependency of United Kingdom)
- Liechtenstein
- Macao (region of the People's Republic of China)
- Monaco
- Panama

The IMF initiated the Offshore Financial Center (OFC) Assessment Program in 2000 to evaluate each jurisdiction's compliance with supervisory banking and AML/CFT standards. In 2008, the OFC Assessment Program was integrated into the broader Financial Sector Assessment Program (FSAP)

2735. Are there specific U.S. laws that address offshore tax evasion?

The United States has enacted several laws to combat offshore tax evasion, including, but not limited to the following:

- Bank Secrecy Act (BSA) requires the filing of a Report of Foreign Bank and Financial Accounts (FBAR) by U.S. taxpayers who have a financial interest in, or signature or other authority over, any foreign financial accounts, including bank, securities or other financial accounts in a foreign

country, which have a maximum value exceeding US$10,000 (alone or in aggregate) at any time during a calendar year. For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section.

- The IRS requires U.S. taxpayers to file Form 8938 – Statement of Specified Foreign Financial Assets. Different from FBARs (e.g., different definitions, thresholds, valuations, due dates), U.S. taxpayers may be required to file one or both FBAR and Form 8938.
- Foreign Account Tax Compliance Act (FATCA) (2010) requires U.S. taxpayers to report certain foreign financial accounts and offshore assets and requires foreign financial institutions (FFIs) to identify accounts owned by U.S. persons to the IRS. For further guidance, please refer to the Foreign Account Tax Compliance Act section.

In 2015, the U.S. Congress introduced the Stop Tax Haven Abuse Act which, if passed, would authorise the Treasury Department to impose restrictions on foreign jurisdictions or financial institutions operating in the United States that significantly impede U.S. tax enforcement, such as reporting requirements to the IRS and the SEC on select business activities, AML/CFT requirements for investment advisers and persons engaged in forming new business entities and other restrictions on foreign income and taxation of specific U.S. corporations with foreign income.

2736. What key international treaties and conventions have influenced or shaped U.S. international tax reporting laws?

The United States has adopted several international treaties, conventions and resolutions including, but not limited to, the following:

- Convention on Mutual Administrative Assistance in Tax Matters, also referred to as the Multilateral Agreements on Administrative Assistance in Tax Matters (MAATM) (2010) by the OECD and the Council of Europe (COE) – With over 100 participating jurisdictions, this convention aims to facilitate international cooperation in the exchange of financial information to better assess and collect taxes. Although the United States has signed the MAATM, it has not yet been ratified.
- Multilateral Competent Authority Agreement on Automatic Exchange of Financial Account Information: Common Reporting Standard (CRS) (2014) – Developed by the Organisation for Economic Co-operation and Development (OECD) as an automatic information exchange (AIE) standard for participating jurisdictions to obtain information from their financial institutions and automatically exchange that information on an annual basis. The OECD published guidance: the Standard for Automatic Exchange of Financial Account Information in Tax Matters, the CRS Implementation Handbook and CRS Related Frequently Asked Questions to assist jurisdictions with implementing the CRS.
- European Union Savings Tax Directive (EUSTD) (2003) – An AIE similar to the U.S. FATCA, requiring EU members to provide other EU members with financial information on EU residents for tax purposes.

2737. How does the Financial Action Task Force (FATF) address tax crimes?

FATF encourages countries to include tax crimes as a predicate offense for money laundering by expanding the scope of money laundering in its 2012 update to the FATF Recommendations. For further guidance, please refer to the Financial Action Task Force section.

2738. What are some examples of recent offshore tax evasion scandals?

The following are recent offshore tax evasion scandals:

- In February 2016, the DOJ filed a deferred prosecution agreement against Swiss bank Julius Baer requiring payment of US$547 million for conspiracy to defraud the IRS, file false federal income tax returns and evade federal income taxes. Julius Baer assisted U.S. taxpayers in hiding assets in offshore accounts and in evading U.S. taxes on income earned in those accounts. Additionally, two Julius Baer client advisers plead guilty to felony tax charges for their role in these criminal acts and faced a maximum sentence of five years in prison. To help U.S. taxpayers hide assets, the advisers took the following types of actions:
  - Held U.S. taxpayers' assets in undeclared accounts managed by third-party asset managers;
  - Utilised "code word arrangements" to avoid identifying U.S. taxpayers by name;
  - Opened and maintained accounts in the name of various structures (e.g., foundations, trusts) or non-U.S. relatives to conceal the beneficial ownership of the accounts of U.S. taxpayers.
- Julius Baer earned approximately US$87 million in profits on nearly 2,600 undeclared accounts between 2001 and 2011 but had helped U.S. taxpayers evade their U.S. tax obligations from at least the 1990s. In 2008, Julius Baer began exiting relationships on U.S. taxpayer accounts that lacked evidence of U.S. tax compliance. In 2009, Julius Baer decided to voluntarily approach U.S. law enforcement authorities regarding its conduct related to U.S. taxpayers but ultimately did not self-report at the request of its Swiss regulator.
- In April 2016, over 11.5 million documents (Panama Papers) from Mossack Fonseca (MF), a Panama-based law firm specialising in the formation and management of entities in tax havens, identifying the beneficial owners of 214,000 offshore entities were leaked by an anonymous source, according to the International Consortium of Investigative Journalists (ICIJ). In September 2016, the same source that leaked the Panama Papers also leaked information from the Bahamas corporate registry, linking approximately 140 international and local politicians to offshore companies in the Bahamas. The ICIJ published the leaked information in its Offshore Leaks Database. According to media reports, in February 2017, the two founders of Mossack Fonseca were arrested for their alleged involvement in a separate money laundering investigation involving corruption in Latin America. These leaks had corruption, tax evasion and cybersecurity implications. For further guidance, please refer to the sections: Anti-Bribery and Corruption Compliance Programs and Cyber Events and Cybersecurity.

2739. What has been the regulatory and legal response to the Panama Papers/Bahamas Leaks and general use of offshore tax havens?

Regulatory and tax authorities launched numerous investigations in multiple countries (e.g., United States, United Kingdom, Germany, Australia, Sweden, Hong Kong, Chile, Singapore, India); formed committees and task forces to investigate the implications of the leaks; and introduced new legislation to address tax evasion and its enablers including, but not limited to, the following:

- **Customer Due Diligence Requirements for Financial Institutions (Beneficial Ownership Rule)** – Though the Beneficial Ownership Rule was finalised in July 2016, it was introduced in 2012, years before the Panama Papers/Bahamas Leaks, as the lack of identifying beneficial owners of legal entity customers was highlighted as a gap in the AML/CFT framework of the United States. For further guidance, please refer to the Beneficial Owners section.
- **Tackling Offshore Tax Evasion: A Requirement to Correct (2016) by Her Majesty's Revenue and Customs (HMRC)** (2016) – Introduced a new criminal offense to apply to corporations that "fail to prevent their representatives from facilitating tax evasion, where the corporation cannot show they took responsible steps to prevent this."
- In May 2016, the Financial Crimes Enforcement Network (FinCEN) announced pending legislation requiring the collection of information (e.g., employee identification number [EIN]) on **foreign-owned single member LLCs**, also referred to as **disregarded entities**. Currently there is no obligation for these disregarded entities to obtain an EIN or report to the IRS thereby making them attractive corporate vehicles used to avoid and evade taxes.

2740. How can financial institutions prepare for ongoing regulatory interest in users of offshore structures and companies?

To prepare for the ongoing regulatory interest, financial institutions can do the following:

- Assess exposure to the offshore world (e.g., offshore centres, tax havens, corporate vehicles, shell companies) and update AML/CFT policies and procedures accordingly;
- Update Know Your Customer (KYC) programs to reflect recent regulatory changes (e.g., identification of beneficial owners); collect enhanced due diligence on select high risk customers (e.g., country of registration/domicile and ownership/control percentages of beneficial owners, nominee shareholders); and gain an understanding of customers' purpose(s) for using offshore structures to ensure offshore tax evasion or other financial crimes are not being enabled;

For guidance on high-risk business entities, please refer to the Business Entities: Shell Companies, Private Investment Companies section.

2741. Who is responsible for examining financial institutions for tax evasion?

In the United States, the Internal Revenue Service (IRS) is responsible for tax collection and tax law enforcement.

2742. Does FinCEN share Suspicious Activity Reports (SARs) and other reports with the IRS?

Yes. FinCEN shares its Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs) and other information with the IRS.

In 2015, the OECD's Tax Force on Tax Crimes (TFTC) published Improving Co-operation Between Tax and Anti-Money Laundering Authorities: Access by Tax Administrations to Information Held by Financial Intelligence Units for Criminal and Civil Purposes to share best practices on a "whole of government" approach to combating tax and other financial crimes (e.g., unfettered access, joint decision-making between the FIU and tax administration on the allocation of access, sole FIU decision-making on access).

2743. What key guidance and resources have been provided related to offshore tax evasion and voluntary tax compliance programs?

The following key guidance and resources have been provided related to offshore tax evasion and voluntary tax compliance programs:

- **Abusive Offshore Tax Avoidance Schemes – Talking Points** by the IRS
- **Offshore Compliance Initiative News, Indictments, Pleas, Sentencings and Other Developments** by the Tax Division of the U.S. Department of Justice (DOJ)
- **International Academy for Tax Crime Investigation** by the OECD
- **EU-US Trade and Investment Relations: Effects on Tax Evasion, Money Laundering and Tax Transparency** (2017) by Dr. Isabelle Ioannides with Simona Guagliardo for the European Parliamentary Research Service (EPRS)
- **Offshore Financial Centers Background Paper** (2000) by the International Monetary Fund (IMF)
- **Working Group on Offshore Financial Centers Report** (2000) by the Financial Stability Forum (FSF)
- **Tax Haven Abuses: The Enablers, the Tools and Secrecy** by the United States Senate Permanent Subcommittee on Investigations (2006)
- **OECD Bribery Awareness Handbook for Tax Examiners** (2009) by the OECD
- **Foreign Account Tax Compliance Act (FATCA) Portal** (2010) by the Internal Revenue Service (IRS)
- **The OECD Initiative on Tax Havens** (2010) by Congressional Research Service (CRS) Report for Congress by James K. Jackson
- **Tax Co-operation 2010: Towards a Level Playing Field - Assessment by the Global Forum on Transparency and the Exchange of Information** (2010) by the Organisation for Economic Co-Operation and Development (OECD)

- **Best Practices Paper: Managing the Anti-Money Laundering and Counter-Terrorist Financing Policy Implications of Voluntary Tax Compliance Programmes** (2012) by FATF
- **Effective Inter-Agency Co-operation in Fighting Tax Crimes and Other Financial Crimes** (2012) by the OECD
- **International Co-operation Against Tax Crimes and Other Financial Crimes: A Catalogue of the Main Instruments** (2012) by the OECD
- **Bribery and Corruption Awareness Handbook for Tax Examiners and Tax Auditors** (2013) by the OECD
- **Improper Use of Tax Treaties, Tax Avoidance and Tax Evasion** (2013) by the United Nations (UN) by Philip Baker
- **Tax Crimes and Money Laundering Typology Research** (2013) by the Eurasian Group on Combating Money Laundering and the Financing of Terrorism (EAG)
- **Transparency of Company Ownership and Control** (2013) by various global partners (e.g., Group of Twenty Finance Ministers and Central Bank Governors (G-20), Financial Action Task Force (FATF), Global Forum on Transparency and Exchange of Information for Tax Purposes)
- **FATF Guidance: Transparency and Beneficial Ownership** (2014) by FATF
- **Offshore Financial Centers (OFCs): IMF Staff Assessments** (2014) by the International Monetary Fund (IMF)
- **Standard for Automatic Exchange of Financial Account Information** (2014) by the OECD
- **Preventing the Granting of Treaty Benefits in Inappropriate Circumstances** (2014) by the OECD and G20
- **Improving Co-operation Between Tax and Anti-Money Laundering Authorities: Access by Tax Administrations to Information Held by Financial Intelligence Units for Criminal and Civil Purposes** (2015) by the OECD
- **Update on Voluntary Disclosure Programmes: A Pathway to Tax Compliance** (2015) by the OECD
- **Tax Havens: International Tax Avoidance and Evasion** (2015) by the CRS for Congress by Jane G. Gravelle
- **Tax Systems: A Channel for Corruption or a Way to Fight It?** (2015) by Transparency International (TI)
- **Financial Secrecy Index** (FSI) (launched in 2015, releases periodic country reports evaluating secrecy and offshore financial activities) by the Tax Justice Network (TJN)

Voluntary Tax Compliance Programs

2744. What is a voluntary tax compliance program and how has it been abused for money laundering and terrorist financing?

The Financial Action Task Force (FATF) defines a voluntary tax compliance (VTC) program as any program "designed to facilitate legalisation of the taxpayer's situation vis-à-vis funds or other assets that were previously unreported or incorrectly reported." The purposes of VTC programs include, but are not limited to, the following:

- Raise tax revenue;
- Increase tax honesty and compliance; and
- Facilitate asset repatriation.

Examples of VTC programs include, but are not limited to, the following:

- Initiated in January 2012, the **Offshore Voluntary Disclosure Program (OVDP)** is a VTC program administered by the IRS for U.S. taxpayers to resolve their civil tax and penalty obligations as a path to avoid criminal liability. The OVDP is designed specifically for taxpayers facing potential criminal liability and/or substantial civil penalties for the wilful failure to report foreign financial assets and pay tax liabilities on those assets. The OVDP is a continuation of past similar programs of the IRS (e.g., Offshore Voluntary Disclosure Initiative [OVDI] from 2011).
- Initiated in 2013, the **Swiss Bank Program,** similar to a VTC program, is an amnesty initiative administered by the DOJ for Swiss banks to resolve potential criminal liabilities in the United States. As a result, approximately 80 non-prosecution agreements have been executed.
- Initiated in 2009, the **New Disclosure Opportunity (NDO)** is a VTC program administered by the HM Revenue and Customs (HMRC) for U.K. taxpayers. Other U.K. VTC programs include the Liechtenstein Disclosure Facility (LDF) and Crown Dependencies Disclosure Facilities.
- A permanent program, the **Voluntary Disclosures Program (VDP)** is a VTC program administered by the Canada Revenue Agency (CRA) for Canadian taxpayers;

VTC programs without appropriate AML/CFT preventive measures can be abused by criminals if declared or repatriated funds/assets are not properly vetted. Many countries are implementing VTC programs ahead of anticipated automatic information exchange (AIE) programs to be implemented under the Common Reporting Standard (CRS) lead by the OECD.

2745. How can VTC programs be protected from abuses for money laundering and terrorist financing?

FATF suggests the following four principles to protect VTC programs from abuse:

- **Application of AML/CFT preventive measures** (e.g., use accounts of financial institutions subject to AML/CFT laws and regulations, conduct due diligence on taxpayers and sources of funds, identify beneficial owners, train on risks for employees, particularly compliance personnel);

- **Prohibition on exempting AML/CFT requirements** (e.g., partial or no application of AML/CFT preventive measures such as accepting wire transfers that do not include originator/beneficiary information pursuant to AML/CFT recordkeeping rules);
- **Domestic coordination and cooperation** (e.g., information sharing mechanisms with domestic tax, regulatory and law enforcement authorities); and
- **International cooperation** (e.g., mutual legal assistance, treaties and information exchange with international authorities).

Foreign Account Tax Compliance Act

Overview

2746. What is the Foreign Account Tax Compliance Act?

The Foreign Account Tax Compliance Act (FATCA), enacted in 2010 as part of the Hiring Incentives to Restore Employment (HIRE) Act, is designed to combat tax evasion by U.S. taxpayers by requiring U.S. taxpayers to report certain foreign financial accounts and offshore assets and by requiring foreign financial institutions (FFIs) to identify accounts owned by U.S. persons to the Internal Revenue Service (IRS). FFIs failing to comply with FATCA requirements may be subject to significant tax withholding on dividends, interest and other payments originating in the United States.

The final regulations implementing FATCA for FFIs were issued in January 2013 under 26 C.F.R. Parts 1 and 301 – Regulations Relating to Information Reporting by Foreign Financial Institutions and Other Foreign Entities. Temporary and proposed regulations have been issued for U.S. taxpayers under 26 C.F.R. Part 1 – Reporting of Specified Foreign Financial Assets.

2747. What is the stated primary objective of FATCA?

The central thrust of FATCA is to identify U.S. account holders who have assets outside of the United States and provide reporting of that information to the IRS. The stated policy objective of FATCA is to achieve reporting on U.S. accounts, rather than withholding.

2748. Is FATCA an AML/CFT law?

No, FATCA is a tax law. However, FATCA resembles in many respects AML/CFT legislation and, indeed, the FATCA regulations permit reliance on existing AML/CFT compliance processes (e.g., Know Your Customer [KYC]) to identify customers subject to FATCA reporting requirements.

2749. Are the filing requirements under FATCA the same as the Report of Foreign Bank and Financial Accounts (FBAR) filing requirements under the Bank Secrecy Act (BSA)?

The reporting thresholds under FATCA and the BSA are different. Filers may be required to file one or both. Key differences include, but are not limited to, the following:

- Reporting thresholds
- Due dates

- Definition of "interest" in an account or asset
- Types of reportable foreign assets
- Valuation of reportable foreign assets

For further guidance on FBARs, please refer to Report of Foreign Bank and Financial Accounts section.

2750. Who is impacted by FATCA?

FATCA imposes requirements on three primary groups:

- FFIs that maintain accounts for U.S. account holders or foreign entities with 10 percent or more ownership by U.S. persons;
- U.S. taxpayers holding specified financial assets outside of the United States; and
- U.S. financial institutions acting as withholding agents and with other FATCA-related responsibilities.

Further guidance is provided on the obligations of FFIs and U.S. financial institutions below.

2751. How is a "foreign financial institution" defined for the purposes of FATCA?

A foreign financial institution (FFI) is a non-U.S. entity that:

- Accepts deposits in the ordinary course of business (e.g., banks, credit unions, building societies);
- Holds financial assets for others (e.g., broker-dealers, trust companies, clearing organisations, custodians); or
- Engages primarily in the business of investing, reinvesting or trading in securities, partnerships or commodities (e.g., mutual funds, hedge funds, venture capital funds, private equity funds).

2752. Are any types of FFIs exempt from FATCA?

Yes. FFIs in the following categories may be exempt from FATCA:

- Governmental entities
- Nonprofit organisations
- Retirement entities

2753. What are the obligations of FFIs under FATCA?

Under FATCA, the obligations for FFIs that have signed an agreement with the IRS include:

- Registering with the IRS as a participating FFI (PFFI) or as a "registered deemed-compliant FFI" (RDCFFI);
- Conducting customer due diligence to identify U.S. account holders or accounts held by foreign entities substantially owned by U.S. persons;

- Ensuring that a 30 percent tax on certain payments of U.S. source income is withheld when paid to non-participating FFIs and account holders who are unwilling to provide the required identification information or documentation (e.g., recalcitrant account holder);
- Closing of accounts in certain instances of noncompliance;
- Submitting annual reports to the IRS with information about U.S. account holders and accounts held by foreign entities substantially owned by U.S. persons;
- Conducting compliance reviews and certifying compliance with FATCA; and
- Providing additional information to the IRS in determining whether the FFI's obligations were met under FATCA.

2754. How is "substantial ownership" defined for FATCA purposes?

FATCA defines "substantial ownership" as:

- "With respect to any corporation, any specified United States person which owns, directly or indirectly, more than 10 percent of the stock of such corporation (by vote or value),
- With respect to any partnership, any specified United States person which owns, directly or indirectly, more than 10 percent of the profits, interests or capital interests in such partnership, and
- In the case of a trust:
    - Any specified United States person treated as an owner of any portion of such trust under subpart E of part I of subchapter J of chapter 1, and
    - To the extent provided by the Secretary in regulations or other guidance, any specified United States person which holds, directly or indirectly, more than 10 percent of the beneficial interests of such trust."

2755. How is "substantial ownership" different from "beneficial ownership"?

While similar, the definition of "beneficial owner" in the AML/CFT rule "Customer Due Diligence Requirements for Financial Institutions," finalised in July 2016, uses a two-pronged concept – ownership and effective control – by defining a "beneficial owner" as a natural person, not another legal entity, who meets the following criteria:

- **Ownership prong** – Each individual, up to four, who owns, directly or indirectly, 25 percent or more of the equity interest in a legal entity customer; and
- **Control prong** – At least one individual who exercises significant responsibility to control, manage or direct (e.g., a C-suite Executive, Managing Member, General Partner, President, Treasurer) the legal entity.

For further guidance on AML/CFT requirements on beneficial ownership, please refer to the Beneficial Owners section.

2756. Can an authorised third party assume the responsibilities for FFIs under FATCA?

Yes. FFIs can participate in expanded affiliated groups (EAG), a group of affiliated FFIs in which a lead financial institution (foreign or domestic) takes on FATCA responsibilities.

Qualified intermediaries (QIs), withholding foreign partnerships (WPs) or withholding foreign trusts (WTs), under a written agreement, can also assume withholding and reporting obligations of FFIs under FATCA.

2757. What are the obligations of U.S. financial institutions under FATCA?

Under FATCA, the obligations for U.S. financial institutions include:

- Registering with the IRS as a sponsoring entity for FFIs or as the lead financial institution for EAGs;
- Registering foreign branches directly or as qualifying intermediaries (QIs) with the IRS;
- Ensuring that a 30 percent tax on certain payments of U.S. source income is withheld when paid to foreign entities that have not provided required information for purposes of FATCA; and
- Submitting reports to the IRS about nonfinancial foreign entities substantially owned by U.S. persons.

FATCA also requires U.S. taxpayers to self-report assets held at FFIs in excess of a specific threshold, determined by residence and tax filing status (separate or joint) on IRS Form 8938: Statement of Specified Foreign Financial Assets.

2758. What steps has the U.S. taken to improve international compliance with FATCA?

To address certain legal issues on information sharing directly with the IRS, the U.S. pursued arrangements with foreign governments to provide for alternative reporting by FFIs to resident country governments, who would share this information with the IRS under a tax treaty or other agreement.

In July 2012, the U.S. Treasury Department published model intergovernmental agreements (IGAs) to implement the information sharing with FATCA partner countries. The IGAs address privacy restrictions and other concerns of FFIs on sharing customer information and provide a mechanism for bilateral sharing of information between governments called the International Data Exchange (IDE). Two types of model IGAs are provided:

- Model 1 IGA – PFFIs report directly to the Host Country Tax Authority (HCTA) in the FATCA partner country, who in turn, automatically reports to the IRS.
- Model 2 IGA – PFFIs report directly to the IRS; FATCA partner countries enable this direct exchange (e.g., by removing domestic legal impediments).

Many countries have signed IGAs or have reached agreements in substance regarding FATCA. For further guidance on IGAs and a list of FATCA partner countries, please visit the U.S. Department of the Treasury's FATCA IGA Resource Center at http://www.irs.gov/Businesses.

2759. How is "U.S. source income" defined for the purposes of FATCA?

"U.S. source income" is defined by IRS rules and regulations and generally refers to interest, dividends and gains on asset sales from U.S. locations.

2760. How is "fixed, determinable, annual or periodical (FDAP)" income defined by the IRS?

The IRS defines FDAP income as all income, except:

- Gains derived from the sale of real or personal property (including market discount and option premiums, but not including original issue discount); and
- Items of income excluded from gross income, without regard to the U.S. or foreign status of the owner of the income, such as tax-exempt municipal bond interest and qualified scholarship income.

Income is fixed when it is paid in amounts known ahead of time. Income is determinable whenever there is a basis for figuring the amount to be paid. Income can be periodic if it is paid from time to time. It does not have to be paid annually or at regular intervals. Income can be determinable or periodic, even if the length of time during which the payments are made is increased or decreased.

2761. Are PFFIs required to report on non-U.S. account holders under FATCA?

Yes. Accounts owned by foreign entities in which U.S. taxpayers hold a substantial ownership interest are subject to FATCA reporting requirements. Substantial ownership interest has been defined as greater than or equal to a 10 percent direct or indirect ownership interest.

2762. What are the effective dates for the various provisions of FATCA?

There are different effective dates for the various provisions of FATCA based on multiple factors (e.g., existence of IGA, model type of IGA, account balance, income type):

- Registration/FFI Agreement:
  - The effective date of any FFI agreement entered into before July 1, 2013, is July 1, 2013 (important because the effective date becomes the driver for other requirements), and the effective date of any FFI agreement entered into after July 1, 2013, will be the actual date of the agreement.
  - Registration through the FATCA Registration website became available on January 1, 2014. (The first list of Registered FFIs was published in June 2014 and will continue to be published monthly.)
- Due Diligence:
  - Due diligence procedures for new accounts must be in place by the later of January 1, 2014, or the effective date of the FFI agreement.
  - Pre-existing accounts of prima facie FFIs must be reviewed by the later of June 30, 2014, or six months after the effective date of the FFI agreement.

  - Pre-existing high-value accounts (in excess of US$1 million) of individuals must be reviewed by the later of December 31, 2014, or one year after the effective date of the FFI agreement.
  - All other pre-existing accounts must be reviewed by the later of December 31, 2015, or two years after the effective date of the FFI agreement, except for the following exempted accounts:
    - Pre-existing accounts of individuals with a balance of US$50,000 or less;
    - Pre-existing accounts of entities with a balance of US$250,000 or less; and
    - Pre-existing insurance contracts with a balance or value of US$50,000 or less.

- Reporting:
  - A report of U.S. account holders to the IRS covering only identification and select account information (e.g., balance) were due by March 31, 2015 (FFIs in Model 1 IGA jurisdictions were required to report by September 30, 2015).
  - Reporting on income paid (except certain gross proceeds from the sale or redemption of property) in addition to the aforementioned information began in 2016.
  - Reporting on gross proceeds paid to custodial accounts in addition to the aforementioned information begins September 30, 2017.

- Withholding:
  - Withholding requirements for payments of fixed, determinable, annual or periodical (FDAP) income began on July 1, 2014.

2763. Must account balances be aggregated to determine when customers must be reviewed under FATCA?

Yes. Although not an immediate requirement, account balances should be aggregated to determine if customers are "high-value" accounts, thus subject to specific measures under FATCA.

2764. Who is responsible for overseeing compliance with FATCA?

The IRS is responsible for writing and implementing regulations and overseeing PFFIs' compliance with FATCA.

2765. What are the consequences of noncompliance with FATCA?

PFFIs that do not report the required information on U.S. account holders will be subject to a 30 percent withholding on U.S. source income (e.g., interest, dividends, proceeds from securities sales). PFFI account holders who do not provide the necessary identification information or documentation are also subject to the same withholding.

U.S. taxpayers who do not report the required information are subject to a US$10,000 penalty, with an additional penalty of up to US$50,000 for continued failure to file after IRS notification. A 40 percent penalty on any understatement of taxes associated with non-disclosed assets can also be imposed. In some cases, filers may be subject to criminal penalties.

2766. What key steps should PFFIs take to ensure compliance with FATCA?

PFFIs should take the following key steps to ensure compliance with FATCA:

- Assemble a multidisciplinary work group and project management office to direct compliance efforts including, but not limited to:
    - Compliance
    - Legal
    - Treasury
    - Operations
    - IT
    - Systems
    - Audit
    - Private banking
    - Asset management
    - Risk management
- Brief senior management on the requirements for FATCA compliance and need for resources.
- Address the following issues related to IT and systems when designing an efficient and effective due diligence process:
    - Identification of U.S. person indicia
    - "Tagging" accounts of U.S. persons
    - Identification of related accounts
    - Aggregation of account balances for account holders
    - Required changes to client onboarding and acceptance processes to incorporate FATCA status to facilitate reporting and withholding obligations
    - Inventory of electronically available information to target due diligence searches of electronic databases
    - Searching electronic documentation
    - Tracking compliance efforts including missing documentation

  - Assembling information for reporting, on an entity-level and enterprise-level, where applicable

- Address potential conflicts and roadblocks to FATCA reporting requirements with applicable privacy restrictions, including the ability of customers to waive privacy rights.
- Establish capabilities and processes to identify incoming funds that are subject to possible withholding, apply proper withholding calculations, and maintain records for reporting purposes.
- Prohibit employees on advising clients on account identification avoidance.
- Develop an internal awareness and training program on FATCA.
- Develop a communication strategy for customers to address questions and concerns that may arise with the implementation of FATCA requirements.

PFFIs and the FFI Agreement

2767. What is a "PFFI" for the purposes of FATCA?

A "PFFI" is an FFI that signs an FFI agreement with the IRS.

2768. Why would an FFI enter into an agreement with the IRS?

An FFI must enter into an agreement with the IRS to avoid a 30 percent withholding on U.S. source income payments to the FFI for its own account or the accounts of its customers.

2769. What is an "FFI Agreement" for the purposes of FATCA?

An FFI agreement is a signed commitment in which FFIs agree to identify U.S. account holders, report account holder information to the IRS, withhold on payments to certain account holders, and close accounts in certain instances of noncompliance in accordance with FATCA. Under the agreement, PFFIs must also do the following:

- Adopt policies and procedures for FATCA compliance;
- Periodically conduct reviews of compliance;
- Designate a Responsible Officer (RO) to certify the PFFI's compliance to the IRS; and
- Periodically provide the IRS with certifications and other information that will assist the IRS in determining whether the PFFI has met its obligations under the FFI agreement.

2770. What is a "deemed-compliant FFI" for the purposes of FATCA?

"Deemed-compliant FFIs" are FFIs with a low risk of tax evasion, such as retirement plans and certain investment vehicles. FFIs that have applied for the "deemed-compliant" status from the IRS are not subject to the reporting and withholding requirements of FATCA. There are three categories of deemed-compliant FFIs:

- **Registered deemed compliant FFIs (RDCFFIs)** – Must meet IRS definition requirements, agree to conditions and register with the IRS, and renew their IRS certification every three years. Examples of registered deemed-compliant FFIs might be non-reporting members of FFI groups, qualified investment vehicles and restricted funds.
- **Certified deemed compliant FFIs** – Must certify directly to specific withholding agents using Form W-8, and examples might include retirement plans, nonprofit organisations and FFIs with only low-value accounts.
- **Owner-documented deemed compliant FFIs** – Must certify directly to withholding agents, provide ownership information, do not maintain accounts for non-participating FFIs, maintain low-value accounts, and are not affiliated with certain other FFIs.

2771. What is a "limited FFI"?

A "limited FFI" is defined as an "FFI that due to local law restrictions, cannot comply with the terms of an FFI agreement, or otherwise be treated a PFFI or RDCFFI, and that is agreeing to satisfy certain obligations for its treatment as a limited FFI." One of the restrictions of limited FFIs is a prohibition on establishing accounts for U.S. persons.

2772. What are the expanded affiliated group requirements for PFFIs?

All FFIs in an expanded affiliate group (EAG) must be PFFIs or RDCFFIs in order for any FFI to become a PFFI. An EAG must appoint a lead financial institution (lead FI) for the group. The lead FI can register and submit information and annual reports to the IRS on behalf of the EAG.

Registration

2773. What are the registration requirements for PFFIs and deemed-compliant FFIs under FATCA?

The registration process serves as the FFI agreement for participating FFIs and certification for deemed-compliant FFIs. As part of the registration, PFFIs must do the following:

- Select a FATCA Responsible Officer (RO) (typically the individual who signs the FFI agreement);
- Select up to five Points of Contact (POCs) with at least one in-house POC (typically the RO). POCs may include third parties, located in the home country of the PFFI or in the United States (e.g., employee of an affiliate, service provider);
- In instances where the RO or other in-house individual cannot register the FFI, delegate FATCA registration duties (including signing) by power of attorney to an authorised third party (ATP) (e.g., U.S.-licensed tax professional subject to U.S. regulatory jurisdiction);
- Submit an affirmative statement that the person signing the FFI agreement (or certification) has the authority to act for the FFI;
- Provide positive identity verification for the individual who will sign the agreement (or certification) on behalf of the FFI (e.g., RO, ATP); and

- Obtain a Global Intermediary Identification Number (GIIN).

Further details and instructions are provided on Form 8957 – Foreign Account Tax Compliance Act (FATCA) Registration.

2774. What is a FATCA ID? Is it the same as a GIIN?

A FATCA ID is an identification number assigned to member FFIs of an EAG. It is not the same as a GIIN. A GIIN is issued to FFIs who have successfully registered with the IRS.

2775. When did the IRS begin accepting registrations?

The IRS began accepting registrations through its electronic submissions process on January 1, 2014. The first list of Registered FFIs was published in June 2014 and will continue to be published monthly.

Paper registration forms can also be submitted to the IRS by mailing to the following address:

FATCA, Stop 6099 AUSC
3651 South IH 35
Austin, TX 78741

2776. Are other financial institutions with FATCA responsibilities required to register with the IRS?

Yes. In addition to PFFIs, the following may be required to register with the IRS:

- Registered deemed-compliant FFIs (RDCFFIs);
- Lead FIs (i.e., U.S. or foreign financial institutions designated as the lead institution authorised to register on behalf of an EAG);
- Member FIs (i.e., members institutions of an EAG);
- Limited FFIs (although most limited FFIs are required to register, they will not be provided GIINs); and
- Sponsoring entities (i.e., entities authorised to perform due diligence, withholding and reporting obligations under FATCA on behalf of an FFI).

U.S. financial institutions acting as lead FIs of EAGs or registering as a QI on behalf of a foreign branch may also be required to register with the IRS.

Due Diligence

2777. What is the objective of an FFI's due diligence under FATCA?

The objective of an FFI's due diligence is to put account holders into one of three "buckets":

- U.S. account holders
- Recalcitrant account holders
- Non-U.S. account holders

Each of these buckets is subject to different withholding and reporting requirements, making a robust tracking and documentation system vital to compliance with FATCA.

Identification of U.S. Account holders

2778. How can participating FFIs identify U.S. account holders?

Participating FFIs must conduct due diligence on their existing and new account holders (both individuals and entities) to identify U.S. accounts and their owners. FFIs are permitted to rely on electronic records to perform due diligence on the accounts of U.S. persons.

The following are indicia of U.S. person account ownership and should be used to identify accounts requiring further due diligence for final determination of U.S. account status:

- Identification of an account holder as a U.S. person;
- A U.S. birthplace;
- A U.S. telephone number;
- Standing instructions to transfer funds to an account maintained in the United States, or directions regularly received from a U.S. address;
- An "in care of" address or a "hold mail" address in the United States that is the sole address with respect to the client; and
- A power of attorney or signatory authority granted to a person with a U.S. address.

2779. What steps are required if indicia of U.S. account ownership is noted?

When indicia of U.S. account ownership is noted, additional steps and documentation are required to establish the status of the account holder (U.S. or non-U.S.), such as:

- Obtaining an IRS Form W-9, IRS Form W-8BEN and non-U.S. passport
- Explanation of renunciation of U.S. citizenship or other specified documentation

Based on the review of the additional documentation requested, account holders will be classified as U.S. or non-U.S. persons. Account holders who refuse to provide documentation will be classified as "recalcitrant account holders."

Pre-Existing Individual Accounts

2780. What date should be used by participating FFIs to distinguish between pre-existing and new individual accounts?

The effective date of an FFI agreement should be used to distinguish pre-existing accounts from new individual accounts.

2781. What steps does FATCA outline for reviewing pre-existing individual accounts?

FATCA suggests the following approach to identify U.S. classification for pre-existing individual accounts:

- **Step One**: Accounts with an aggregate balance or value of less than US$50,000 do not need to be reviewed, unless the FFI elects otherwise. This threshold must include the aggregated balances of all accounts owned by an individual to the extent that an FFI's systems can link accounts through common client numbers, identification numbers or other means. Each joint holder of an account will be attributed the total account balance for purposes of this aggregation.
- **Step Two**: Certain cash value insurance and annuity contracts held by individuals in pre-existing accounts with a value or balance of US$250,000 or less are exempt from review, unless the FFI elects otherwise.
- **Step Three**: Accounts with a balance or value greater than US$50,000 but less than US$1 million are subject to a review of electronically searchable information for U.S. person indicia. If no indicia are found, the account is classified as a non-U.S. account.
- **Step Four**: Accounts with a balance or value exceeding US$1 million are subject to a search of both electronic and non-electronic file information for U.S. person indicia, and inquiries of the relationship manager(s) must also be made. If no indicia are noted, the account is classified as a non-U.S. account.

If indicia are present in Steps Three or Four, additional steps and documentation are required to determine whether the account holder is a U.S. person, such as:

- Obtaining an IRS Form W-9, IRS Form W-8BEN and non-U.S. passport
- Explanation of renunciation of U.S. citizenship or other specified documentation

Based on the review of the additional documentation requested, account holders will be classified as U.S. or non-U.S. persons. Account holders who refuse to provide documentation will be classified as "recalcitrant account holders."

2782. How often are participating FFIs required to review pre-existing individual accounts?

After going through this exercise to classify pre-existing individual account holders, FFIs must annually re-test individual accounts with year-end balances that exceed US$500,000 and who were not previously subject to a review of account files.

New Individual Accounts

2783. How are "new" individual accounts defined?

New individual accounts are those opened after the effective date of the participating FFI's agreement with the IRS, and they include accounts opened by individuals who already have an existing account with the FFI.

2784. What steps does FATCA outline for reviewing new individual accounts?

Participating FFIs should take the following steps to determine U.S./non-U.S. classification of new individual accounts:

- Review the information provided at the opening of the account, including identification and any documentation collected under anti-money laundering/Know Your Customer (AML/KYC) rules.
- If U.S. indicia are identified as part of that review, obtain additional documentation to determine U.S. ownership, or treat the account as held by a recalcitrant account holder.

Pre-Existing Entity Accounts

2785. What date should be used by participating FFIs to distinguish pre-existing and new entity accounts?

The effective date of an FFI agreement should be used to distinguish pre-existing accounts from new entity accounts.

2786. What steps does FATCA outline for reviewing pre-existing entity accounts?

FATCA suggests the following approach to identify U.S./non-U.S. classification for pre-existing entity accounts:

- **Step One:** Pre-existing entity accounts with aggregate account balances of US$250,000 or less are exempt from review until the account balance exceeds US$1 million. These thresholds are based on the aggregated balances of all accounts owned by an entity to the extent that an FFI's system can link accounts through common client numbers, identification numbers or other means.
- **Step Two:** For remaining pre-existing entity accounts, electronically searchable information will need to be reviewed to determine U.S./non-U.S. classification. Generally, participating FFIs can rely on AML/KYC records and other existing account information to determine account status. For accounts identified as U.S. accounts or passive investment entities, all substantial U.S. owners (generally, 10 percent direct or indirect ownership) will need to be identified.

Entities reviewed in the above process must be put into one of the following "buckets":

- U.S. accounts (those with one or more "substantial" U.S. owners – defined generally as a 10 percent direct or indirect ownership)
- Foreign financial institutions:
  - Participating
  - Deemed-compliant
  - Non-participating
- Excepted entities (under Section 1471(f)):
  - Foreign governments or political subdivisions of foreign governments

  - International organisations and their wholly owned agencies
  - Foreign central banks
- Recalcitrant account holders
- Non-financial foreign entities (NFFEs):
  - Excepted entity
  - Passive investment entity

Similar to the process for individual accounts, pre-existing entity accounts should be reviewed in a structured manner to determine their proper classification. Accounts already identified as U.S. accounts for other U.S. tax purposes are considered U.S. accounts.

2787. How are "nonfinancial foreign entities" defined for the purposes of FATCA?

Nonfinancial foreign entities (NFFEs) are defined as foreign entities that are not financial institutions under the FATCA definition. NFFEs are subject to withholding under FATCA if they refuse to provide ownership information to participating FFIs or U.S. withholding agents.

New Entity Accounts

2788. How are "new" entity accounts defined?

New entity accounts are those opened after the effective date of the participating FFI's agreement with the IRS, and they include accounts opened by individuals who already have an existing account with the FFI.

2789. What steps does FATCA outline for reviewing new entity accounts?

For new entity accounts, the same process described above for pre-existing entity accounts may be followed, except all information obtained in the account opening process must be considered, not just the electronically searchable information. This includes all information gathered for purposes of opening and maintaining the account, corresponding with the account holder and complying with regulatory requirements, including AML/KYC requirements.

Recalcitrant Account holders

2790. How is a "recalcitrant account holder" defined for the purposes of FATCA?

A recalcitrant account holder is any holder of an account maintained by a participating FFI if the account holder is not an FFI and the account holder either:

- Fails to comply with the participating FFI's request for documentation or information to establish whether the account is a U.S. account;
- Fails to provide a valid Form W-9 upon the request of the participating FFI;

- Fails to provide a correct name and TIN upon request of the FFI after the participating FFI receives notice from the IRS indicating a name/TIN mismatch; or
- Fails to provide a valid and effective waiver of foreign law if foreign law prevents reporting with respect to the account holder by the participating FFI.

2791. What actions are participating FFIs required to take with respect to recalcitrant account holders?

The U.S. Treasury Department and the IRS intend to require a participating FFI to report the number and aggregate value of financial accounts held by the following:

- Recalcitrant account holders;
- Related or unrelated non-participating FFIs; and
- Recalcitrant account holders who have U.S. indicia.

Recalcitrant account holders will be subject to a 30 percent withholding tax.

Certification

2792. What certification requirements are participating FFIs required to provide under FATCA?

The FATCA Responsible Officers (ROs) of participating FFIs must provide certifications of the following:

- Compliance with the provisions of FATCA to the IRS;
- Required due diligence on pre-existing accounts was completed by provided deadlines; and
- Formal or informal practices or procedures were not in place at any time from August 6, 2011, forward to assist account holders in the avoidance of U.S. account identification.

2793. Are certifications required to be verified through third-party audits?

No. Verification of such compliance through third-party audits is not mandated, but may be required by the IRS in certain cases.

Reporting

2794. What are the annual reporting requirements of participating FFIs?

Participating FFIs are required to report annually the following to the IRS for its specified U.S. accounts:

- Name, address and taxpayer identification number (TIN);
- Account number;
- Account balance or value at year-end;

- Gross receipts from the account;
- Gross amount of dividends paid or credited to the account;
- Gross amount of interest paid or credited to the account;
- Other income paid or credited to the account; and
- Gross proceeds from the sale or redemption of property paid or credited to the account with respect to which the FFI acted as an agent for the account holder.

2795. When are annual reports due?

Reporting on the first four items in the aforementioned list began in 2015; reporting on dividends, interest and other income began in 2016; and reporting on gross proceeds will start in 2017.

Due dates are based on multiple factors (e.g., existence of IGA, model type of IGA, account balance, income type).

2796. What are the reporting requirements for an organisation with multiple FFIs?

As with registration requirements, in an organisation with multiple FFIs, a "lead" FFI must be appointed, and each affiliate in the group must execute an FFI agreement in order for all FFIs to be considered participating FFIs or deemed-compliant FFIs. The lead FFI can then submit required annual reports on behalf of the organisation with multiple FFIs.

2797. Are participating FFIs required to include closed accounts in their annual reports to the IRS?

In the case of a U.S. account closed or transferred in its entirety by an account holder during the year, the participating FFI will be required to report the income paid or credited to the account for the year until the date of transfer or closure, and will also be required to report the amount or value withdrawn or transferred from the U.S. account as a gross withdrawal. The FFI will also be required to report the U.S. account as closed or transferred.

Withholding

2798. What are the withholding obligations of FFIs?

Participating FFIs agree to withhold a tax equal to 30 percent of withholdable and passthru payments of U.S. source income to the following account holders:

- FFIs that have not signed agreements with the IRS and that do not fall under an exception.
- Individuals and entities that fail to provide sufficient information to determine whether or not they are a U.S. person (recalcitrant account holders) or fail to agree to waive applicable restrictions on the reporting of their information to the IRS.

2799. How are "passthru payments" defined for the purposes of FATCA?

A "passthru payment" is defined as any withholdable payment or other payment to the extent attributable to a withholdable payment. The IRS indicates that passthru payments to nonparticipating FFIs and recalcitrant account holders are subject to withholding.

2800. How are "custodial payments" defined for the purposes of FATCA?

A "custodial payment" is a payment with respect to which an FFI acts as a custodian, broker, nominee, or otherwise as an agent for another person. A custodial payment that is a withholdable payment will be treated as a withholdable payment (and thus as a passthru payment), and the FFI must apply the appropriate withholding unless the withholding obligation has been satisfied by another withholding agent.

2801. How can requests for adjustments or refunds of withheld funds be made?

The U.S. Treasury Department and the IRS issued guidance regarding the procedures necessary for requesting the following:

- Adjustments for overwithholding by withholding agent;
- Adjustments for overwithholding by a participating FFI;
- Repayment of backup withholding;
- Collective credit or refund procedures for overpayments; and
- Adjustments for underwithholding.

For further guidance, please refer to Section 10 – Adjustments for Overwithholding and Underwithholding and Refunds of IRS Bulletin 2014-29 (Rev. Proc. 2014-38).

2802. Are any entities exempt from withholding?

Yes. Withholding requirements do not apply to payments to the following beneficial owners of such payments:

- Any foreign government, any political subdivision of a foreign government, or any wholly owned agency or instrumentality of these entities;
- Any international organisation or any wholly owned agency or instrumentality of an international organisation;
- Any foreign central bank; or
- Any other class of persons identified by the Secretary of the U.S. Treasury Department as posing a low risk of tax evasion.

2803. What are the obligations for U.S. financial institutions as a withholding agent under FATCA?

To comply with its obligations as a withholding agent, U.S. financial institutions are required to determine whether to treat entities to which they make withholdable payments as:

- U.S. persons;
- Participating FFIs;
- Deemed-compliant FFIs;
- Non-participating FFIs;
- Entities described in Section 1471(f); or
- Excepted NFFEs or other NFFEs.

2804. What key guidance and resources have been provided related to FATCA?

The following key guidance and resources have been provided related to FATCA:

- FATCA informational sites administered by the IRS:
  - FATCA – Regulations and Other Guidance
  - FATCA – Current Alerts and Other News
  - FATCA Related Forms (e.g., FATCA registration, FATCA report, Form 8938 – Statement of Specified Foreign Financial Assets)
  - FATCA Information for Foreign Financial Institutions and Entities
  - Foreign Financial Institution (FFI) Search and Download Tool (approved FFIs with GIINs)
  - International Data Exchange Services (IDES) (transmit and exchange FATCA data with the United States)
  - FATCA Financial Institution Registration
  - FATCA Information for U.S. Financial Institutions and Entities
  - FATCA Information for Governments
  - FATCA Information for Individuals

- FATCA frequently asked questions (FAQs) are organised into the following categories:
    - General
    - Registration System FAQs
    - FFI List FAQs
    - IDES [International Data Exchange Services] Technical FAQs
    - Form 8938 FAQs
    - International Compliance Management Model (ICMM) FAQs
- Summary of Key FATCA Provisions (2012) by the IRS
- Details on the FATCA Registration Process for Foreign Financial Institutions (FFI) by the IRS
- Basic Questions and Answers on Form 8938 by the IRS
- Comparison of Form 8938 and FBAR Requirements by the IRS

INTERNATIONAL PERSPECTIVES AND INITIATIVES

Basics

2805. What key international groups have played an important role in the development and implementation of global AML/CFT standards?

Recognising the international focus on money laundering and terrorist financing, many groups have become active in issuing guidance and driving AML/CFT efforts, including:

- The **United Nations' (UN)** purpose is to maintain international peace and security; develop friendly relations among nations; cooperate in solving international economic, social, cultural and humanitarian problems; promote respect for human rights and fundamental freedoms; and be a centre for harmonising the actions of nations in attaining these ends.
- The **Financial Action Task Force (FATF)** is an intergovernmental policy-making body composed of more than 30 countries whose purpose is to establish and promote international legislative and regulatory standards in the areas of money laundering and terrorist financing, and to monitor members' progress in adhering to these standards, known as the FATF Recommendations. FATF works to identify trends to disseminate to the global community for combating money laundering, terrorist financing and the proliferation of weapons of mass destruction (WMDs). For additional guidance on FATF, please refer to the Financial Action Task Force section.
- The **Egmont Group of Financial Intelligence Units (Egmont Group)**, formed in 1995, has been the leading international association of financial intelligence units (FIUs). As of 2014, there are more than 130 member countries that meet annually to discuss global issues of importance with regard to money laundering as well as terrorist financing. The Egmont Group acts as a conduit for information sharing and, when pertinent, passes information on to the corresponding law enforcement agency to investigate. Examples of members are FinCEN (United States), TRACFIN (France), and FINTRAC (Canada).
- The **Wolfsberg Group of Banks (Wolfsberg Group)** is an association of 11 member international banks that creates industry best practices. Formed in 2000, the member banks include Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, J.P. Morgan Chase, Société Générale and UBS. The group has produced work products in the areas of Know Your Customer (KYC) and AML, CFT and anti-corruption best practices.
- The **Basel Committee on Banking Supervision** (BCBS) is a committee of central banks and bank supervisors and regulators from major industrialised countries that meets to discuss issues relating to banking supervision at the Bank for International Settlements (BIS) in Basel, Switzerland. BCBS was formed in 1974 by the Governors of the central banks of the G10. BCBS operates under the expectation that member nations will take into account, and then implement,

the guidance that comes out of these meetings. The goal of BCBS is to create uniform international standards of banking best practices.

- The **World Bank (WB)**, established in 1945, was founded to help countries recover from natural disasters, humanitarian crises and other conflicts that plague the developing world. With 188 member countries, the WB primarily works on reducing global poverty by the distribution of grants for development projects. The WB also has a group whose primary purpose is to curb money laundering and terrorist financing through FATF as its vehicle for change. In recent years, the WB has adopted FATF Recommendations for internal use.
- The **International Monetary Fund (IMF)** is an international body like the World Bank. It oversees the global monetary system and offers aid and assistance to countries as situations arise. The IMF, along with the WB, have created the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) program to help the global community better improve AML/CFT systems to prevent the flow of terrorist dollars into the global monetary infrastructure. This group works by providing technical assistance to countries in need.
- The **European Commission (EC)**, formally known as the Commission of the European Communities, is the executive branch of the European Union (EU) responsible for proposing legislation, implementing decisions, and upholding the EU's treaties. It also is responsible for the general day-to-day running of the EU.
- **Europol,** the European Law Enforcement Agency, was established in 1992 with the aim of improving the effectiveness and cooperation of law enforcement authorities in the EU Member States in preventing and combating terrorism, unlawful drug trafficking, and other serious forms of organised crime.
- **Organisation for Economic Cooperation and Development (OECD)** uses its wealth of information on a broad range of topics to help governments foster prosperity and fight poverty through economic growth and financial stability. The OECD helps ensure the environmental implications of economic and social development are taken into account.
- **International Organisation of Securities Commissions (IOSCO)**, established in 1983, is a global cooperative body recognised as the international standard setter for securities markets. With a membership that regulates more than 95 percent of the world's securities markets in over 100 jurisdictions, IOSCO is the primary international cooperative forum for securities market regulatory agencies.
- **Transparency International (TI),** founded in 1993, is a global civil society organisation with more than 100 chapters. Its mission is to fight against corruption by bringing together relevant players from government, civil society, business and media.
- The **Joint Money Laundering Steering Group** (JMLSG) is made up of the leading trade associations in the financial services industry in the United Kingdom with the aim of promulgating good practice in AML/CFT frameworks and to give practical assistance in interpreting UK AML/CFT laws and regulations (e.g., Proceeds of Crime Act 2002 [POCA], Terrorism Act 2000, Money Laundering Regulations 2007 [MLR]). The JMLSG has published the Prevention of Money

Laundering/Combating Terrorist Financing covering topics such as compliance officer and senior management responsibility, risk-based internal controls, sectoral guidance and sanctions.

- **Asia/Pacific Group on Money Laundering (APG)** is an autonomous and collaborative international organisation that was founded in 1997 in Bangkok, Thailand. It consists of 40 member jurisdictions, and a number of international and regional observers who assess compliance by APG member jurisdictions with the global AML/CFT standards and contribute to the global policy development of anti-money laundering and counterterrorism financing standards through active Associate Membership status in the FATF.
- **Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)**, an organisation with 14 members located in the Eastern and Southern African Region, was established at an inaugural Meeting of the Council of Ministers held in Arusha, Tanzania, on August 27, 1999. The objectives of ESAAMLG are to adopt and implement the FATF Recommendations and implement any other measures contained in multilateral agreements.
- **Organisation of American States (OAS)**, an international organisation headquartered in the United States in Washington, D.C., includes 35 independent states of the Americas. The OAS is the region's principal multilateral forum for strengthening democracy, promoting human rights and confronting shared problems such as poverty, terrorism, illegal drugs and corruption. It plays a leading role in carrying out mandates established by the hemisphere's leaders through the Summits of the Americas.
- **INTERPOL**, established in 1923, is the world's largest international police organisation with 188 member countries. Its mission is to prevent or combat international crime by facilitating cross-border police cooperation and assisting all organisations, authorities and services within the limits of existing laws in different countries.
- **MONEYVAL**, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism, formerly known as PC-R-EV, was established in 1997 by the Council of Europe. With 28 permanent members, two temporary members and numerous observers, MONEYVAL's objective is to ensure its members implement effective systems to counter money laundering and terrorist financing in accordance with international standards.

2806. How are individual country standards monitored for conformity to international AML/CFT standards?

The Financial Action Task Force (FATF) performs mutual evaluations of countries based on its recently consolidated Recommendations (formerly the "Forty plus Nine Recommendations," now referred to as simply the "FATF Recommendations"). Since the end of 2002, the World Bank (WB) and International Monetary Fund (IMF) also have been involved in the effort to assess global AML/CFT standards using the standards set forth in the FATF Recommendations, in addition to publishing their own findings.

For additional guidance on FATF and the Recommendations, please refer to the Financial Action Task Force section.

2807. Do regulatory authorities coordinate activities when examining multinational institutions?

Yes. A number of regulators have taken a proactive approach in close cross-regional collaboration and enforcement activity. An example of recent joint investigations and enforcement activities includes a large multinational U.K. bank being investigated jointly in the U.S. and the U.K.

2808. How do U.S. regulations compare to international AML/CFT regulations?

The United States' role as a leader in the fight against money laundering and terrorist financing dates back nearly 50 years to the passage of the Bank Secrecy Act (BSA) in 1970. Through the ensuing decades and especially following the terrorist activities of September 11, 2001, the United States has reinforced its commitment through the passage of a number of additional money laundering and terrorist financing-related laws, issuance of extensive regulatory guidance (e.g., United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act [USA PATRIOT Act] of 2001) and aggressive enforcement.

That said, the United States, as with many other major jurisdictions, is not in full compliance with the FATF Recommendations. In the past decade, FATF has conducted two mutual evaluations of the United States AML/CFT system, a 2006 assessment based on the Forty Plus Nine FATF Recommendations and a 2016 assessment based on the consolidated FATF Recommendations (updated in 2012 with an updated methodology in 2013). The 2006 mutual evaluation identified several areas in need of improvement, including, but not limited to, the following:

- Customer due diligence relating to beneficial owners;
- Authorised signers, legal persons and trusts;
- Ongoing due diligence; and
- General AML/CFT requirements for designated nonfinancial businesses and professions (DNFBPs) (e.g., accountants, attorneys, dealers in precious metals and stones, real estate agents).

The 2016 mutual evaluation for the United States identified significant gaps in the U.S. framework:

- Poor efforts to prevent criminals from using legal entities to facilitate illicit schemes. This low rating was driven by the inadequate and untimely access to comprehensive and accurate beneficial ownership information in the United States.
- Continued lack of coverage of DNFBPs (e.g., lawyers, accountants, real estate agents, and trust and company service providers), particularly related to CDD, recordkeeping, suspicious transaction reporting and internal controls.

In July 2016, the United States finalised the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) which addressed due diligence for beneficial owners and made the ongoing due diligence obligation an explicit requirement of U.S. AML/CFT laws and regulations. While some DNFBPs, such as casinos and dealers in precious metals and stones, are required to establish AML Programs, many are also required to file certain AML/CFT reports, including, but not limited to the following:

- Filing of Reports of Cash Payments Over US$10,000 Received in a Trade or Business (Form 8300)
- Filing of Reports of Foreign Bank and Financial Accounts (FBARs)
- Filing of Reports of International Transportation of Currency or Monetary Instruments (CMIRs)

In addition to filing reports, DNFBPs are required to comply with sanctions administered by the Office of Foreign Assets Control (OFAC), and in some instances, required to participate in information sharing as outlined by Section 314 of the USA PATRIOT Act.

Despite these controls, it appears that the United States continues to remain deficient in this area according to FATF, particularly as it relates to investment advisers, real estate agents and professional service providers (e.g., attorneys, accountants). For additional guidance, please refer to the sections: Financial Action Task Force, Mutual Evaluations: Methodology and Reports, BSA Reporting Requirements, Beneficial Owners, Nonbank Financial Institutions and Nonfinancial Businesses and Professional Service Providers.

2809. How has the United States addressed its deficiencies in its AML/CFT system in recent years?

The United States has published advisories, guidance or proposed or enacted regulations to address these and other noted vulnerabilities within its AML/CFT system. These include, but are not limited to, the following:

- To address the lack of commitment to compliance efforts and accountability:
  - Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (FinCEN's Advisory issued in August 2014)
  - Individual Accountability for Corporate Wrongdoing (Memorandum issued by Department of Justice (DOJ) (Yates Memo) issued in September 2015)
- To address vulnerabilities related to beneficial owners of legal entities and ongoing due diligence requirements:
  - Customer Due Diligence Requirements for Financial Institutions (FinCEN's final rule issued in July 2016)
- To address vulnerabilities in financial institutions not subject to AML/CFT Program and Customer Identification Program (CIP) requirements:
  - Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks lacking a Federal Functional Regulator (FinCEN's Notice of Proposed Rulemaking [NPRM] issued in August 2016)
- To address wholesale "de-risking:"
  - Risk Management Guidance on Foreign Correspondent Banking (Office of the Comptroller of the Currency [OCC] in October 2016)

- Financial Institution Letters: Statement on Providing Banking Services (Federal Deposit Insurance Corporation [FDIC] in January 2015)

- To address vulnerabilities in the real estate industry:
  - Geographic Targeting Order (GTO) requiring title insurance companies to collect and report purchases of residential real property over a specified amount (e.g., US$500,000 to US$3 million) in specified cities and counties of California, Florida, New York and Texas, made without external financing (e.g., bank loan) that partially used currency or monetary instruments (e.g., cashier's check, traveller's check, money order) (issued in July 2016, renewed in February 2017)
  - Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Housing Government-Sponsored Enterprises (GSEs) (FinCEN's Final Rule issued in February 2014)
  - Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators (FinCEN's Final Rule issued in April 2012)
- To address vulnerabilities with cyber-related attacks:
  - Cyber-Related Sanctions Program (Implemented by the Office of Foreign Assets Control [OFAC] in December 2015)
- To address vulnerabilities in nonbank financial systems such as money services businesses (MSB) and emerging value transfer systems (e.g., prepaid access, virtual currency):
  - Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017 (A bill introduced by the U.S. Senate in May 2017; Section 13 proposed amending the definition of monetary instrument to include funds stored in a digital format [(e.g., prepaid access devices, virtual currency]).
  - Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies (FinCEN's Guidance published in March 2013)
  - Bank Secrecy Act Regulations: Definition of "Monetary Instrument" (FinCEN's Proposed Rule issued in October 2011; proposed amending the definition of monetary instrument to include select tangible prepaid access devices for purposes of Report of International Transportation of Currency or Monetary Instruments [CMIR] requirements)
  - Definitions and Other Regulations Relating to Prepaid Access (FinCEN's Final Rule issued in July 2011)
- To address vulnerabilities related to bulk cash smuggling and trade-based money laundering (TBML) schemes:

  - Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML (FinCEN's Advisory issued in August 2014; also related to the following preceding advisories:
    - Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency (FinCEN Advisory issued in June 2010)
    - Information on Narcotics and Bulk Currency Corridors (FinCEN's Advisory issued in April 2011)
    - Update on U.S. Currency Restrictions in Mexico (FinCEN's Advisory issued in July 2012)
    - Supplement on U.S. Currency Restrictions on Banks in Mexico (FinCEN's Advisory issued in September 2013)
  - CMIR Guidance for Common Carriers of Currency, including Armored Car Services (FinCEN's Guidance issued in August 2014)

- To address vulnerabilities in cross-border funds transfers:
  - Cross-Border Electronic Transmittals of Funds (CBETF) (FinCEN Proposed Rule issued in September 2010)

- To improve how to measure progress:
  - Reformatted SAR Stats (formerly The SAR Activity Review By the Numbers), a compilation of numerical data gathered from the FinCEN Suspicious Activity Reports (SARs) with downloadable data made available for further analysis

- To address financial inclusion:
  - Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers (Request for Information issued by the Consumer Financial Protection Bureau [CFPB] in June 2014)

In some instances, states are ahead of the federal government in proposing and implementing AML/CFT laws and regulations that address emerging risks and other regulatory areas. Examples from New York State include, but are not limited to, the following:

- BitLicense Regulatory Framework for Virtual Currency Firms (Department of Financial Services (DFS) State Regulation proposed in July 2014 and finalised in June 2015)
- Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certification (DFS finalised in 2016)
- Part 500 – Cybersecurity Requirements for Financial Services Companies (DFS regulation finalised in 2017)

For further guidance on Part 504, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications section.

2810. How can multinational financial conglomerates manage their AML/CFT compliance efforts?

For multinational financial conglomerates subject to different AML/CFT requirements for each of their diverse business areas, as well as each jurisdiction in which they operate, the coordination of AML/CFT compliance efforts can be particularly challenging. Even further, common requirements do not necessarily mean common implementation or enforcement.

Institutions will benefit from AML/CFT compliance efforts being as consistent as possible throughout their global operations by, for example, adopting common standards for customer due diligence and enhanced sue diligence and risk assessments. While full consistency is not desirable (e.g., because one jurisdiction may have far more burdensome requirements) or simply cannot be achieved due to the differing business and jurisdictional requirements, the most efficient AML/CFT Compliance Program can be developed by an institution's headquarters to incorporate as many common characteristics as possible. The program then can be further customised across different businesses and jurisdictions to include the specific requirements of those businesses/countries.

Whenever possible and permissible under governing privacy and data transmission laws, centralisation of key monitoring functions, or at least internal sharing of monitoring results among global compliance departments, allows an institution to take a holistic approach to the AML/CFT Compliance Program.

2811. Should multinational institutions organise their AML/CFT compliance functions the same way in every jurisdiction in which they operate?

To the extent feasible, there are advantages to having a consistently designed AML/CFT compliance function in every jurisdiction in which a financial institution operates. However, it is important to note that regulatory bodies in some jurisdictions have strong views on how compliance functions are organised and to whom the AML Officer reports; in these cases, it is important to make adjustments to respect the local requirements and expectations.

2812. What are some obstacles to establishing a global AML/CFT Compliance Program?

One of the biggest challenges in establishing a global AML/CFT Compliance Program is adopting one global standard that meets the specific requirements of each country's AML/CFT laws and regulations. Although the overarching goal is very similar, the individual requirements are different. Global institutions typically implement a global policy with minimum requirements, often dictated by the location of the head office, and adopt local procedures at international locations. It can be difficult for the other offices to meet minimum standards if they are set too high, especially if local resources lack the requisite experience and knowledge and if their local competitors are not implementing such tight controls.

Multinational institutions also are facing the challenge of implementing transaction-monitoring systems on an enterprise level. Systems may need to apply custom rules/parameters to each jurisdiction and accommodate different time zones and currencies.

Another potential obstacle that multinational institutions must consider is the different privacy/data transmission laws and regulations that may exist in the jurisdictions in which the company operates. In some cases, these privacy regulations restrict the use of information and/or cross-border movement of information and may impose significant data protection fines for violations (e.g., General Data Protection Regulation [GDPR]).

Preparing for examinations and responding to regulators across the globe can prove difficult, because even when requirements are similar, understanding the nuances, examination approaches and foci can be minefields for the most seasoned compliance officer.

For guidance on AML/CFT requirements for U.S. financial institutions, please refer to the sections: Bank Secrecy Act, USA PATRIOT Act and Nonbank Financial Institutions and Nonfinancial Businesses.

2813. How do the FATF Recommendations address international cooperation?

FATF Recommendations 36 – 40 address international cooperation. Countries are encouraged to ratify international conventions/treaties and develop a legal basis (e.g., sign treaties, enter a memorandum of understanding [MOU]) to provide mutual legal assistance (e.g., information sharing, freezing of assets, extraditions) to other countries (e.g., financial institutions, FIUs, supervisors, law enforcement) in relation to money laundering and terrorist financing proceedings.

Further details on the roles and key guidance of the United Nations, the Egmont Group, FATF and other key international groups are provided below.

Financial Action Task Force

FATF Basics

2814. What is the Financial Action Task Force (FATF)?

Established in 1989, FATF is an intergovernmental policy-making body composed of more than 30 countries whose purpose is to establish and promote international legislative and regulatory standards in the areas of money laundering, terrorist financing and other related threats; and to monitor members' progress in adhering to these standards. Among other things, FATF works to identify trends to disseminate to the global community for combating money laundering, terrorist financing and the financing of the proliferation of weapons of mass destruction (WMDs).

Additional information on FATF membership standards and current members is included below.

2815. Who leads FATF?

FATF is led by an appointed president who is chosen from among the member countries and supported by the FATF Secretariat, which is housed in Paris, France, at the headquarters of the Organisation for Economic Co-operation and Development (OECD). The FATF president serves one 12-month term.

2816. How does FATF establish international standards for combating money laundering and terrorist financing?

FATF achieves this by hosting plenaries with members multiple times a year and by creating awareness through its publications, such as:

- The FATF Recommendations: International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferations (which replaced the "Forty plus Nine Recommendations") (February 2012);
- Methodology: For Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems (February 2013);
- FATF Public Statements on High-Risk Jurisdictions of Concern (Various dates);
- Various typology and best practices reports (Various dates); and
- Mutual Evaluation Reports (MERs) of member nations (Various dates).

2817. How are decisions made within FATF?

All decisions are made by consensus in plenary meetings by members of FATF. The plenary meetings are assisted by the FATF Secretariat and chaired by the FATF president.

2818. What does FATF hope to achieve by developing its standards and issuing the Recommendations?

FATF has several goals including, but not necessarily limited to:

- Supporting legal/criminal justice systems and law enforcement
- Creating consistency in institutional/regulatory systems for combating money laundering and terrorist financing
- Developing preventive measures that should be taken by financial institutions and certain businesses and professionals
- Fostering international cooperation

2819. How many countries are members of FATF?

Membership is not restricted to countries. Regional organisations can also be members of FATF (e.g., European Commission, Gulf Co-Operation Council). FATF began with 16 members. There are currently more than 30 members. A list of members and observers is available on the FATF website: http://www.fatf-gafi.org/about/membersandobservers/.

2820. With what bodies has FATF collaborated to assist in implementing the Recommendations?

In addition to its Members, FATF collaborates with the following FATF Associate Members, including, but not limited to:

- Asia/Pacific Group on Money Laundering (APG)
- Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) (formerly PC-R-EV)
- Grupo de Acción Financiera de Sudamerica (Financial Action Task Force of South America Against Money Laundering) (GAFISUD)
- Middle East and North Africa Financial Action Task Force (MENAFATF)
- Caribbean Financial Action Task Force (CFATF)
- Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Inter Governmental Action Group Against Money Laundering in West Africa (GIABA)

FATF also has close partnerships with the International Monetary Fund (IMF), the World Bank (WB), the United Nations (U.N.), the Egmont Group, the Group of International Finance Centre Supervisors (GIFCS) and other multinational organisations.

2821. How often has FATF updated its Recommendations?

Since its initial issuance in 1990, FATF has updated its Recommendations four times, in 1996, 2001, 2003 and 2012. The updated FATF Recommendations address the following general areas of a country's AML/CFT system:

- Anti-Money Laundering (AML), Combating the Financing of Terrorism (CFT) and Combating the Financing of Weapons of Mass Destruction (WMDs) policies and coordination
- Money laundering and confiscation
- Terrorist financing and financing of proliferation
- Preventive measures to be taken by financial institutions and other designated non-financial businesses and professions (DNBFPs)
- Transparency and beneficial ownership of legal persons and arrangements
- Powers and responsibilities of competent authorities and other institutional measures
- International cooperation

The FATF Recommendations have been recognised by the IMF, the WB and other multinational organisations as setting international standards for combating money laundering and the financing of terrorism and the proliferation of WMDs. For further guidance, please refer to The FATF Recommendations section.

2822. How are FATF and the Recommendations relevant to U.S. financial institutions?

The United States is a founding member of FATF; therefore, a number of U.S. AML/CFT statutes and regulations are influenced by the FATF Recommendations. For further guidance on how U.S.

AML/CFT laws correspond to FATF Recommendations, please refer to The FATF Recommendations section.

In addition, FATF has the authority to issue a MER of the United States, as a FATF member. The results of the MERs may serve as a catalyst for additional AML/CFT-related rulemaking and/or regulatory guidance. For further guidance on MERs, please refer to the Mutual Evaluations: Methodology and Reports section.

2823. Why did FATF consolidate the Forty plus Nine Recommendations?

FATF, since its inception, has continually adapted its guidance to address new and emerging threats. FATF and other FSRBs determined that consolidation of the Forty plus Nine Recommendations was required in order to clarify and strengthen many existing obligations, increase consistency among jurisdictions' application and implementation of AML/CFT measures, as well as to enforce the Recommendations.

2824. What are the consolidated Recommendations called?

The consolidated Recommendations are simply referred to as "The FATF Recommendations." A specific Recommendation may be referred to by its consolidated number (e.g., consolidated Recommendation 12). A conversion table of the FATF Recommendations is available in The FATF Recommendations section.

2825. What are the benefits of implementing the FATF Recommendations?

There are a number of benefits that a country derives from adherence to the FATF Recommendations including, but certainly not limited to, the following:

- Securing a more transparent and stable financial system;
- Reducing volatility of international capital flows and exchange rates, market disparities and stabilising investment and trade flows;
- Reducing vulnerabilities to infiltration, exploitation or abuse by organised crime groups;
- Implementing tools and resources that support the facilitation of tracking and monitoring illicit funds;
- Supporting international cooperation through participation in binding international obligations;
- Avoiding the risk of sanctions or other actions by the international community; and
- Protecting a country's financial system from becoming a haven for criminals.

2826. Does FATF have enforcement or investigative authority t over its members?

No. FATF has no enforcement or investigative authority. The FATF Recommendations are not rules but rather policies aimed at influencing international AML/CFT standards. While many countries have made a political commitment to fight money laundering and terrorist financing by implementing the Recommendations, and FATF may assess a country's adherence to the Recommendations through

mutual evaluations, the MERs are not reports which a country has an obligation to respond to or address. As a practical matter, however, companies may use the results of the MERs as one input to assessing a country's risk of money laundering and terrorist financing, which does exert some pressure on countries to address shortcomings. For further guidance, please refer to the Mutual Evaluations: Methodology and Reports section.

All potentially suspicious activity should be reported to local investigative authorities (e.g., Financial Crimes Enforcement Network [FinCEN]), not to FATF.

2827. How does FATF monitor new money laundering and terrorist financing methods and trends?

Annually, FATF invites experts from law enforcement and regulatory authorities of member countries to share information on significant money laundering and terrorist financing cases and operations. This exercise helps to identify and describe current money laundering trends and effective countermeasures. Findings are summarised and then released in periodic reports made available on FATF's website. Recent topics include, but are not limited to, the following:

- ML/TF risk assessment methodologies (e.g., national risk assessment)
- Proliferation of weapons of mass destruction (WMDs)
- Anti-corruption and politically exposed persons (PEPs)
- High-risk payment methods (e.g., virtual currency, prepaid cards, mobile payments)
- High-risk professional service providers (e.g., legal professionals)
- High-risk entities vulnerable to terrorist financing (e.g., nonprofit organisations)
- Trade-based money laundering (TBML) (e.g., diamonds)
- Alternative remittance systems (e.g., hawalas)
- Asset recovery
- Voluntary tax compliance programs
- De-Risking (e.g., managing versus avoiding inherent risks of correspondent banking)
- Financial inclusion

2828. What guidance has FATF provided?

Key publications issued by FATF include, but are not limited to, the following:

- **International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations** – The Forty Recommendations, last updated in 2012, are aimed at establishing AML/CFT best practices for jurisdictions, regulators and market participants. For additional guidance, please refer to The FATF Recommendations section.

- **Mutual Evaluation Reports (MERs)** – The mutual evaluation process is designed to evaluate technical compliance with the Forty Recommendations and the overall effectiveness of a country's AML/CFT system. MERs detail the findings of each country's mutual evaluation. For additional guidance on the mutual evaluation process, please refer to the Mutual Evaluations: Methodology and Reports section.
- **Methodology**: **For Assessing Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems** – Revised Methodology published in 2013 to assess technical compliance with the Forty Recommendations and the overall effectiveness of a country's AML/CFT system. For additional guidance, please refer to Mutual Evaluations: Methodology and Reports section.
- **FATF Annual Report** – A publication created annually that summarises the key achievements of FATF and its members, a summary of emerging risks, and strategic outcomes in the fight against money laundering and terrorist financing.
- **FATF Public Statements on High-Risk Jurisdictions of** Concern – Public statements that identify jurisdictions with strategic deficiencies after reviews of the AML/CFT system are conducted by FATF or a member organisation. Public statements include suggested measures for mitigating risks associated with transactions involving identified jurisdictions.
- **Typologies Report** – A publication created annually that summarises recent studies on various topics relating to money laundering and terrorist financing and conclusions of the annual meeting of select money laundering and terrorist financing experts.
- **Global Money Laundering and Terrorist Financing Threat Assessment** – A publication released in 2010 that presents a global overview of the systematic ML and TF threats, their potential negative impacts, and suggested steps for governments to take to mitigate the harm caused by these threats.
- **High-Level Principles and Objectives for FATF and FATF-Style Regional Bodies** – A publication released in 2012 that provides principles (e.g., autonomy, reciprocity) and objectives (e.g., participation in mutual evaluations, contributions to typology reports, establishment of governance structures) that govern the relationship between FATF and FATF-Style Regional Bodies (FSRBs).
- **AML/CFT-Related Data and Statistics** - This guidance released in October 2015 provides a non-exhaustive list of options for using statistics as a complement to qualitative data in the assessment of AML/CFT systems, as well as advice on how to analyse AML/CFT-related statistics and gives concrete examples of statistics that may be useful to assess the effectiveness of AML/CFT systems under the FATF 2013 methodology for assessing Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) systems he methodology.
- Guidance on a Risk-Based Approach to Combating Money Laundering and Terrorist Financing
    - **National Money Laundering and Terrorist Financing Risk Assessment** – A publication released in 2013 that provides guidance on the development and

execution of a risk assessment on a country or national level. Guidance includes the three stages of a risk assessment: identification, analysis and evaluation. Four examples of national-level assessments are provided: Australia, the Netherlands, Switzerland and the United States.

- **Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing** – A publication created in July 2007 that provides high-level guidance for developing a risk-based approach to combating money laundering and terrorist financing.
- **Money Laundering and Terrorist Financing Risk Assessment Strategies** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing.
- **Terrorism Financing: Regional Risk Assessment 2016** – This regional risk assessment for the South East Asia & Australia region, published by Australia's financial intelligence agency (AUSTRAC) and its Indonesian counterpart financial intelligence unit, Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), identifies primary terrorism financing risks from across a broad spectrum of assessed risks to focus on the highest priority risks, including: self-funding from legitimate sources, at-risk nonprofit organisations, cross-border movement of funds/value, and external funding into the region.
- **Guidance for a Risk-Based Approach: The Banking Sector** – This guidance, released in October 2014 and revises the 2007 risk-based approach guidance for the financial sector, outlines the principles involved in applying a risk-based approach to AML/CFT and seeks to assist countries, competent authorities and banks in the design and implementation of a risk-based approach to AML/CFT by providing general guidelines and examples of current practice. The guidance, which is specific to the banking sector, supports the effective implementation and supervision of national AML/CFT measures, by focusing on risks and on mitigation measures; and supports the development of a common understanding of what the risk-based approach to AML/CFT entails.
- **Guidance for a Risk-Based Approach for Money or Value Transfer Services** – A publication created in February 2016 that provides guidance to: MVTS providers on how to evaluate AML/CFT risks; MVTS supervisors on how to conduct risk-based monitoring and supervision of MVTSs; and banks on risk-based due diligence standards for MVTS customers.
- **Guidance for a Risk-Based Approach: Effective Supervision and Enforcement by AML/CFT Supervisors of the Financial Sector and Law Enforcement** – This FATF-issued guidance, published in October 2015, describes the features of effective supervision by regulators and supervisors and clarifies the interplay with the role of law enforcement agencies using a range of illustrative case

examples that aim to assist jurisdictions in undertaking effective supervision of their financial sector.

- **Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services** - A publication created in June 2013 that provides high-level guidance for developing a risk-based approach to addressing the ML and TF risks of new payment products and services (NPPS) (e.g. prepaid cards, mobile payments, electronic money, digital currencies).
- **RBA Guidance for Trust and Company Service Providers (TCSPs)** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing for TCSPs (e.g., acting as a formation agent of legal persons; acting as [or arranging for another person to act as] a director or secretary of a company; providing a registered office; acting as [or arranging for another person to act as] a trustee of an express trust; acting as [or arranging for another person to act as] a nominee shareholder for another person).
- **RBA Guidance for Real Estate Agents** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing for real estate agents.
- **RBA Guidance for Accountants** – A publication created in June 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing for accountants.
- **High Level Principles and Procedures for Dealers in Precious Metals and Dealers in Precious Stones** – A publication created in July 2008 that provides guidance on developing a risk-based approach to combating money laundering and terrorist financing in the precious metals and precious stones industries.
- **Risk-Based Approach Guidance for Legal Professionals** – A publication created in October 2008 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing for legal professionals.
- **Risk-Based Approach for Casinos** – A publication created in December 2008 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing for casinos.
- **Guidance for Money Services Businesses – Risk-Based Approach** – A publication created in July 2009 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing in money services businesses (MSBs).
- **Risk-Based Approach for the Life Insurance Sector** – A publication created in October 2009 that provides guidance on the development of a risk-based approach to combating money laundering and terrorist financing in the insurance sector.

- Reports on Specific Sectors/Industries
  - **Money Laundering/Terrorist Financing Risks and Vulnerabilities Associated with Gold –** Using a series of case studies and red flag indicators, this joint FATF-Asia/Pacific Group report, published in July 2015, identifies the many features that make gold attractive to criminals to use as a vehicle for money laundering and raises awareness of the key vulnerabilities of gold and the gold market, particularly with anti-money laundering/countering the financing of terrorism practitioners, and companies involved in the gold industry.
  - **Best Practices: Combating the Abuse of Non-Profit Organisations (Recommendation 8)** – FATF Recommendation 8 requires that the laws and regulations that govern nonprofit organisations (NPOs) be reviewed so that these organisations cannot be abused for the financing of terrorism. This paper, published in June 2015, provides an overview of the FATF best practices for preventing misuse of NPOs for the financing of terrorism while, at the same time, respecting legitimate actions of NPOs. **Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals** – A publication created in June 2013 that details the vulnerabilities of legal professionals (e.g., attorneys, notaries) that includes examples of abuse (e.g., misuse of client accounts, creation and management of legal entities, property purchases) and risk indicators about clients, attorneys, source of funds and retainers.
  - **The Role of Hawalas and Other Similar Service Providers in Money Laundering and Terrorist Financing** – A publication created in October 2013, which details vulnerabilities of hawalas and other similar service providers (HOSSPs).
  - **Money Laundering and Terrorist Financing through Trade in Diamonds** – A publication created in October 2013, which details the vulnerabilities of the diamond trade, including how diamonds can be used in trade-based money laundering (TBML).
  - **Illicit Tobacco Trade** – A report released in June 2012 to FATF and related international governing bodies detailing the risks posed by the global illicit tobacco trade.
  - **Money Laundering Using Trust and Company Service Providers** – A publication created in October 2010 that provides comprehensive analysis and evaluation of the effectiveness of FATF's Forty plus Nine Recommendations in relation to TCSPs, their role in the detection, prevention and prosecution of money laundering and terrorist financing, and the potential need for additional international requirements or sector-specific international standards.
  - **The Misuse of Corporate Vehicles, Including Trust and Company Service Providers** – A publication created in October 2006 that details the methods of abusing corporate vehicles in money laundering and terrorist financing.

- **Money Laundering and Terrorist Financing Through the Real Estate Sector** – A publication created in May 2008 that details the vulnerabilities of the real estate sector.
- **Money Laundering of Casinos and Gaming Sector Report** – A publication created in March of 2009 that details the vulnerabilities of casinos and the gaming sector.
- **Money Laundering through the Football Sector** – A publication created in July 2009 that details the vulnerabilities of major sports organisations (e.g., football).
- **Money Laundering and Terrorist Financing in the Securities Sector** – A publication created in October 2009 that details the vulnerabilities of securities firms.
- **Combating the Abuse of Non-Profit Organisations: International Best Practices Paper** – Guidance related to Special Recommendation VIII – Non-Profit Organisations, created in 2002, that summarises best practices to managing the risks of nonprofit organisations.

- Reports Related to Various Payment Methods/Channels
  - **FATF Report: Money Laundering Through the Physical Transportation of Cash** – Published in October 2015, this joint FATF/Middle East & North Africa Financial Action Task Force (MENAFATF) report identifies the main challenges that law enforcement, customs and other agencies face to detect and disrupt the physical transportation of cash. Based on analysis of data from over 60 countries, the report contains a number of real case studies to illustrate the techniques used to transport cash across borders as well as red flags indicators to be used by all agencies.
  - **Guidance for a Risk-Based Approach: Virtual Currencies** – Following on from a preliminary assessment of the ML/TF risks of virtual currencies in June 2014, this FATF guidance published in June 2015, focuses on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers.
  - **Virtual Currencies: Key Definitions and Potential AML/CFT Risks** – A publication created in June 2014 which details key definitions and the various types and vulnerabilities of virtual currencies (e.g., Bitcoin).
  - **International Best Practices: Detecting and Preventing the Illicit Cross-Border Transportation of Cash and Bearer Negotiable Instruments** – Guidance related to Special Recommendation IX, created in 2010, that summarises the best preventive measures with regard to cross-border transport of monetary instruments.
  - **Money Laundering Using New Payment Methods** – A publication created in 2010 that summarises key risk factors that can be used to assess new payment

methods (NPM), case studies and typologies involving NPMs and the ongoing challenges faced in developing appropriate legislation and regulations.

- **Trade-Based Money Laundering** – A publication created in June 2006 that details the vulnerabilities of the international trade system.
- **Report on New Payment Methods** – A publication created in October 2006 that details the vulnerabilities of emerging payment methods, including prepaid cards, internet payment systems, mobile payments and digital precious metals.
- **Money Laundering (ML) and Terrorist Financing (TF) Vulnerabilities of Commercial Websites and Internet Banking Systems** – A publication created in July 2008 that details the vulnerabilities of electronic commerce.
- **Money Laundering Vulnerabilities of Free Trade Zones** – A publication created in March 2010 that details the vulnerabilities of more than 3,000 "free trade zones" – designated areas within countries that offer a free trade environment with minimal regulation – in more than 130 countries.
- **Combating the Abuse of Alternative Remittance Systems: International Best Practices** – A publication created in June 2003, which details the vulnerabilities of alternative remittance systems, also known as informal value transfer systems (IVTS).
- **Combating the Abuse of Alternative Remittance Systems: International Best Practices Paper** – Guidance related to Special Recommendation VI: Alternative Remittance, created in 2004, which summarises best practices to managing the risks of alternative remittance systems.

- Reports Related to Terrorism
  - **FATF Report: Emerging Terrorist Financing Risks** – The Emerging Terrorist Financing Risks report, published in October 2015, explores the emerging terrorist financing threats and vulnerabilities posed by foreign terrorist fighters (FTFs), fundraising through social media, new payment products and services, and the exploitation of natural resources.
  - **FATF Report: Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL)** – FATF's report on the financing of the Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL), published in February 2015, analyses how this terrorist organisation generates and uses its funding, and highlights a number of new and existing measures to disrupt ISIL financing.
  - **FATF Report: Financial Flows Linked to the Production and Trafficking of Afghan Opiates** – A publication released in June 2014 that provides an overview of drug trafficking of opiates through Afghanistan and the interrelationship between drug trafficking and terrorist financing.

- **International Best Practices: Targeted Financial Sanctions Related to Terrorism and Terrorist Financing (Recommendation 6)** – A publication created in June 2013, which details best practices for implementing financial sanctions (e.g., freezing of assets) of designated persons in accordance with FATF Recommendation 6 and relevant United Nations Security Council Resolutions (UNCSRs).
- **FATF Report: Terrorist Financing in West Africa** – A publication created in October 2013, in collaboration with the Inter Governmental Action Group against Money Laundering in West Africa (GIABA) that identifies typologies related to terrorism and terrorist financing in West Africa and general observations of the regions' AML/CFT efforts.
- **FATF Report: Risk of Terrorist Abuse in Non-Profit Organisations** – A publication released in June 2014 that details the vulnerabilities of nonprofit organisations to abuse by terrorists (e.g., raising of funds, diversion of funds, use of logistical networks and programs to garner ideological support for recruitment).
- **Guidance for Financial Institutions in Detecting Terrorist Financing** – A publication created in 2002 that provides guidance to financial institutions in detecting terrorist financing, including, but not limited to, account opening and transaction red flags, common sources of funds for terrorist organisations (e.g., kidnapping, extortion, use of nonprofit organisations as front companies, skimming from legitimate businesses).
- **FATF Terrorist Financing Report** – A publication created in February 2008 that analyses the methods of raising and moving funds between terrorist organisations. The report also covers suggested controls for mitigating the risks of this activity.

- Reports Related to Non-Proliferation of WMDs
  - **Typologies of Proliferation Financing** – A publication created in August 2008 that analyses the threat of "proliferation financing" – financing that facilitates the movement and development of proliferation-sensitive items (e.g., weapons of mass destruction [WMDs]) by exploiting global commerce by masking acquisitions as legitimate trade, abusing free trade zones and operating in countries with weak export controls. The report covers methods of financing and suggested controls for mitigating the risks of this activity.
  - **FATF Guidance: The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction** – A publication created in June 2013 that consolidates previous guidance on the implementation of FATF Recommendation 7 – Targeted Financial Sanctions Related to Proliferation and UNSCRs related to weapons of mass destruction (WMDs).

- **Best Practices Paper: Sharing Among Domestic Competent Authorities Information Related to the Financing of Proliferation –** A publication created in February 2012 which details best practices for information and exchange related to WMDs in accordance with Recommendation 2 – National Cooperation and Coordination.

- Reports Related to Corruption and Transparency
  - **FATF Guidance: Transparency and Beneficial Ownership** – This FATF guidance from October 2014 aims to assist countries to design and implement measures that will deter and prevent the misuse of corporate vehicles, such as companies, trusts and other types of legal persons and arrangements, for money laundering, terrorist financing and other illicit purposes.
  - **Best Practices Paper: The Use of FATF Recommendations to Combat Corruption** – A publication created in October 2013 that builds on past FATF guidance on corruption and politically exposed persons (PEPs) and summarises anti-corruption best practices identified by AML/CFT and anti-corruption experts in partnership with the G20 Anti-Corruption Working Group (ACWG). Topics covered include relevant AML/CFT measures for combating corruption; key risk factors; best practices for cooperation and examples of successful coordination and cooperation efforts.
  - **FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)** – A publication created in June 2013 which details best practices for detecting and conducting due diligence on PEPs in accordance with Recommendation 12 – Politically Exposed Persons and Recommendation 22 – DNFBPs: Customer Due Diligence. Topics covered include foreign and domestic PEPs; beneficial ownership; sources of information used to detect and identify PEPs; red flags for potentially suspicious activity and examples of abuse (e.g., use of corporate vehicles to obscure ownership).
  - **Corruption: A Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight against Corruption** – A publication created in October 2012 which details how to use the FATF Recommendations to combat corruption. Topics covered include identifying politically exposed persons (PEPs); safeguarding and increasing transparency of financial systems; detecting, investigating and prosecuting corruption; and money laundering and recovering stolen assets.
  - **Specific Risk Factors in the Laundering of Proceeds of Corruption** – Assistance to Reporting Institutions – A publication created in June 2012 specifically to help reporting institutions in better analysing and understanding risk factors for corruption-related money laundering, including politically exposed persons (PEPs).

- **Laundering the Proceeds of Corruption** – A publication created in July 2011 that describes links between corruption and money laundering drawn from publically available expert resources and identifies key vulnerabilities within the current AML/CFT framework.

- Reports Related to Asset Confiscation, Tax Programs and Other Topics
  - **Best Practices Paper: Best Practices on Confiscation (Recommendations 4 and 38) and a Framework for Ongoing Work on Asset Recovery** – A publication created in October 2012 which details best practices in the implementation of an effective confiscation and asset recovery infrastructure in an international context in accordance with Recommendation 4 – Confiscation and Provisional Measures and Recommendation 38 – Mutual Legal Assistance: Freezing and Confiscation.
  - **Best Practices Paper: Confiscation (Recommendations 3 and 38)** – Guidance related to Recommendation 3 – Provisional Measures and Confiscation, and Recommendation 38 – Mutual Legal Assistance and Extradition, created in 2010, that summarises methods of effective tracing and confiscation within each jurisdiction and internationally.
  - **International Best Practices: Freezing of Terrorist Assets** – Guidance related to Special Recommendation III – Freezing and Confiscating Terrorist Assets, created in 2009, that summarises effective methods of freezing terrorist-related funds or other assets.
  - **Best Practices Paper: Managing the Anti-Money Laundering and Counter-Terrorist Financing Policy Implications of Voluntary Tax Compliance Programmes** – A publication created in October 2012, which outlines best practices for implementing voluntary tax compliance programs (VTC) that do not impede AML/CFT efforts. The publication details the vulnerabilities of VTCs, particularly when repatriating assets (e.g., lack of due diligence on repatriated funds).
  - **FATF Guidance: Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion** – A publication created in February 2013 that outlines how to implement an effective AML/CFT system without impeding access of legitimate businesses and underserved consumers from the formal financial system. Topics covered include vulnerable groups (e.g., low income, rural, undocumented) and the flexibility of the risk-sensitive application of FATF Recommendations in low-risk scenarios.
  - **Organised Maritime Piracy and Related Kidnapping for Ransom** – A publication created in July 2011 that examines the financial impact of these crimes, and current challenges with tracing the illicit flows associated with maritime piracy and kidnapping for ransom.

- **Money Laundering Risks Arising from Trafficking of Human Beings and Smuggling of Migrants** – A study published in July 2011 describing the money flows from these issues and their potential scale.
- **FATF Guidance on Anti-Money Laundering and Terrorist Financing Measures and Financial Inclusion** – A publication released in June 2012 providing guidance on how governments can balance their national goal of financial inclusion of financially underserved populations without compromising measures taken to combat money laundering and terrorist financing efforts.
- **Operational Issues Financial Investigations Guidance** – A publication created in June 2012 that provides guidance on how to enhance the functions, responsibilities, powers and tools of law enforcement to effectively conduct money laundering, terrorist financing and asset-tracing investigations.
- **Consolidated FATF Standards on Information Sharing: Relevant Excerpts from the FATF Recommendations and Interpretive Notes –** A publication created in June 2016 that provides guidance on: minimum due diligence standards for basic and beneficial ownership; the sharing of information within the private sector, between the public and private sectors, among public authorities in various contexts (e.g., implementation of financial sanctions, processing wire transfers, conducting investigations, providing mutual legal assistance); and assessing the effective implementation of FATF standards on information sharing mechanisms.

The FATF Recommendations

Recommendation Basics

2829. What are the key sections of the FATF Recommendations?

The FATF Recommendations are organised into seven main categories:

- **AML/CFT Policies and Coordination (Recommendations 1 and 2)** – Provides guidance on how to assess risks and apply a risk-based approach in developing an AML/CFT framework and how parties (e.g., financial institutions, regulatory authorities, law enforcement) can share information and coordinate efforts with each other, domestically and internationally.
- **Money Laundering and Confiscation (Recommendations 3 and 4)** – Advises countries to criminalise money laundering and apply it to the widest range of predicate offenses; provides guidance on legislative measures to enable authorities to freeze, seize or confiscate proceeds and property from money laundering and terrorist financing.
- **Terrorist Financing and Financing of Proliferation (Recommendations 5 through 8)** – Advises countries to criminalise terrorist financing and designate terrorist financing as a money laundering predicate offense; provides guidance on the legislative measures to designate and delist targets and to enable authorities to freeze funds or assets of designated targets subject to sanctions related to terrorism, terrorist financing and proliferation of weapons of mass destruction (WMDs);

encourages countries to review laws and regulations that relate to nonprofit organisations to evaluate their adequacy in guarding against abuse for the financing of terrorism.

- **Preventive Measures (Recommendations 9 through 23)** – Advises countries to modify secrecy laws to enable implementation of FATF's Recommendations (e.g., to facilitate information sharing between appropriate authorities); outlines several measures or controls for financial institutions to mitigate risks and prevent money laundering and terrorist financing, including:
  - Risk assessments to identify vulnerabilities and appropriate controls to mitigate the risks associated with new customers, products and business practices including new delivery mechanisms.
  - Development of an enterprisewide program, including policies on information sharing, consistently applied across foreign branches and subsidiaries, with enhanced measures for those located in high-risk jurisdictions;
  - Risk-based due diligence (e.g., collection of information at account opening and ongoing, verification of identity, reporting of suspicious transactions, obtaining senior management approval) on customers and beneficial owners, with enhanced measures for politically exposed persons, correspondent banks and money or value transfer services (MVTS) also known as money services businesses (MSBs);
  - Ability to stop (e.g., freeze, seize, confiscate) transaction(s)/asset(s) if it involves a designated target subject to sanctions;
  - Reporting of suspicious transactions to financial intelligence units (FIU) with measures to ensure confidentiality and to protect financial institutions from criminal and civil liability (i.e., Safe Harbor);
  - Recordkeeping to permit reconstruction of transaction(s) and, if necessary, to provide evidence for prosecution of criminal activity, including, but not limited to, originator/beneficiary information in wire transfers;
  - Development of policies that outline the conditions in which a financial institution may rely upon a third party to perform due diligence on its behalf; and
  - Due diligence requirements for designated non-financial businesses and professions (DNFBP) (e.g., casinos, real estate agents, dealers in precious metals and stones, attorneys, accountants, trust service providers).
- **Transparency and Beneficial Ownership of Legal Persons and Arrangements (Recommendations 24 and 25)** – Provides guidance on measures to prevent the misuse of legal persons or legal arrangements (e.g., trusts) for money laundering and terrorist financing, including bearer shares or bearer share warrants, by facilitating the collection of and access to beneficial ownership and control information;
- **Powers and Responsibilities of Competent Authorities and Other Institutional Measures (Recommendations 26 through 35)** – Provides guidance on the development of an effective AML/CFT system, including, but not limited to:

- Designation of competent and empowered authorities to supervise financial institutions and DNFBPs for compliance with AML/CFT laws and regulations with a risk-based approach;
- Establishment of a financial intelligence unit (FIU) as the central agency to receive and analyse required reporting (e.g., suspicious transaction reporting, large currency transactions, disclosures of cross-border movement of currency and negotiable instruments) and disseminate guidance, statistics and feedback to relevant authorities in a secure and confidential process;
- Designation of competent and empowered law enforcement authorities with the responsibility of conducting domestic and international money laundering and terrorist financing investigations, and the authority to identify, trace and initiate freezing and seizing of assets;
- Establishment of a large currency transaction reporting requirement above a fixed amount, domestically and internationally;
- Establishment of a declaration or disclosure system to detect cross-border transportation of currency and bearer negotiable instruments (BNI), also referred to as monetary instruments;
- Establishment of sanctions (e.g., civil, criminal, administrative penalties) for non-compliance with AML/CFT laws and regulations for financial institutions, DNFBPs and senior management.

- **International Cooperation (Recommendations 36 through 40)** – Countries are encouraged to ratify international conventions/treaties and develop a legal basis (e.g., sign treaties, memorandum of understanding (MOU)) to provide mutual legal assistance (e.g., information sharing, freezing of assets, extraditions) to other countries (e.g., financial institutions, FIUs, supervisors, law enforcement) in relation to money laundering and terrorist financing proceedings. Suggested treaties include:
  - United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention, 1988);
  - United Nations Convention Against Transnational Organised Crime (Palermo Convention, 2000);
  - The United Nations Convention Against Corruption, 2003;
  - The International Convention for the Suppression of the Financing of Terrorism (the Terrorist Financing Convention, 1999); and
  - Other relevant treaties where applicable.

2830. What were the major changes between the Forty plus Nine Recommendations and the consolidated FATF Recommendations?

There were no significant changes to the content or objectives of the FATF Recommendations. The changes were a consolidation of the Forty plus Nine Recommendations, and reorganisation into categories that are more consistent with emerging money laundering and terrorist financing trends.

The following table shows how the current FATF Recommendations correspond to the previous Forty plus Nine Recommendations and where they are discussed in this publication.

No.	Section	Category	Recommendation	Former Number	U.S. AML/CFT FAQ Guide Topics
1*	A	AML/CFT Policies and Coordination	Assessing risks and applying a risk-based approach	NA	• The Fundamentals • Risk Assessments: Enterprisewide, Horizontal, Line of Business/Legal Entity, Geographic, Product/Services, Customer
2	A	AML/CFT Policies and Coordination	National cooperation and coordination	R.31	• The Fundamentals: Overview of the U.S. Regulatory Framework • USA PATRIOT Act: 314 – Cooperative Efforts to Deter Money Laundering
3	B	Money Laundering and Confiscation	Money laundering offense	R.1 and R.2	• The Fundamentals: Overview of U.S. AML/CFT Laws
4*	B	Money Laundering and Confiscation	Confiscation and provisional measures	R.3	• Office of Foreign Assets Control and International Sanctions Programs
5*	C	Terrorist Financing and Financing of Proliferation	Terrorist financing offense	SRII	• The Fundamentals: Overview of U.S. AML/CFT Laws
6*	C	Terrorist Financing and Financing of Proliferation	Targeted financial sanctions related to terrorism and terrorist financing	SRIII	• OFAC: Counter Terrorism Sanctions Program
7*	C	Terrorist Financing and Financing of Proliferation	Targeted financial sanctions related to proliferation	NA	• OFAC: Non-Proliferation Sanctions Program
8*	C	Terrorist Financing and Financing of Proliferation	Nonprofit organisations	SRVIII	• Know Your Customer Types: Charitable Organisations and Nongovernmental Organisations

No.	Section	Category	Recommendation	Former Number	U.S. AML/CFT FAQ Guide Topics
9	D	Preventive Measures	Financial institution secrecy laws	R.4	• The Fundamentals: Overview of U.S. AML/CFT Laws • USA PATRIOT Act: Section 314 – Cooperative Efforts to Deter Money Laundering
10*	D	Preventive Measures	Customer due diligence	R.5	◦ USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts ◦ USA PATRIOT Act: Section 326 – Verification of Identification ◦ Know Your Customer, Customer Due Diligence and Enhanced Due Diligence
11	D	Preventive Measures	Recordkeeping	R.10	◦ Bank Secrecy Act: BSA Recordkeeping Requirements
12*	D	Preventive Measures	PEPs	R.6	◦ USA PATRIOT Act: Section 312 – Senior Foreign Political Figure ◦ Know Your Customer Types: Politically Exposed Persons

No.	Section	Category	Recommendation	Former Number	U.S. AML/CFT FAQ Guide Topics
13	D	Preventive Measures	Correspondent banking	R.7	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act Section 313 – Prohibition on U.S. Correspondent Accounts with Foreign Shell Banks • USA PATRIOT Act Section 319 - Forfeiture of Funds in United States Interbank Accounts (Foreign Bank Certifications) • Know Your Customer Types: Correspondent Banking
14*	D	Preventive Measures	Money or value transfer services	SRVI	• Nonbank Financial Institutions: Money Services Businesses
15	D	Preventive Measures	New technologies	R.8	• Know Your Customer's Activities: Product Considerations: Electronic Banking and Digital Value
16*	D	Preventive Measures	Wire transfers	SRVII	• BSA: Funds Transfer Recordkeeping Requirement and the Travel Rule • Know Your Customer's Activities: Product Considerations: Funds Transfers
17*	D	Preventive Measures	Reliance on third parties	R.9	• Know Your Third Parties
18*	D	Preventive Measures	Internal controls and foreign branches and subsidiaries	R.15 and R.22	• USA PATRIOT Act: Section 352 - AML Program
19*	D	Preventive Measures	Higher-risk countries	R.21	• Geographic Risk Assessments
20*	D	Preventive Measures	Reporting of suspicious transactions	R.13 and SRIV	• Suspicious Activity Reports

No.	Section	Category	Recommendation	Former Number	U.S. AML/CFT FAQ Guide Topics
21	D	Preventive Measures	Tipping-off and confidentiality	R.14	• SARs: Confidentiality & Safe Harbor
22*	D	Preventive Measures	DNFBPs: Customer due diligence	R.12	• Nonbank Financial Institutions and Nonfinancial Businesses
23*	D	Preventive Measures	DNFBPs: Other measures	R.16	• Nonbank Financial Institutions and Nonfinancial Businesses
24*	E	Transparency and Beneficial Ownership of Legal Persons and Arrangements	Transparency and beneficial ownership of legal persons	R.33	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act: Section 326 – Verification of Identification • Beneficial Owners
25*	E	Transparency and Beneficial Ownership of Legal Persons and Arrangements	Transparency and beneficial ownership of legal arrangements	R.34	• USA PATRIOT Act: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts • USA PATRIOT Act: Section 326 – Verification of Identification • Beneficial Owners
26*	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Regulation and supervision of financial institutions	R.23	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
27	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Powers of supervisors	R.29	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
28	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Regulation and supervision of DNFBPs	R.24	• Nonbank Financial Institutions and Nonfinancial Businesses

No.	Section	Category	Recommendation	Former Number	U.S. AML/CFT FAQ Guide Topics
29*	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Financial Intelligence Units	R.26	• The Fundamentals: Financial Crimes Enforcement Network (FinCEN)
30*	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Responsibilities of law enforcement and investigative authorities	R.27	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
31	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Powers of law enforcement and investigative authorities	R.28	• The Fundamentals: Key U.S. Regulatory Authorities and Law Enforcement Agencies
32*	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Cash couriers	SRIX	• BSA: Report of International Transportation of Currency or Monetary Instruments (CMIR) • Know Your Customer's Activities: Product Considerations: Bulk Shipments of Currency and Bulk Cash Smuggling
33	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Statistics	R.32	• Suspicious Activity Reports: SAR Statistics and Trends
34	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Guidance and feedback	R.25	• Suspicious Activity Reports: SAR Statistics and Trends
35	F	Powers and Responsibilities of Competent Authorities and Other Institutional Measures	Sanctions	R.17	• The Fundamentals: Enforcement Actions
36	G	International Cooperation	International instruments	R.35 and SRI	• The Fundamentals: Overview of U.S. AML/CFT Laws
37	G	International Cooperation	Mutual legal assistance	R.36 and SRV	• International Perspectives and Initiatives

No.	Section	Category	Recommendation	Former Number	U.S. AML/CFT FAQ Guide Topics
38*	G	International Cooperation	Mutual legal assistance: Freezing and confiscation	R.38	• Office of Foreign Assets Control and International Sanctions Programs • International Perspectives and Initiatives
39	G	International Cooperation	Extradition	R.39	• International Perspectives and Initiatives
40*	G	International Cooperation	Other forms of international cooperation	R.40	• International Perspectives and Initiatives

FATF Recommendations with an asterisk (*) also have interpretive notes which provide further guidance.

For additional guidance on how the United States applies AML/CFT requirements to the various types of financial and nonfinancial institutions, please refer to the sections: Bank Secrecy Act, USA PATRIOT Act, and Nonbank Financial Institutions and Nonfinancial Businesses.

2831. Are the FATF Recommendations applicable only to financial institutions?

No. The FATF Recommendations are applicable to DNFBPs and regulatory and law enforcement authorities in addition to financial institutions.

2832. Which of the FATF Recommendations are applicable to financial institutions?

All of the FATF Recommendations affect financial institutions, either directly through specific guidance for customer due diligence (CDD) programs, recordkeeping and suspicious transaction reporting or indirectly by establishing the legal and regulatory frameworks in which financial institutions must operate. The FATF Recommendations related directly to CDD, recordkeeping and suspicious transaction reporting are Recommendations 9 through 25.

Key FATF Definitions with Comparisons to U.S. Definitions

2833. What are FATF's "designated categories of offenses for money laundering"?

As part of its ongoing efforts to identify new methods of money laundering and the associated sources of illicit funds, in 2012 FATF added "Tax Offenses" to the list of potential predicate crimes. Otherwise, the term "designated categories of offenses for money laundering" is defined as activities that should be considered as predicate crimes to money laundering. FATF's designated categories of offenses include the following:

- Participation in an organised criminal group and racketeering
- Terrorism, including terrorist financing

- Trafficking in human beings and migrant smuggling
- Sexual exploitation, including sexual exploitation of children
- Illicit trafficking in narcotic drugs and psychotropic substances
- Illicit arms trafficking
- Illicit trafficking in stolen and other goods
- Corruption and bribery
- Fraud
- Counterfeiting currency
- Counterfeiting and piracy of products
- Environmental crime
- Murder, grievous bodily injury
- Kidnapping, illegal restraint and hostage-taking
- Robbery or theft
- Smuggling (including in relation to customs and excise duties and taxes)
- Tax crimes (related to direct taxes and indirect taxes)
- Extortion
- Forgery
- Piracy
- Insider trading and market manipulation

2834. Should all categories of offenses be included within a country's definition of predicate offenses?

Each country decides, in accordance with its domestic law, the range of offenses to be covered as predicate offenses under each of the above categories. Some countries have opted to define these offenses by listing activities designated as serious offenses, by minimum penalty of imprisonment (e.g., one year imprisonment), or by a combination of these approaches.

2835. How does the U.S. list of predicate crimes compare to that outlined by FATF?

The United States lists hundreds of specified unlawful activities (SUAs) including 20 of the 21 designated categories of predicate offenses recommended by FATF, including, but not limited to, the following:

- Racketeering activity (e.g., any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter or dealing in a controlled substance or listed

chemical as defined by the Controlled Substances Act), which is chargeable under state law and punishable by imprisonment for more than one year;

- Terrorist financing;
- Counterfeiting (e.g., currency, goods);
- Fraud (e.g., securities fraud, wire fraud);
- Slavery, trafficking in persons and alien smuggling;
- Illegal arms sales (e.g., chemical weapons, nuclear material); and
- Illegal gambling.

Tax crimes are not SUAs, although tax evasion with income from legitimate sources is considered a predicate crime for money laundering in the United States, if intent to violate federal law can be proven.

For further guidance on tax-related disclosures and programs, please refer to the Report of Foreign Bank and Financial Accounts and Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act sections.

2836. What is dual criminality? How is it important to prosecuting transnational criminal activity?

In many circumstances, dual criminality, where the illicit activity is considered a predicate offense to money laundering in both countries (e.g., crime occurred in one country, proceeds from the crime detected in another country), may be required to facilitate mutual legal assistance, and ultimately prosecution for money laundering.

With the globalisation of the world economy, the rise of transnational organised crimes and the focus on foreign corruption, mechanisms to coordinate international cooperation (e.g., Recommendation 2 – National Cooperation and Coordination, Recommendations 36 – 40 related to International Cooperation) to combat money laundering and terrorist financing is imperative more than ever.

2837. How does FATF define "financial institution"?

FATF defines the term "financial institution" as any person or entity who/that conducts, as a business, one or more of the following activities or operations for, or on behalf of, a customer:

- Acceptance of deposits and other repayable funds from the public (inclusive of private banking)
- Lending (e.g., consumer credit, mortgage credit, factoring)
- Financial leasing (not including financial leasing arrangements in relation to consumer products)
- The transfer of money or value, in both the formal and informal or underground sectors (i.e., informal value transfer systems)
- Issuing and managing means of payment (e.g., credit and debit cards, checks, traveller's checks, money orders, banker's drafts, electronic money)

- Financial guarantees and commitments
- Trading in:
    - Money market instruments (e.g., checks, bills, CDs, derivatives)
    - Foreign exchange
    - Exchange, interest rate and index instruments
    - Transferable securities
    - Commodity futures trading
- Participation in securities issues and the provision of financial services related to such issues
- Individual and collective portfolio management
- Safekeeping and administration of cash or liquid securities on behalf of other persons
- Otherwise investing, administering or managing funds or money on behalf of other persons
- Underwriting and placement of life insurance and other investment-related insurance (applies to both insurance undertakings and to insurance intermediaries [e.g., agents, brokers])
- Money and currency changing

2838. How does FATF define "designated nonfinancial businesses and professions"?

FATF defines designated nonfinancial businesses and professions (DNFBPs) as the following:

- Casinos (including online casinos)
- Real estate agents
- Dealers in precious metals
- Dealers in precious stones
- Lawyers, notaries, other independent legal professionals and accountants
    - Refers to sole practitioners, partners or employed professionals within professional firms; it is not meant to refer to professionals who are employees of other types of businesses, nor to professionals working for government agencies who already may be subject to measures that would combat money laundering and terrorist financing
- Trust and company service providers
    - Refers to all persons or businesses who are not covered elsewhere under the Recommendations, and which, as a business, provide any of the following services to third parties:
        - Acting as a formation agent of legal persons

- Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
- Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
- Acting as (or arranging for another person to act as) a trustee of an express trust
- Acting as (or arranging for another person to act as) a nominee shareholder for another person

2839. Should all financial institutions and DNFBPs described above be subject to the Recommendations?

A country may decide that the application of a measure is not necessary, either fully or partially, to a particular type or size of financial institution. For example, in the United States, quantitative thresholds are included in some of the definitions of financial institutions that are subject to AML/CFT requirements (e.g., an MSB must conduct US$1,000 or more in MSB activity with the same person [in one type of activity] on the same day to be subject to AML/CFT requirements).

However, if a country decides to limit the scope of financial institutions obligated to comply with AML/CFT requirements, the reasoning must be justified and risk-based (i.e., low risk for money laundering and terrorist financing).

2840. How does the BSA's definition of "financial institution" compare to that outlined by the FATF?

The BSA's definition largely parallels the FATF guidance except that, as indicated in the 2016 MER of the United States, it does not include professional service providers such as lawyers, notaries and other independent legal professionals and accountants. The USA PATRIOT Act significantly expanded "financial institutions" so that the definition includes, but is not necessarily limited to:

- Depository institutions (e.g., insured banks, private banks, credit unions, thrift and savings institutions, commercial banks or trust companies, agencies or branches of foreign banks in the United States)
- Broker-dealers registered or required to register with the Securities and Exchange Commission (SEC)
- Securities/commodities broker-dealers
- Futures commission merchants (FCMs), introducing brokers (IBs), commodity pool operators (CPOs) and commodity trading advisers (CTAs) registered or required to register under the Commodity Exchange Act (CEA)
- Investment bankers or investment companies

- Casinos (State-licensed or Indian) with annual gaming revenue of more than US$1 million
- Money services businesses (e.g., licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally; currency exchanges; issuer or seller of traveller's checks, money orders or similar instruments; sellers or providers of prepaid access)
- Operators of credit card systems
- Insurance companies
- Dealers in precious metals, precious stones or jewels
- Pawnbrokers
- Loan or finance companies (e.g., nonbank residential mortgage lenders or originators (RMLO))
- Travel agencies
- Telegraph companies
- Businesses engaged in vehicle sales, including automobile, airplane and boat sales
- Persons involved in real estate closings and settlements
- The U.S. Postal Service
- Agencies of the federal government or any state or local government carrying out a duty or power of a business described in the definition of a "financial institution"
- Any business or agency that engages in any activity that the Secretary of the Treasury determines, by regulation, to be an activity that is similar to, related to, or a substitute for any activity in which any of the above entities are authorised to engage (e.g., housing government-sponsored enterprises [GSE])
- Any other business designated by the U.S. Secretary of the Treasury, with cash transactions that have a high degree of usefulness in criminal, tax or regulatory matters.

The U.S. has not issued AML/CFT regulations for a number of NBFIs even though they are defined as financial institutions under the USA PATRIOT Act. For additional guidance on how the United States applies AML/CFT requirements to the various types of financial and nonfinancial institutions, please refer to the sections: Bank Secrecy Act, USA PATRIOT Act, and Nonbank Financial Institutions and Nonfinancial Businesses.

Although not required to maintain an AML Program, professional service providers are subject to select BSA reporting requirements (e.g., Form 8300, Report of International Transportation of Currency or Monetary Instruments (CMIR), Report of Foreign Bank and Financial Accounts (FBAR)). Additionally, assuming they are U.S. persons, professional service providers are required to comply with the Office of Foreign Assets Control (OFAC) laws and regulations. For further guidance, please refer to the Professional Service Providers section.

2841. How does FATF define "money or value transfer services (MVTS)"?

FATF defines MVTS as "financial services that involve the acceptance of cash, checks, other monetary instruments or other stores of value and the payment of a corresponding sum in cash or other form to a beneficiary by means of a communication, a message, a transfer or through a clearing network to which the MVTS provider belongs."

FATF uses the term new payment products and services (NPPS) to describe some of the product offerings of MVTS (e.g., prepaid cards, mobile payments, electronic money, digital currencies).

The term hawalas and other similar service providers (HOSSPs) are used to describe informal value transfer systems (IVTS).

2842. How does the BSA's definition of MVTS compare to that outlined by FATF?

The BSA uses the term "money services business (MSB)" to describe businesses that provide MVTS/NPPS services. MSB activities parallel those outlined by FATF and include the following:

- **Issuer or seller of traveller's checks or money orders** – A person that:
  - "Issues traveller's checks or money orders that are sold in an amount greater than US$1,000 to any person on any day in one or more instances or
  - Sells traveller's checks or money orders in an amount greater than US$1,000 to any person on any day in one or more transactions."
- **Check casher –** A person that accepts checks or monetary instruments in return for currency or a combination of currency and other monetary instruments or other instruments, in an amount greater than US$1,000 for any person on any day in one or more transactions.
- **Dealer in foreign exchange** – A person that "accepts the currency, or other monetary instruments, funds, or other instruments denominated in the currency, of one or more countries in exchange for the currency, or other monetary instruments, funds or other instruments denominated in the currency, of one or more countries in an amount greater than US$1,000 for any other person on any day in one or more transactions, whether or not for same-day delivery."
- **Providers of prepaid access –** The participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access (provider). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program.
- **"Prepaid access" is defined as "**Access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number." Prepaid access applies to a very broad range of prepaid services, including but not limited to open-loop prepaid access, closed-loop prepaid access, prepaid access

given for the return of merchandise, and many prefunded employee programs such as a Health Savings Account.

- **Sellers of prepaid access** – Any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if:
  - That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or
  - That person sells prepaid access (including closed-loop prepaid access) to funds that exceeds US$10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales.
- **Money transmitter** – A money transmitter is defined as the following:
  - Any person engaged in the transfer of funds
  - A person who provides money transmission services
- "**Money transmission services**" is defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means."
- "**By any means**" includes money transmission through the following:
  - A financial agency or institution;
  - A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both;
  - An electronic funds transfer network; or
  - An informal value transfer system.
  - U.S. Postal Service – "The United States Postal Service except with respect to the sale of postage or philatelic products" (e.g., stamp-related collectible products)

For further guidance on MSBs and other IVTSs, please refer to the Money Services Businesses section.

2843. How does FATF define "bearer negotiable instrument (BNI)"?

FATF defines bearer negotiable instruments (BNIs) as "monetary instruments in bearer form such as: traveller's checks; negotiable instruments (including checks, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including checks, promissory notes and money orders) signed, but with the payee's name omitted."

Additionally, bearer shares refer to "negotiable instruments that accord ownership in a legal person to the person who possesses the bearer share certificate."

2844. How does the BSA's definition of BNI compare to that outlined by FATF?

The BSA uses the term "monetary instruments" to describe BNIs. The definition of monetary instruments varies based on the specific AML/CFT requirement. For example, for the Report of International Transportation of Currency or Monetary Instruments (CMIR), monetary instruments are defined as:

- Coin or currency of the United States or of any other country;
- Traveller's checks in any form;
- Negotiable instruments (e.g., checks, promissory notes, money orders) in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery;
- Incomplete instruments (including checks, promissory notes, and money orders) that are signed but on which the name of the payee has been omitted; and
- Securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery.

For CMIRs, monetary instruments do not include:

- Checks or money orders made payable to the order of a named person which have not been endorsed or which bear restrictive endorsements;
- Warehouse receipts; or
- Bills of lading.

For the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, monetary instruments include:

- Bank check or draft
- Foreign draft
- Cashier's check
- Money order
- Traveller's check

For further guidance on the AML/CFT requirements for monetary instruments, please refer to the following sections: Report of International Transportation of Currency or Monetary Instruments and Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments.

2845. Has FATF's definition for "politically exposed person" (PEP) evolved?

Yes. FATF has expanded the definition of a PEP by breaking it down into two categories: foreign PEPs and domestic PEPs.

Foreign PEPs are defined as individuals who are or have been entrusted with prominent public functions in a foreign country (e.g., heads of state, senior politicians, senior government, judicial or

military officials, senior executives of state-owned corporations, important political party officials). FATF also states that business relationships with family members or close associates of PEPs have similar reputational risks to PEPs themselves, and therefore should be included in the definition of PEP, as well.

FATF advises that the definition of PEP was not meant to include junior- or middle-ranking individuals in the categories mentioned above. FATF also suggests that persons who are or have been entrusted with a prominent function by an international organisation (e.g., deputy directors, and members of the board or equivalent functions) be considered in the definition of PEP.

Domestic PEPs are individuals who are, or have been, entrusted domestically with prominent public functions (e.g., heads of state or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials).

2846. How does the BSA's definition of beneficial owners compare to that outlined by FATF?

After the implementation of the Beneficial Ownership Rule, the first prong of the BSA's definition of "beneficial owner" parallels that outlined by FATF by applying a 25 percent threshold for determining due diligence measures, with some exceptions. Additionally, the BSA adds a second prong, the "control" prong, which may be a party who does not meet the ownership test.

Prior to the implementation of the Beneficial Ownership Rule, Section 312 of the USA PATRIOT Act required covered institutions (e.g., depository institutions, broker-dealers in securities) to conduct due diligence on beneficial owners defined as "individual[s] who [have] a level of control over [of 10 percent], or entitlement to, the funds or assets in the account that, as a practical matter, enables the individual[s], directly or indirectly, to control, manage or direct the account."

For further guidance, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts and Beneficial Owners.

2847. How does FATF define "customer due diligence"?

FATF does not specifically define "customer due diligence (CDD)." The term generally refers to any type of measure used to mitigate ML/TF risks, including, but not limited to, the following:

- Collection and verification of customer information
- Monitoring and reporting of potentially suspicious activity
- Recordkeeping and reporting of high-risk transactions or movement of funds (e.g., cross-border movement of currency or BNIs and wire transfers)

The term "simplified measures" refers to due diligence applied to low/moderate risk customers. "Enhanced measures" applies to due diligence applied to high-risk customers.

Per FATF, CDD measures should be applied at the beginning of customer relationships and ongoing.

2848. How does the BSA's definition of "customer due diligence" compare to that outlined by FATF?

Similar to FATF, the BSA does not specifically define "customer due diligence." In some instances, CDD refers to any type of measure used to mitigate ML/TF risk (e.g., collection of customer information, suspicious activity monitoring). In some instances, CDD refers only to measures to collect and verify customer information, generally referred to as Know Your Customer (KYC). These KYC measures include, but are not limited to, the following:

- USA PATRIOT Act Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts (including Politically Exposed Persons [PEPs])
- USA PATRIOT Act Section 326 – Verification of Identification (often referred to as the Customer Identification Program [CIP])

In 2014, the KYC requirements under the BSA were updated to include beneficial owners of legal entities in select instances under the rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule), which was finalised in July 2016. For further guidance, please refer to the Beneficial Owners section.

For further guidance on CIP and specialised due diligence, please refer to the sections: Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts, Section 326 – Verification of Identification and Know Your Customer, Customer Due Diligence and Enhanced Due Diligence.

2849. How does FATF define "beneficial owner"?

FATF defines "beneficial owner" as "the natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those persons who exercise ultimate effective control over a legal person or arrangement."

2850. How does the BSA's definition of "beneficial owner" compare to that outlined by FATF?

After the implementation of the Beneficial Ownership Rule, the first prong of the BSA's definition of "beneficial owner" parallels that outlined by FATF by applying a 25 percent threshold for determining due diligence measures, with some exceptions. Additionally, the BSA adds a second prong, the "control" prong, which may be a party who does not meet the ownership test.

For further guidance, please refer to the sections: Section 326 – Verification of Identification and Beneficial Owners.

2851. How does FATF define "sanctions"?

FATF uses the term "sanctions" to describe the following:

- Penalties for non-compliance with AML/CFT laws and regulations (e.g., civil, criminal, administrative).
- Targeted financial sanctions (e.g., freezing of assets) of designated persons (e.g., terrorists)

FATF is concerned with how proportionate or dissuasive penalties are, as well as their applicability to senior personnel in addition to financial institutions.

2852. How does the U.S. definition of "sanctions" compare to that outlined by FATF?

The U.S. uses the term "sanctions" to describe economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. These "sanctions" are administered by the Office of Foreign Assets Control (OFAC). For further guidance on economic and trade sanctions, please refer to the Office of Foreign Assets Control and International Sanctions Program section.

Consistent with FATF, the U.S. has outlined multiple penalties for violations and non-compliance with U.S. AML/CFT laws and regulations, including, but not limited to, the following:

- Regulatory enforcement actions;
- Civil and criminal penalties;
- Seizure and forfeiture of funds; and
- Incarceration of the individuals involved.

2853. Does FATF provide guidance on "thresholds" for determining when certain measures should be required?

FATF suggests the following thresholds as the minimum amount of a transaction (or a series of transactions) that should prompt certain AML/CFT measures (e.g., CDD, recordkeeping, or suspicious transaction reporting requirements):

- For application of the money laundering offense to predicate crimes: Recommendation 3 – Money Laundering Offense: Suggests the use of a threshold approach (e.g., term of imprisonment) to include the widest range of predicate crimes.
- For due diligence on customers executing transactions conducted by financial institutions under Recommendation 10 – Customer Due Diligence: US/EUR 15,000.
- For due diligence on customers executing cross-border wire transfers: Recommendation 16 – Wire Transfers: US/EUR 1,000.
- For due diligence on customers executing transactions conducted by casinos under Recommendation 22 – DNFBPs: Customer Due Diligence: US/EUR 3,000.
- For due diligence on customers executing transactions conducted by dealers in precious metals and stones when engaged in any cash transaction under Recommendation 22 – DNFBPs: Customer Due Diligence and Recommendation 23 – DNFBPs: Other Measures: US/EUR 15,000.
- For due diligence on customers transporting cross-border bearer negotiable instruments (BNI): Recommendation 32 – Cash Couriers: US/EU 15,000.

- For application of simplified measures on low-risk insurance products under Recommendation 10 – Customer Due Diligence: life insurance policies with annual premiums less than US/EUR 1,000; single premiums of less than US/EUR 2,500.

2854. Does the BSA utilise thresholds to determine when certain measures should be required?

Yes. The U.S. utilises thresholds for reporting (e.g., suspicious activity, large currency transactions), recordkeeping (e.g., funds transfers, monetary instruments) and activity thresholds for financial institutions subject to AML/CFT requirements. For example:

- Suspicious activity reports (SARs): US$5,000 for all financial institutions except money services businesses (MSBs) whose threshold is US$2,000.
- Currency Transaction Reports (CTRs), Reports of International Transportation of Currency or Monetary Instruments (CMIRs), Form 8300: US$10,000.
- Funds Transfers Recordkeeping Requirement: US$3,000.
- Cash purchases of monetary instruments: Between US$3,000 and US$10,000.
- Activity thresholds of "financial institutions" subject to select AML/CFT requirements:
  - MSBs: Check cashers/Issuers of traveller's checks or money orders: US$1,000.
  - Dealers in precious metals, precious stones or jewels: US$50,000.
- There is no minimum threshold for OFAC sanctions.

For further guidance, please refer to the following sections: Bank Secrecy Act and Office of Foreign Assets Control and International Sanctions Program.

2855. How are "risk assessments" defined by FATF?

FATF defines risk assessments as "a product or process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand ML/TF risks and serves as a first step in addressing them… and making judgments" about [ML/TF risks]… which are defined as "a function of three factors: threat, vulnerability and consequence."

Threat is defined by FATF as "a person or group of people, object or activity, with the potential to cause harm."

2856. How are "risk assessments" addressed by FATF?

FATF addresses risk assessments in multiple ways, including, but not limited to, the following:

- FATF Recommendations
  - Recommendation 1 – Assessing Risks & Applying a Risk-Based Approach provides guidance on how to assess risks and apply a risk-based approach (RBA) in developing an AML/CFT system.

The principles in Recommendation 1 can be used by governments/lawmakers in developing a risk-based AML/CFT system, by regulatory authorities in developing risk-based examinations and by financial institutions in developing risk-based AML/CFT Compliance Programs.

  - Other recommendations address applying measures (e.g., customer due diligence, regulatory oversight) based on risk (e.g., Recommendation 10 – Customer Due Diligence, Recommendation 19 – Higher Risk Countries, Recommendation 26 – Regulation and Supervision of Financial Institutions, Recommendation 28 – Regulation and Supervision of DNFBPs)

- Guidance on Risk Assessments – FATF provides guidance on various types of risk assessments including, but not limited to, the following:
  - Government/Lawmakers, Law Enforcement, Regulatory Authorities (e.g., National Money Laundering and Terrorist Financing Risk Assessment [2013])
  - Financial institutions and NBFIs (e.g., RBA Guidance for Casinos [2008], RBA Guidance for Money Services Businesses [2009])
  - Professional service providers (e.g., RBA Guidance for Legal Professionals [2008], RBA Guidance for Accountants [2008])
  - High-risk products and payment vehicles (e.g., Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet-Based Payment Services [2013], Virtual Currencies: Key Definitions and Potential AML/CFT Risks [2014])
- Execution of Risk Assessments
  - FATF published its first "Global Money Laundering & Terrorist Financing Threat Assessment" (GTA) in July 2010. The GTA provides a global overview of the most prevalent systemic ML/TF threats, their potential negative impacts, and suggested steps for governments to take to mitigate the harm caused by these threats.

While FATF does not explicitly address all types of assessments (e.g., proliferation of weapons of mass destruction (WMDs)), the same principles can be applied to any area of focus by identifying a clear purpose and scope for each assessment.

2857. What is "de-risking" and how has FATF addressed it?

De-risking often refers to a financial institution's policy to exit from a high-risk customer group or activity to reduce its inherent risk profile. To avoid risk, as opposed to managing risk, some financial institutions may opt out of offering services to certain categories of high-risk customers (e.g., foreign correspondents, money transmitters, marijuana-related businesses [MRBs]) or customers located in high-risk geographies. While this may reduce risk and simplify the KYC and suspicious activity monitoring programs of individual financial institutions, it may increase overall money laundering risk in the system as money is moved through less transparent or less regulated financial systems (e.g., hawalas, financial institutions in lax AML/CFT jurisdictions).

Many financial institutions have taken steps to de-risk because of perceived regulatory pressures. FATF and other international authorities, however, have released guidance cautioning against wholesale de-risking while attempting to provide further clarification on regulatory expectations on servicing inherently high-risk customers (e.g., Office of the Comptroller of the Currency [OCC] Risk Management Guidance on Foreign Correspondent Banking, Federal Deposit Insurance Corporation [FDIC] Financial Institution Letter: Statement on Providing Banking Services, Financial Action Task Force [FATF] Clarifies Risk-Based Approach: Case-by-Case, Not Wholesale De-Risking, International Monetary Fund [IMF] The Withdrawal of Correspondent Banking Relationships: A Case for Policy Action).

2858. How does the U.S. approach to "risk assessments" compare to that outlined by FATF?

In the U.S., financial institutions are expected to develop and maintain risk-based compliance programs. This requires that they conduct risk assessments. Bank regulators, in particular, expect the financial institutions they supervise to conduct, among others:

- **Enterprisewide risk assessment** – An exercise intended to identify the aggregate money laundering (ML) and terrorist financing (TF) risks facing an organisation that may not be apparent in a risk assessment focused on a line of business, legal entity, or other assessment unit. In other words, it is the big picture view, or profile, of an organisation's ML/TF risks that aggregates the results of other risk assessment exercises in order to quantify and relate the total risks for the organisation to the established risk appetite and tolerance for the enterprise.
- **Horizontal risk assessment** – An exercise intended to identify systemic ML/TF risks of designated high-risk products/services and/or customers across an organisation regardless of which line of business or legal entity owns these activities or customers.
- **Line of business/legal entity risk assessment** – An exercise intended to identify the level of vulnerability of each line of business (LOB) or legal entity (LE) to ML/TF. This is accomplished by evaluating, for a specific LOB or LE, among other factors, the ML/TF risks of products/services, the customer base (e.g., type, location) and geography (e.g., customers, transactions, operations) and the controls (e.g., policy and procedures, customer acceptance and maintenance standards, transaction monitoring, management oversight, training, personnel) mitigating those risks at the business line or legal entity level.
- **Product/service risk assessment** – An exercise intended to identify the inherent ML/TF risks of the products and services offered by a financial institution.
- **Geographic risk assessment** – An exercise intended to identify the inherent ML/TF risks of the international and domestic jurisdictions in which a financial institution and its customers conduct business.
- **Customer risk assessment** – An exercise intended to identify the level of inherent ML/TF risks in the types of customers (e.g., individual, institutional, financial institution, not-for-profit) served by a financial institution.

- **OFAC/Sanctions risk assessment** – An exercise intended to identify an organisation's level of vulnerability to noncompliance with economic sanctions administered by OFAC or any sanctions program as required by the financial institution's policy. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types, the geographic origin and destination of transactions, and the strength of the controls mitigating those risks.

For further guidance, please refer to the Risk Assessments section.

2859. Has the United States conducted a national risk assessment?

Yes. The most recent National Money Laundering Risk Assessment (NMLRA) was published in 2015 by the U.S. Treasury with input from multiple federal agencies and offices (e.g., Federal Bureau of Investigation [FBI], the Internal Revenue Service (IRS), the Drug Enforcement Administration [DEA], the Office of Foreign Assets Control [OFAC], Financial Crimes Enforcement Network [FinCEN], Immigration and Customs Enforcement [ICE], United States Secret Service [USSS]) as an update to the U.S. Money Laundering Threat Assessment (MLTA), published in 2005. The NMLRA contains detailed analyses of money laundering vulnerabilities, similar to those identified in the MLTA (2005) across banking, insurance, casinos and MSBs including, but not limited to, the following:

- Use of currency and monetary instruments (e.g., bank notes, cashier's check, money order, traveller's check) in transactions structured under regulatory recordkeeping and reporting thresholds (e.g., US$10,000 for currency transactions, US$3,000 for monetary instruments), commingled with licit funds, used in bulk cash smuggling activities and in trade-based money laundering (TBML) (e.g., Black Market Peso Exchange [BMPE]);
- Establishment of bank and brokerage accounts using nominees (i.e., agent acting by or on behalf of a third party) to disguise the identities of the individuals who control the accounts;
- Creation of legal entities (e.g., shell companies, shelf companies) without accurate information about the identity of the beneficial owner;
- Misuse of products and services (e.g., correspondent banking services, funnel accounts, omnibus accounts, remote deposit capture [RDC], prepaid access cards, virtual currency) resulting from deficient compliance with AML/CFT obligations; and
- Complicit merchants (e.g., wholesalers), third-party payment processors (TPPPs), money services businesses (MSBs) (e.g., foreign exchange dealers, money transmitters) and other financial institutions (e.g., banks, broker-dealers, casinos) with deficient compliance with AML/CFT obligations, and in some cases, wittingly facilitating illicit activity.

The National Terrorist Financing Risk Assessment (NTFRA) was also published in 2015 by the U.S. Treasury, with input from many of the same federal agencies and offices that collaborated on the NMLRA, as well as Customs and Border Protection (CBP), the Bureau of Counterterrorism, the Bureau of International Narcotics and Law Enforcement and the National Counterterrorism Center (NCTC). This report contains detailed analyses of terrorist financing vulnerabilities, including, but not limited to, the following:

- Global terrorism and terrorist financing threats

  - Terrorist threats to the United States (e.g., al-Qaeda, Al-Nusrah Front [ANF], Islamic State of Iraq and the Levant [ISIL], Hizballah, Hamas, Taliban, Haqqani Network, foreign terrorist fighters)
  - Terrorist financing sources (e.g., kidnapping for ransom [KFR], extortion, drug trafficking, private donations through charitable organisations, state sponsorship, cybercrime, identity theft) and vulnerabilities (e.g., charitable organisations, licensed and unlicensed MSBs, foreign correspondent banking, cash smuggling, virtual currency)
- Counterterrorism and CFT efforts
  - Law enforcement efforts (e.g., reorientation, interagency coordination and cooperation, information sharing)
  - Financial/regulatory efforts (e.g., Office of Foreign Assets Control [OFAC] sanctions)
  - International efforts (e.g., United Nations [UN], Financial Action Task Force [FATF])

FATF recommends that each country continues to conduct self-assessments to evaluate and ultimately mitigate money laundering and terrorist financing risks on a national level. For further guidance, please refer to the Risk Assessments section.

High-Risk and Non-Cooperative Jurisdictions

2860. What are "Non-Cooperative Countries and Territories"?

Non-Cooperative Countries and Territories (NCCT) was a term used to describe jurisdictions designated by FATF that had detrimental rules and practices that seriously hampered the international fight against money laundering and terrorist financing. Since FATF revised its International Co-operation Review Group (ICRG) procedures in 2010, the term was changed from "Non-Cooperative Countries and Territories" to "High-Risk and Non-Cooperative Jurisdictions."

2861. How does FATF define "High-Risk and Non-Cooperative Jurisdictions"?

High-Risk and Non-Cooperative Jurisdictions describe two primary groups:

- Group 1: Jurisdictions with strategic AML/CFT deficiencies subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from the jurisdictions; and
- Group 2: Jurisdictions with strategic AML/CFT deficiencies that either:
  - Have not made sufficient progress in addressing the deficiencies; or
  - Have not committed to an action plan developed with FATF to address the deficiencies.

2862. Why did FATF change from "Non-Cooperative Countries and Territories" to "High-Risk and Non-Cooperative Jurisdictions"?

In 2006, FATF removed the last country from the NCCT designation (Myanmar, formerly Burma). From 2007 through 2010, FATF continued to evaluate countries and jurisdictions, but without any being considered "non-cooperative" the focus shifted to ensuring that existing programs were effective and efficient.

In 2009, FATF issued procedures for the ICRG at the request of member countries, and in 2010 released its identification of "High-Risk and Non-Cooperative Jurisdictions."

2863. What is the difference between a "High-Risk Jurisdiction" and a "Non-Cooperative Jurisdiction"?

FATF has not articulated a clear distinction between the two designations. It appears, however, that the level of engagement and degree of cooperation demonstrated by the jurisdiction under review will determine if a jurisdiction is identified as "high-risk" or as "non-cooperative."

2864. When and where does FATF identify "High-Risk and Non-Cooperative Jurisdictions"?

FATF provides updates on designated "High-Risk and Non-Cooperative Jurisdictions" in two public documents:

- FATF Public Statements, published three times a year: in February, June and October; and
- "Improving Global AML/CFT Compliance: Ongoing Process," which is released once a year and focuses specifically on jurisdictions that have deficiencies but also a political commitment to improvement.

A list of these jurisdictions is available on the FATF website: http://www.fatf-gafi.org/topics

2865. What are the consequences of being a FATF designated High-Risk or Non-Cooperative Jurisdiction?

FATF's previous Recommendation 21 recommended that countries exercise caution and conduct enhanced due diligence when developing business relationships or conducting transactions with any person, company or financial institution from a country or territory listed as NCCTs, now referred to as "High-Risk or Non-Cooperative."

Today, the same principle applies under the new Recommendation 19: Higher-Risk Countries. As a result, a jurisdiction's designation by FATF can cause significant adverse consequences for its financial development as businesses and financial institutions will have limited access to financial world markets. Additionally, FATF calls for countries to take "countermeasures" against any listed jurisdiction not taking the necessary steps to correct their AML/CFT deficiencies.

A financial institution in the United States should review the FATF Public Statements on High-Risk and Non-Cooperative Jurisdictions to determine whether the customer located in such country or doing business in such country should be considered high-risk for purposes of its AML/CFT Compliance Program.

2866. What additional countermeasures has FATF suggested member countries take against "High-Risk or Non-Cooperative Jurisdictions" beyond Recommendation 19: Higher-Risk Countries?

FATF suggests reviewing the public reports to identify the specific deficiencies of each country, and developing countermeasures accordingly. However, in general, FATF advises that effective countermeasures include:

- Enhanced due diligence (EDD) requirements on customers and beneficial owners of individuals or businesses within designated countries before establishing account relationships
- More intensive monitoring of transactions involving designated countries
- Consideration of location of relevant designated countries' financial institutions when approving establishment of subsidiaries, branches or representative offices in member countries
- Informing nonfinancial sector businesses of the heightened money laundering and terrorist financing risk of entities within designated countries

2867. When did the process for designating countries as "High-Risk or Non-Cooperative" begin?

FATF began assessing select non-member countries and territories in 1998. It was not until 2000 that the NCCT process was formalised by the issuance of reports listing NCCTs as well as the framework, procedures and criteria used to designate NCCTs. After the last NCCT country was removed in 2006, FATF continued using MERs to assess countries based on their effectiveness and efficiency in implementing laws and sustaining measures to mitigate money laundering and terrorist financing. Additionally, FATF began issuing public statements expressing concerns over some jurisdictions. In 2009, the Group of 20 (G20) formally requested that FATF resume the process of designating high-risk jurisdictions. This process resumed in 2010, after issuing formal ICRG procedures in 2009.

2868. What is the process of designating a jurisdiction as "High-Risk or Non-Cooperative"?

In 2009, FATF established the ICRG, which produces procedures governing the reviews of select countries and territories. The review of countries by the ICRG begins with the results of a country's MER. Those with identified deficiencies are referred to the ICRG. The ICRG procedures are not published for the public; however, the MER details are outlined in the section below, and it is known that FATF continues to assess countries against the Forty plus Nine Recommendations, even though the new FATF Recommendations have been released.

2869. How are countries and territories selected for review?

Countries are selected for review based on a number of factors. The primary factor is the result of a country's MER, but in addition, FATF may consider a member's experience and the interests of other member nations when determining which countries to refer to the ICRG. Generally, larger financial centres and countries with a history of being uncooperative are reviewed first. However, FATF cautions that certain jurisdictions with deficient AML/CFT systems may not be immediately selected for review because they are not prioritised by FATF members.

2870. Who conducts the reviews of selected "High-Risk or Non-Cooperative Jurisdictions"?

FATF established the International Co-operation Review Group (ICRG), which is a specialised body with the designated responsibility of reviewing "High-Risk or Non-Cooperative Jurisdictions." The ICRG may include representatives from FATF and other regional groups (e.g., the Review Group on Asia/Pacific, the Review Group on the Americas, Europe and Africa/Middle East) consisting of representatives from FATF member governments that act as a conduit of information between the reviewed country or territory and FATF.

2871. Have countries been designated as "High-Risk or Non-Cooperative Jurisdictions" and removed as they improve their AML/CFT regime?

Yes. FATF has designated several countries as "High-Risk or Non-Cooperative Jurisdictions" (e.g., Iran, Democratic People's Republic of Korea [DPRK], Guyana). Guyana was previously designated as a jurisdiction with strategic deficiencies but has improved its AML/CFT regime and is no longer subject to FATF's ongoing monitoring process. For the most recent "High-Risk or Non-Cooperative Jurisdictions" please refer to http://www.fatf-gafi.org/countries/#high-risk.

2872. How is a country or territory removed from designation as a "High-Risk or Non-Cooperative Jurisdiction"?

Once designated, a jurisdiction must periodically report on its progress in plenary meetings (e.g., recent AML/CFT reforms, implementation plans), and submit to ongoing monitoring by the ICRG in order to first be designated as making progress in its efforts to remediate deficiencies.

FATF then performs on-site visits to ensure effective implementation of the recent AML/CFT reforms. Once the ICRG is satisfied that sufficient steps have been taken, recommendations for delisting are made at plenary meetings, and jurisdictions are identified as no longer requiring ongoing monitoring (e.g., Trinidad and Tobago in 2012, Guyana in 2016).

2873. Can a financial institution assume that a country is compliant with the FATF Recommendations or has a strong AML/CFT system if it's not listed as an NCCT or a "High-Risk or Non-Cooperative Jurisdiction"?

No. While FATF's designations help member nations to identify the countries and jurisdictions with particularly weak AML/CFT programs, the mutual evaluation process may identify instances of compliance with the Recommendations of member countries. However, if a jurisdiction is not designated by FATF as "High-Risk or Non-Cooperative," a U.S. financial institution may want to assess the volume of business activity such jurisdiction conducts with other member nations to determine the specific level of risk to which it is exposed.

2874. How does FATF deal with noncomplying members?

FATF's actions include:

- Sending a letter from the FATF president or high-level mission to the noncomplying member country to apply peer pressure so that the jurisdiction takes action to tighten its AML/CFT system

- Requiring that the noncomplying member country deliver progress reports at plenary meetings
- Referral to the ICRG for the development of corrective action plans, and continued monitoring
- Calling upon international financial institutions to perform scrutiny on business relations and transactions with persons, companies and financial institutions in the noncomplying member country
- Suspending membership

Members and Observers

2875. What criteria must be met for a country to become a member of FATF?

In order to qualify for membership in FATF, a country must:

- Be strategically important
- Be a full and active member of a relevant FSRB
- Provide a letter from a minister or a person who is of equal political level, making a political pledge to implement the Recommendations within a reasonable time frame and to be able to undergo the mutual evaluation process
- Effectively criminalise money laundering and terrorist financing
- Make it mandatory for financial institutions to identify their customers, maintain customer records and report suspicious transactions
- Establish a Financial Intelligence Unit (FIU)

2876. What is the benefit of becoming a member of FATF?

Countries and territories listed as being FATF members are recognised as being compliant, or largely compliant, with international AML/CFT practices. Membership in FATF, therefore, provides comfort that a jurisdiction is operating under a sound AML/CFT system; however, it is not a guarantee that all of the companies operating in that jurisdiction are fully compliant with all requirements.

2877. What is an observer of FATF?

Being an observer can be the first step on the path toward becoming a member of FATF. Observers include FSRBs with similar functions to FATF. Some FATF members are also members of these organisations. Some are international organisations that have specific money laundering missions or functions.

2878. How does a country or territory become an observer of FATF?

To receive observer status, a country or territory must first make a request to FATF for consideration. The potential observer must have an AML/CFT system (e.g., criminal and regulatory framework) in place or plans for the development of such an infrastructure. The observer status can only be granted

by the consensus of FATF members at one of the organisation's three annual meetings. A list of members and observers is available on the FATF website: www.fatf-gafi.org.

2879. How can a country transition from being an observer to membership in the FATF?

The process of an observer obtaining member status takes approximately two years and depends on the results of a mutual evaluation. For additional guidance on mutual evaluations, please see the Mutual Evaluations: Methodology and Reports section.

2880. What are FSRBs?

FSRBs are international bodies and organisations that have observer status with FATF. Some FATF members are also members of FSRBs.

Mutual Evaluations: Methodology and Reports

2881. How does FATF ensure that all of its member countries are in compliance with the FATF Recommendations?

FATF relies heavily on the various enforcement agencies within each country (e.g., within the United States, it would be FinCEN and the federal financial regulators such as the Office of the Comptroller of the Currency [OCC], and the Federal Deposit Insurance Corporation [FDIC]). In addition, FATF members agree to conduct mutual evaluations of their AML/CFT systems to ensure compliance with the Recommendations. Each member agrees to be evaluated by an internationally accepted assessment methodology.

Within FATF, the Working Group on Evaluations and Implementation (WGEI) administers the mutual evaluation process. They monitor, coordinate and review the mutual evaluation procedures, develop interpretation and provide guidance to the Recommendations, develop and coordinate the training of new assessors, and serve as the point of contact between FATF, the GIFCS, the IMF and the WB.

2882. Has FATF released guidance on the mutual evaluation process?

Yes. FATF published "Methodology: Assessing the Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT Systems" in February 2013. This guidance provides an overview of the assessment methodology used in evaluations/assessments, descriptions of what is necessary for an effective AML/CFT system, and guidance and interpretation concerning the methodology.

Does the MER assess or evaluate anything besides compliance with the FATF Recommendations?

Yes. Through assessment of adherence to the FATF Recommendations, FATF is also able to perform an in-depth evaluation of a country's system for preventing criminal abuse of the financial system; it helps FATF to quantify each country's risk exposure to money laundering and terrorist financing, among other financial crimes.

2883. Did the process for mutual evaluations change along with the consolidated FATF Recommendations?

The mutual evaluation process is designed to measure and evaluate the implementation progress of the FATF Recommendations. Since the FATF Recommendations were consolidated, and fundamentally remain unchanged, the evaluation process largely remains the same, with the exception of the updated methodology to evaluate compliance and overall effectiveness. The mutual evaluation process involves the following:

- The completion of a mutual evaluation questionnaire, a self-assessment exercise in which each member country provides information on the status of its implementation of the FATF Recommendations;
- An on-site visit, in which each member country is examined for compliance and effectiveness by a select team of legal, financial and law enforcement experts from other member governments;
- The preparation of a MER describing the findings and the effectiveness of the member country's AML/CFT system, which is made available on the FATF website; and
- Submission of follow-up reports two years after the evaluation indicating the member country's progress since the mutual evaluation, with particular focus on the areas of improvement identified in the mutual evaluation.

2884. How are updates on progress provided after a mutual evaluation is conducted?

For some countries that have already received a MER, FATF issues a "Follow-Up Report to the Mutual Evaluation Report," which frequently highlights a country's progress in implementing corrective action to address deficiencies and further develop enhancements to laws, regulatory expectations, control processes and so forth, for adherence to the FATF Recommendations.

2885. How long does the mutual evaluation process take?

The mutual evaluation process takes approximately 10 months to one year to complete per country. This includes the time it takes for the jurisdiction to complete the pre-on-site self-assessment questionnaire, and for the reviewers to conduct the on-site visit, draft the preliminary and final reports and discuss findings with FATF and the country under review. The timeline varies slightly from one evaluation to the next. It may be affected by factors such as the date at which the plenary will next meet and endorse the final draft report.

2886. Who conducts the mutual evaluation?

Mutual evaluations are conducted by FSRBs, the IMF and the WB. Each evaluation team consists of a minimum of four experts, plus two members of the FATF Secretariat. This includes:

- One member with legal expertise (e.g., judge, prosecutor)
- Two members with financial sector expertise (e.g., regulator) and experience with both financial institutions and DNFBPs

- One law enforcement professional (e.g., police, customs, FIU)

Additional experts may be added, depending on the size or complexity of the country under review.

The evaluation team typically consists of members drawn from countries that have a history, understanding and close relationship with the country being evaluated.

2887. How are the assessors trained to conduct mutual evaluations?

A five-day training session is provided for prospective assessors by FATF, FSRBs, the IMF and the WB to ensure assessors have the same level of knowledge to conduct the assessment.

2888. Who is interviewed by the assessors? How are they selected?

The FATF Evaluation Team interviews representatives from ministries, criminal justice and operational entities, and financial sector bodies selected across geographic regions as well as industry lines (e.g., casinos, insurance industry). A detailed program for the on-site visit portion of a mutual evaluation is devised in consultation with the country being evaluated. The details of the meeting (e.g., timing, interviewees) are determined with consideration to the particular nature of the country, its risks and industries.

2889. Are the results of the mutual evaluation available to the public?

Yes. In 2005, FATF began publishing the MERs on its website: www.fatf-gafi.org. Today, FATF is publishing the "Follow-Up Report to the Mutual Evaluation Report" for countries already reviewed at least once, and continues to publish MERs for countries that have not previously been evaluated (e.g., new member countries).

2890. Have there been any changes to the rating scale used to assess compliance with the consolidated FATF Recommendations?

Yes. FATF utilises two rating scales to measure technical compliance with the FATF Recommendations and overall effectiveness of the AML/CFT system. FATF still uses the following rating scale to assess technical compliance with the Recommendations:

- **Compliant** – The Recommendation is fully observed with respect to all criteria.
- **Largely Compliant** – There are only minor shortcomings, with a large majority of the essential criteria being fully met.
- **Partially Compliant** – The country has taken some substantive steps and complies with some of the essential criteria.
- **Noncompliant** – There are major shortcomings with a large majority of essential criteria not being met.
- **Not Applicable** – A requirement, or part of the requirement, does not apply due to structural, legal or institutional features of the country.

2891. What key factors are used when assessing compliance with the FATF Recommendations?

While the categories have changed slightly with the consolidation of the FATF Recommendations, the key factors used when assessing compliance largely remain the same. It is important to note that the FATF Recommendations are applicable to criminal justice systems and regulatory authorities in addition to financial institutions. Different factors are considered when assessing applicable FATF Recommendations relevant to each area.

The following factors may be considered to assess overall compliance of a country's AML/CFT system with the FATF Recommendations:

- Range of money laundering and terrorist financing predicate offenses
- Evidentiary standards applied to money laundering/terrorist financing offenses
- Number and nature of precondition(s) required prior to providing mutual assistance (e.g., dual criminality, treaty, secrecy provisions)
- Quantity and quality of Suspicious Transaction Reports (STRs)
- Number of money laundering/terrorist financing investigations initiated
- Number of prosecutions
- Number of convictions
- Existence of penalties for failures of compliance
- Number and amount of penalties
- Existence of mechanisms to freeze/seize criminal proceeds
- Existence of sanctions for failure to freeze/confiscate assets
- Number of cases where sanctions have been applied
- Number and amount of frozen/seized assets
- Number of resources within regulatory and law enforcement authorities
- Expertise of resources
- Number, frequency and duration of examinations conducted by regulatory authorities
- Failures identified in financial institutions in examinations by regulatory authorities
- Information sharing (e.g., between FIU, financial institutions, law enforcement)
- Quality of coordination between financial institutions, regulatory and law enforcement authorities

2892. What rating scale is used to assess the effectiveness of an AML/CFT system?

The following rating scale is used to assess effectiveness, defined by FATF as "the extent to which the defined outcomes are achieved":

- **High Level of Effectiveness** – Minor improvements needed; the Immediate Outcome is achieved to a large extent.
- **Substantial Level of Effectiveness** – Moderate improvements needed; the Immediate Outcome is achieved to a large extent.
- **Moderate Level of Effectiveness** – Major improvements needed; the Immediate Outcome is achieved to some extent.
- **Low Level of Effectiveness** – Fundamental improvements needed; the Immediate Outcome is not achieved or achieved to a negligible extent.

2893. What are "Immediate Outcomes" and "Intermediate Outcomes"?

FATF defines "Immediate Outcomes" as the 11 desired outcomes of an effective AML/CFT system with respect to the "high-level objective" of protecting financial systems and the economy "from the threats of money laundering and the financing of terrorism and proliferation, thereby strengthening financial sector integrity and contributing to safety and security." These include the following:

- ML and TF risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation of WMDs.
- International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.
- Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks.
- Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.
- Legal persons and arrangements are prevented from misuse for ML or TF, and information on their beneficial ownership is available to competent authorities without impediments.
- Financial intelligence and all other relevant information are appropriately used by competent authorities for ML and TF investigations.
- ML offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.
- Proceeds and instrumentalities of crime are confiscated.
- TF offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.
- Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the nonprofit organisations (NPO) sector.
- Persons and entities involved in the proliferation of WMDs are prevented from raising, moving and using funds, consistent with the relevant United Nations Security Council Resolutions (UNSCRs).

"Intermediate Outcomes" refers to the following:

- Policy, coordination and cooperation mitigate ML and TF risks.
- Proceeds of crime and funds in support of terrorism are prevented from entering the financial and other sectors or are detected and reported by these sectors.
- ML threats are detected and disrupted, and criminals are sanctioned and deprived of illicit proceeds. TF threats are detected and disrupted, terrorists are deprived of resources, and those who finance terrorism are sanctioned, thereby contributing to the prevention of terrorist acts.

2894. What are the key factors used when assessing effectiveness of an AML/CFT system?

When evaluating effectiveness, assessors are instructed to consider the aforementioned technical compliance factors and two overarching questions:

- To what extent is the Outcome being achieved?
- What can be done to improve effectiveness?

For each Outcome, the following is also provided to assist assessors in evaluating overall effectiveness:

- Characteristics of an effective system; and
- Core issues to be considered in determining if the Outcome is being achieved including examples of specific information and factors that could support the conclusions on core issues.

2895. What have been the results of MERs conducted in recent years?

The Fourth Round uses the updated methodology which was adopted in 2013 to incorporate the 2012 update to the Recommendations. The following table summarises the ratings of the most recent Fourth Rounds Assessments which were published between 2014 and 2016:

Technical Compliance						
No.	Recommendation	Non-Compliant (NC)	Largely Compliant (LC)	Compliant (C)	Partially Compliant (PC)	N/A
R1	Assessing Risks and Applying a Risk-Based Approach	16%	29%	3%	52%	0%
R2	National Cooperation and Coordination	3%	35%	23%	39%	0%
R3	Money Laundering Offence	3%	61%	23%	13%	0%
R4	Confiscation and Provisional Measures	0%	58%	29%	13%	0%

Technical Compliance						
No.	**Recommendation**	**Non-Compliant (NC)**	**Largely Compliant (LC)**	**Compliant (C)**	**Partially Compliant (PC)**	**N/A**
R5	Terrorist Financing Offence	6%	48%	26%	19%	0%
R6	Targeted Financial Sanctions Related to Terrorism and Terrorist Financing	16%	29%	16%	39%	0%
R7	Targeted Financial Sanctions Related to Proliferation	39%	19%	6%	35%	0%
R8	Non-Profit Organisations	23%	39%	3%	35%	0%
R9	Financial Institution Secrecy Law	0%	23%	74%	3%	0%
R10	Customer Due Diligence	3%	45%	10%	42%	0%
R11	Recordkeeping	3%	32%	58%	6%	0%
R12	Politically Exposed Persons	10%	32%	19%	39%	0%
R13	Correspondent Banking	6%	32%	42%	19%	0%
R14	Money or Value Transfer Services	3%	35%	39%	23%	0%
R15	New Technologies	13%	26%	35%	26%	0%
R16	Wire Transfers	13%	10%	16%	61%	0%
R17	Reliance on Third Parties	13%	35%	19%	32%	0%
R18	Internal Controls and Foreign Branches and Subsidiaries	6%	32%	23%	39%	0%
R19	Higher Risk Countries	16%	16%	32%	35%	0%

Technical Compliance						
No.	**Recommendation**	**Non-Compliant (NC)**	**Largely Compliant (LC)**	**Compliant (C)**	**Partially Compliant (PC)**	**N/A**
R20	Reporting of Suspicious Transactions	3%	23%	61%	13%	0%
R21	Tipping-Off and Confidentiality	3%	35%	58%	3%	0%
R22	DNFBPs: Customer Due Diligence	16%	39%	3%	42%	0%
R23	DNFBPs: Other Measures	10%	26%	6%	58%	0%
R24	Transparency and Beneficial Ownership of Legal Persons	19%	29%	0%	52%	0%
R25	Transparency and Beneficial Ownership of Legal Arrangements	23%	26%	3%	45%	3%
R26	Regulation and Supervision of Financial Institutions	6%	45%	10%	39%	0%
R27	Powers of Supervisors	3%	48%	35%	13%	0%
R28	Regulation and Supervision of DNFPBs	19%	19%	0%	61%	0%
R29	Financial Intelligence Units	3%	39%	35%	23%	0%
R30	Responsibilities of Law Enforcement and Investigative Authorities	0%	26%	68%	6%	0%
R31	Powers of Law Enforcement and Investigative Authorities	0%	52%	29%	19%	0%
R32	Cash Couriers	3%	52%	29%	16%	0%
R33	Statistics	6%	29%	16%	48%	0%
R34	Guidance and Feedback	6%	52%	13%	29%	0%

Technical Compliance						
No.	**Recommendation**	**Non-Compliant (NC)**	**Largely Compliant (LC)**	**Compliant (C)**	**Partially Compliant (PC)**	**N/A**
R35	Sanctions	0%	26%	6%	68%	0%
R36	International Instruments	0%	48%	32%	19%	0%
R37	Mutual Legal Assistance	3%	65%	19%	13%	0%
R38	Mutual Legal Assistance: Freezing and Confiscation	6%	71%	10%	13%	0%
R39	Extradition	3%	61%	29%	6%	0%
R40	Other Forms of International Cooperation	6%	55%	16%	23%	0%

Effectiveness						
No.	**Immediate Outcome**	**Low Level**	**Moderate Level**	**Substantial Level**	**High Level**	**N/A**
IO1	Risk, Policy and Coordination	19%	48%	32%	0%	0%
IO2	International Cooperation	13%	32%	52%	3%	0%
IO3	Supervision	29%	58%	13%	0%	0%
IO4	Preventive Measures	29%	68%	3%	0%	0%
IO5	Legal Persons and Arrangements	42%	45%	13%	18%	0%
IO6	Financial Intelligence	32%	35%	29%	3%	0%

Effectiveness						
No.	Immediate Outcome	Low Level	Moderate Level	Substantial Level	High Level	N/A
IO7	Money Laundering Investigation and Prosecution	48%	35%	16%	0%	0%
IO8	Confiscation	32%	35%	26%	6%	0%
IO9	Terrorist Financing Investigation and Prosecution	29%	29%	39%	3%	0%
IO10	Terrorist Financing Preventive Measures and Financial Sanctions	35%	45%	16%	3%	0%
IO11	Proliferation Financial Sanctions	45%	29%	23%	3%	0%

The following areas are some of the common deficiencies that have been identified in MERs:

- Ineffective CDD programs that are inconsistent with FATF standards, not tailored to particular customer types, exempt a significant number of customers, and either fail to identify ultimate beneficial ownership in legal persons and legal arrangements or fail to provide timely access to collected beneficial ownership information.
- Lack of national risk assessment or incomplete or inconsistent understanding of ML/TF risks among regulatory authorities that do not align with national risk assessments, when conducted; excludes risks related to corruption or proliferation of weapons of mass destruction (WMD).
- Inadequate processes to manage risks associated with money value transfer service (MVTS) providers.
- Inadequate processes to identify and manage risks associated with PEPs, both foreign and domestic.
- Inadequate processes to identify and manage risks with legal persons and arrangements.
- Inadequate processes to freeze and confiscate terrorist assets and/or proceeds from crimes, particularly as it relates to crimes other than drug, terrorism and tax-related offenses (e.g., foreign corruption).
- Poor extension of AML/CFT requirements to all categories of DNFBPs.
- Inadequate safeguarding of nonprofit organisations from abuse by terrorists.

- Inadequate systems and controls to identify and report suspicious activity, to maintain adequate records within financial institutions or to request additional information from financial institutions by financial intelligence units (FIUs).
- Inadequate skills, training and resources within regulatory and law enforcement authorities.
- Poor coordination among government agencies, especially among financial supervisors and regulators, investigators, law enforcement authorities and the public.
- Shortcomings in international cooperation/mutual assistance due to the existence of various limiting factors (e.g., strong secrecy provisions, restrictions placed on counterparty's use of information, precondition of treaty, dual criminality stipulation).
- Ineffective application of sanctioning powers for breaches of AML/CFT obligations.
- Insufficient collection of statistics and provision of guidance and feedback to financial institutions.
- Insufficient use of collected financial intelligence to initiate ML/TF investigations by law enforcement.
- Inadequate monitoring and measurement of success.

2896. What were the key findings of the 2006 mutual evaluation of the United States?

The 2006 MER issued for the United States was based on the Forty plus Nine Recommendations prior to the consolidation in 2012. The results of the U.S. MER were as follows:

- Compliant: 15 out of 49 (31 percent)
- Largely Compliant: 28 out of 49 (57 percent)
- Partially Compliant: 2 out of 49 (4 percent)
- Noncompliant: 4 out of 49 (8 percent)

The United States made significant structural changes/statutory amendments with the passage of the USA PATRIOT Act in 2001 and experienced an increase in prosecutions, seizures and enforcement actions since the mutual evaluation conducted in 1999. The United States also developed its efforts in improving coordination and information sharing between the financial community and regulatory authorities, both domestically and internationally, and assisting state and local governments with investigating and prosecuting money laundering and financial crimes and increasing penalties for money laundering.

The mutual evaluation completed on the United States in 2006 highlighted specific areas as needing improvement including, but not limited to:

- Customer due diligence relating to beneficial owners, authorised signers, legal persons and trusts;
- Ongoing due diligence and general requirements for DNFBPs (e.g., casinos, accountants, attorneys, dealers in precious metals and precious stones, real estate agents).

Full details of the U.S. MERs are available at the FATF website: http://www.fatf-gafi.org/.

2897. How did the United States' mutual evaluation compare to other major developed countries in the recent round or MERs?

The 2016 MERs issued for the United States and its peers, Australia and Canada, were based on the FATF Recommendations after the consolidation in 2012, utilising the updated methodology of 2013. The results of these MERs were as follows:

	United States		Australia		Canada	
TECHNICAL COMPLIANCE WITH FORTY RECOMMENDATIONS						
Compliant (C)	9	23%	12	30%	11	28%
Partially Compliant (PC)	6	15%	10	25%	6	15%
Largely Compliant (LC)	21	53%	12	30%	18	45%
Noncompliant (NC)	4	10%	6	15%	5	13%
EFFECTIVENESS WITH ELEVEN IMMEDIATE OUTCOMES (IOs)						
Low Effectiveness	1	9%	0	0%	1	9%
Moderate Effectiveness	2	18%	6	55%	5	45%
Substantial Effectiveness	4	36%	4	36%	5	45%
High Effectiveness	4	36%	1	9%	0	0%

The recent MERs for these three countries identified similar significant gaps related to beneficial owners and DNFBPs. More specifically, identified gaps included, but were not limited to, the following:

- United States
  - Poor efforts to prevent criminals from using legal entities to facilitate illicit schemes. This low rating was driven by the inadequate and untimely access to comprehensive and accurate beneficial ownership information in the United States.
  - Continued lack of coverage of DNFBPs (e.g., lawyers, accountants, real estate agents, and trust and company service providers), particularly related to CDD, recordkeeping, suspicious transaction reporting and internal controls.
- Australia
  - Absence or lack of comprehensive statistics to monitor and measure success and effectiveness of AML/CTF measures (e.g., ML/TF/confiscation statistics from national task forces)
  - Lack of coverage of select DNFBPs (e.g., lawyers, real estate agents)

  - Lack of TF risk assessment of legal persons and arrangements and lack of timely and accessible information on beneficial owners for relevant authorities
  - Lack of coverage of nonprofit organisation (NPOs)
  - Although quality financial intelligence is collected and disseminated, there is a lack of ML/TF investigations triggered by this information by law enforcement

- Canada:
  - Lack of or inadequate coverage of select DNFBPs (e.g., legal counsel, legal firms, notaries, real estate agents, dealers in precious metals and stones)
  - Inadequate coverage of legal persons and arrangements

Full details of all MERs are available at the FATF website: http://www.fatf-gafi.org/.

2898. Has the United States conducted a self-assessment of its money laundering risks?

Yes. The National Money Laundering Risk Assessment (NMLRA) was published in 2015 by multiple federal agencies (e.g., Federal Bureau of Investigation [FBI], the Internal Revenue Service [IRS], the Drug Enforcement Administration [DEA], the Office of Foreign Assets Control [OFAC], Financial Crimes Enforcement Network [FinCEN], Immigration and Customs Enforcement [ICE], United States Secret Service [USSS]), as an update to the U.S. Money Laundering Threat Assessment (MLTA), published in 2005. The NMLRA contains detailed analyses of money laundering vulnerabilities, similar to those identified in the MLTA (2005), across banking, insurance, casinos and MSBs including, but not limited to, the following:

- Use of currency and monetary instruments (e.g., bank notes, cashier's check, money order, traveller's check) in transactions structured under regulatory recordkeeping and reporting thresholds (e.g., US$10,000 for currency transactions, US$3,000 for monetary instruments), commingled with licit funds, used in bulk cash smuggling activities and in trade-based money laundering (TBML) (e.g., Black Market Peso Exchange [BMPE]);
- Establishment of bank and brokerage accounts using nominees (i.e., agent acting by or on behalf of a third party) to disguise the identities of the individuals who control the accounts;
- Creation of legal entities (e.g., shell companies, shelf companies) without accurate information about the identity of the beneficial owner;
- Misuse of products and services (e.g., correspondent banking services, funnel accounts, omnibus accounts, remote deposit capture [RDC], prepaid access cards, virtual currency) resulting from deficient compliance with AML/CFT obligations; and
- Complicit merchants (e.g., wholesalers), third-party payment processors (TPPPs), money services businesses (MSBs) (e.g., foreign exchange dealers, money transmitters) and other financial institutions (e.g., banks, broker-dealers, casinos) with deficient compliance with AML/CFT obligations, and in some cases, wittingly facilitating illicit activity.

The National Terrorist Financing Risk Assessment (NTFRA) was also published in 2015 by the U.S. Treasury, with input from many of the same federal agencies and offices that collaborated on the NMLRA, as well as Customs and Border Protection (CBP), the Bureau of Counterterrorism, Bureau of International Narcotics and Law Enforcement and the National Counterterrorism Center (NCTC). This document contains detailed analyses of terrorist financing vulnerabilities, including, but not limited to, the following:

- Global terrorism and terrorist financing threats
    - Terrorist threats to the United States (e.g., al-Qaeda, Al-Nusrah Front [ANF], Islamic State of Iraq and the Levant [ISIL], Hizballah, Hamas, Taliban, Haqqani Network, foreign terrorist fighters)
    - Terrorist financing sources (e.g., kidnapping for ransom [KFR], extortion, drug trafficking, private donations through charitable organisations, state sponsorship, cybercrime, identity theft) and vulnerabilities (e.g., charitable organisations, licensed and unlicensed money services businesses [MSBs], foreign correspondent banking, cash smuggling, virtual currency)
- Counterterrorism and CFT efforts
    - Law enforcement efforts (e.g., reorientation, interagency coordination and cooperation, information sharing)
    - Financial/regulatory efforts (e.g., Office of Foreign Assets Control [OFAC] sanctions)
    - International efforts (e.g., United Nations [UN], Financial Action Task Force [FATF])

FATF recommends that each country continues to conduct self-assessments to evaluate and ultimately mitigate money laundering and terrorist financing risks on a national level. For further guidance, please refer to the Risk Assessments section.

2899. How has the U.S. responded to the AML/CFT deficiencies identified within its regulatory framework?

The National Money Laundering Strategy (NMLS) was written by the U.S. Departments of Homeland Security, Justice, Treasury, and State, as well as by the Federal Reserve, the OCC, and the FDIC. The most recent NMLS was published in 2007 in direct response to the MLTA. Nine key goals were outlined:

- Continuing to safeguard the banking system
- Enhancing financial transparency in money services businesses (MSBs)
- Stemming the flow of illicit bulk cash out of the United States
- Attacking trade-based money laundering at home and abroad
- Promoting transparency in the ownership of legal entities
- Examining anti-money laundering regulatory oversight and enforcement at casinos

- Implementing and enforcing anti-money laundering regulations for the insurance industry
- Supporting global anti-money laundering capacity building and enforcement efforts
- Improving how to measure progress

Since then, the United States has published advisories and guidance, or proposed or enacted regulations to address these and other noted vulnerabilities within its AML/CFT system. These include, but are not limited to, the following:

- To address the lack of commitment to compliance efforts and accountability:
  - Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance (FinCEN's Advisory issued in August 2014)
  - Individual Accountability for Corporate Wrongdoing (Memorandum issued by Department of Justice (DOJ) (Yates Memo) issued in September 2015)
- To address vulnerabilities related to beneficial owners of legal entities and ongoing due diligence requirements:
  - Customer Due Diligence Requirements for Financial Institutions (FinCEN's final rule issued in July 2016)
- To address vulnerabilities in financial institutions not subject to AML/CFT Program and Customer Identification Program (CIP) requirements:
  - Customer Identification Programs, Anti-Money Laundering Programs and Beneficial Ownership Requirements for Banks lacking a Federal Functional Regulator (FinCEN's Notice of Proposed Rulemaking [NPRM] issued in August 2016)
- To address wholesale "de-risking:"
  - Risk Management Guidance on Foreign Correspondent Banking (Office of the Comptroller of the Currency [OCC] in October 2016)
  - Financial Institution Letters: Statement on Providing Banking Services (Federal Deposit Insurance Corporation [FDIC] in January 2015)
- To address vulnerabilities in the real estate industry:
  - Geographic Targeting Order (GTO) requiring title insurance companies to collect and report purchases of residential real property over a specified amount (e.g., US$500,000 to US$3 million) in specified cities and counties of California, Florida, New York and Texas, made without external financing (e.g., bank loan) that partially used currency or monetary instruments (e.g., cashier's check, traveller's check, money order) (issued in July 2016, renewed in February 2017)
  - Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Housing Government-Sponsored Enterprises (GSEs) (FinCEN's Final Rule issued in February 2014)

- Anti-Money Laundering Program and Suspicious Activity Report Filing Requirements for Residential Mortgage Lenders and Originators (FinCEN's Final Rule issued in April 2012)

- To address vulnerabilities with cyber-related attacks:
  - Cyber-Related Sanctions Program (Implemented by the Office of Foreign Assets Control [OFAC] in December 2015)

- To address vulnerabilities in nonbank financial systems such as money services businesses (MSB) and emerging value transfer systems (e.g., prepaid access, virtual currency):
  - Combating Money Laundering, Terrorist Financing, and Counterfeiting Act of 2017 (A bill introduced by the U.S. Senate in May 2017; Section 13 proposed amending the definition of monetary instrument to include funds stored in a digital format [(e.g., prepaid access devices, virtual currency]).
  - Application of FinCEN's Regulations to Persons Administering, Exchanging or Using Virtual Currencies (FinCEN's Guidance published in March 2013)
  - Bank Secrecy Act Regulations: Definition of "Monetary Instrument" (FinCEN's Proposed Rule issued in October 2011; proposed amending the definition of monetary instrument to include select tangible prepaid access devices for purposes of Report of International Transportation of Currency or Monetary Instruments [CMIR] requirements)
  - Definitions and Other Regulations Relating to Prepaid Access (FinCEN's Final Rule issued in July 2011)

- To address vulnerabilities related to bulk cash smuggling and trade-based money laundering (TBML) schemes:
  - Update on U.S. Currency Restrictions in Mexico: Funnel Accounts and TBML (FinCEN's Advisory issued in August 2014; also related to the following preceding advisories:
    - Newly Released Mexican Regulations Imposing Restrictions on Mexican Banks for Transactions in U.S. Currency (FinCEN Advisory issued in June 2010)
    - Information on Narcotics and Bulk Currency Corridors (FinCEN's Advisory issued in April 2011)
    - Update on U.S. Currency Restrictions in Mexico (FinCEN's Advisory issued in July 2012)
    - Supplement on U.S. Currency Restrictions on Banks in Mexico (FinCEN's Advisory issued in September 2013)
  - CMIR Guidance for Common Carriers of Currency, including Armored Car Services (FinCEN's Guidance issued in August 2014)

- To address vulnerabilities in cross-border funds transfers:
    - Cross-Border Electronic Transmittals of Funds (CBETF) (FinCEN Proposed Rule issued in September 2010)
- To improve how to measure progress:
    - Reformatted SAR Stats (formerly The SAR Activity Review By the Numbers), a compilation of numerical data gathered from the FinCEN Suspicious Activity Reports (SARs) with downloadable data made available for further analysis
- To address financial inclusion:
    - Request for Information Regarding the Use of Mobile Financial Services by Consumers and Its Potential for Improving the Financial Lives of Economically Vulnerable Consumers (Request for Information issued by the Consumer Financial Protection Bureau [CFPB] in June 2014)

In some instances, states are ahead of the federal government in proposing and implementing AML/CFT laws and regulations that address emerging risks and other regulatory areas. Examples from New York State include, but are not limited to, the following:

- BitLicense Regulatory Framework for Virtual Currency Firms (Department of Financial Services (DFS) State Regulation proposed in July 2014 and finalised in June 2015)
- Part 504 – Banking Division Transaction Monitoring and Filtering Program Requirements and Certification (DFS finalised in 2016)
- Part 500 – Cybersecurity Requirements for Financial Services Companies (DFS regulation finalised in 2017)

For further guidance on Part 504, please refer to the Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications section.

United Nations

2900. What key United Nations treaties and conventions have influenced or shaped U.S. AML/CFT laws?

The United States has ratified the following treaties:

- United Nations Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (Vienna Convention, 1988)
- United Nations Convention Against Transnational Organised Crime (2000) (Palermo Convention)
- The United Nations Convention Against Corruption (2003)
- The International Convention for the Suppression of the Financing of Terroris**m** (1999) (Terrorist Financing Convention) (plus an additional 11 U.N. conventions relating to terrorism [e.g., unlawful seizure of aircraft, violence at airports, hostage-taking, maritime navigation, nuclear terrorism])

The U.N. Security Council has adopted multiple resolutions to maintain international peace and security since the 1940s. These resolutions are formal expressions of the U.N. Security Council and generally include a description of the issue(s) and any action(s) to be taken to address the issue (e.g., freezing funds, travel bans, arms embargoes). Key resolutions relating to the prevention and suppression of terrorism and terrorist financing include, but are not limited to, the following:

- **Al-Qaida Sanctions Lists** – Resolutions 1267 (1999), 1333 (2000), 1526 (2004), 1989 (2011) and its successor resolutions.
- **Taliban Sanctions Lists** – Resolutions 1267 (1999), 1526 (2004), 1988 (2011) and its successor resolutions.
- **Islamic State of Levant/Sham (ISIL/ISIS/Da'esh)-Sanctions Lists** – Resolutions 2249 (2015), 2253 (2015), and its successor resolutions.
- **Resolution 1373** (2001) was passed shortly after the September 11, 2001, attacks in New York City, Washington, D.C. and Pennsylvania. The resolution reaffirmed past resolutions related to combating terrorism (e.g., Resolution 1269 [1999], Resolution 1368 [2001]) and called on all members to fully implement relevant international conventions relating to terrorism. Resolution 1373 provided a mechanism for identifying targets for designation on a national or supranational level.
- **Resolutions related to the proliferation of weapons of mass destruction (WMDs)** – Resolutions 1718 (2006), 1737 (2006), 1747 (2007), 1803 (2008), 1874 (2009), 1929 (2010) and its successor resolutions.

The United Nations Participation Act (UNPA) provided the United States with a framework to implement U.N.-related treaties and resolutions. A comprehensive list of United Nations Security Council Resolutions (UNSCRs) enacted by the United States can be found on OFAC's Resource Center at www.treasury.gov/resource-center/sanctions/Pages/UNSCR-links.aspx.

2901. Which countries are members of the U.N Security Council?

The U.N. Security Council has five permanent members (with status granted by the U.N. Charter of 1945) and 10 nonpermanent elected members that serve two-year terms. The five permanent members include China, France, Russia, the United Kingdom and the United States.

Members of the United Nations that are not members of the U.N. Security Council may participate in discussions, but may not vote on actions taken by the Council. Out of approximately 200 U.N. members, nearly 70 have never been elected to the U.N. Security Council.

2902. What guidance has the United Nations provided?

The U.N. has provided the following key model laws, treaties and guidance on money laundering, terrorism and terrorist financing, corruption, human trafficking and migrant smuggling, mutual assistance in criminal matters and other related topics:

- **Money Laundering**

- **United Nations Convention Against Illicit Traffic In Narcotic Drugs And Psychotropic Substances** (1988) (Vienna Convention)
- **United Nations Convention Against Transnational Organised Crime** (2000) (Palermo Convention)
- **Political Declaration and Action Plan Against Money Laundering** (1988)
- **Naples Political Declaration and Global Action Plan Against Organised Transnational Crime** (1994)
- **Report and Recommendations of the International Conference on Preventing and Controlling Money-Laundering and the Use of the Proceeds of Crime: A Global Approach** (1994)
- **Twentieth Special Session of the General Assembly** (1998): Transcript from the panel discussion on "Attacking the Profits of Crime: Drugs, Money and Laundering" and the General Assembly Political Declaration and Action Plan against Money Laundering
- **Money Laundering and the Financing of Terrorism: The United Nations Response** (2004) (Excerpts from the main legal instruments and resolutions against money laundering and the financing of terrorism adopted under the auspices of the United Nations)
- **United Nations Global Programme against Money Laundering (GPML) Forum Framework of Minimum Standards** (2000)
- **An Overview of the UN Conventions and Other International Standards Concerning Anti-Money Laundering and Countering the Financing of Terrorism** – A publication first compiled in February 2004 and then updated in January 2007 by UNODC's Anti-Money Laundering Unit/Global Programme Against Money Laundering, which provides an overview of various international laws and standards on anti-money laundering and counter-financing of terrorism.
- **Financial Havens, Banking Secrecy and Money Laundering** – A publication created in 2008 featuring the results of a study designed to explore the issues of banking secrecy and financial havens in the context of the global fight against money laundering. The study was prepared on behalf of the United Nations under the auspices of the Global Programme Against Money Laundering, Office for Drug Control and Crime Prevention.
- **Countering Money Laundering** – This publication, created in 1997, provides a comparative analysis of major international conventions against money laundering.

- **Terrorism and Terrorist Financing**
  - **Convention on Offences and Certain Other Acts Committed on Board Aircraft** (1963)

- **Convention for the Suppression of Unlawful Seizure of Aircraft** (1970)
- **Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation** (1971)
- **Convention on the Prevention and Punishment of Offences against Internationally Protected Persons, Including Diplomatic Agents** (1973)
- **International Convention against the Taking of Hostages** (1979)
- **Convention on the Physical Protection of Nuclear Material** (1980)
- **Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation** (1988)
- **Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation** (1988)
- **Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf** (1988)
- **Convention on the Marking of Plastic Explosives for the Purpose of Detection** (1991)
- **International Convention for the Suppression of Terrorist Bombings** (1997)
- **International Convention for the Suppression of the Financing of Terrorism** (1999) (Terrorist Financing Convention)
- **Digest of Terrorist Cases** – A publication created in 2010 that provides practical ideas and expert insights on how to deal with cases of terrorism. Topics include, but are not limited to, the following:
    - Violent Offences Not Requiring a Specific Terrorist Intent
    - Association for the Purpose Of Preparing Terrorist Acts
    - Relationship Between Terrorism and Other Forms of Crime (e.g., corruption, narcotics trafficking, organised crime, using minor offences to catch major criminals, false identity and immigration offences)
    - The Statutory Framework for Terrorism Prosecutions
    - Investigation and Adjudication Issues
    - International Cooperation
    - Innovations and Proposals
- **Legislative Guide to the Universal Anti-Terrorism Conventions and Protocols** – A publication created in 2004 that provides a summary of the

development and requirements of the international terrorism conventions to assist those responsible for incorporating anti-terrorism conventions in national legislation.

  - **Guide for Legislative Incorporation of the Provisions of the Universal Legal Instruments Against Terrorism** – A publication created in 2006 that provides guidance on how anti-terrorism conventions and protocols can be integrated and harmonised with domestic law and other international standards.
  - **Preventing Terrorist Acts: A Criminal Justice Strategy Integrating Rule of Law Standards in Implementation of United Nations Anti-Terrorism Instruments** – A publication created in 2006 that provides guidance on topics including, but not limited to, the responsibility to protect against terrorism, scope and elements of a preventive criminal justice strategy against terrorism, offenses, procedural improvements and mechanisms for international cooperation.
  - **Criminal Justice Responses to Terrorism Handbook** – A publication created in 2009 that provides guidance on the key components of an effective criminal justice response to terrorism and criminal justice accountability and oversight mechanisms.
  - **Counter-Terrorism Legislation Database** – An online resource of legal resources on international terrorism established in 2009.
  - **Frequently Asked Questions on International Law Aspects of Countering Terrorism** – A publication created in 2009 that provides an overview of the international law framework in which counter-terrorism works, including general principles of international criminal law, humanitarian law, refugee law and human rights law, which may be relevant in a counter-terrorism context.

- **Drug Trafficking, Human Trafficking and Migrant Smuggling**
  - **World Drug Report** – An annual report by the United Nations Office on Drugs and Crime (UNODC) that provides an overview of major developments in drug markets related to production, trafficking, consumption and impact on health. Covered drugs included opiates, cocaine, cannabis and amphetamines (including ecstasy).
  - **Global Report on Trafficking in Persons** – A publication created in 2012 with scheduled updates every two years that provides an overview of human trafficking and the worldwide response at global, regional and national levels.
  - **Toolkits to Combat Trafficking in Persons and Smuggling of Migrants** – First released in 2005, the publication covers topics such as legal frameworks, victim identification and assistance and the international response to human trafficking.
- **Corruption**
  - **Stolen Asset Recovery Initiative (StAR)** – A partnership between the United Nations Office on Drugs and Crime (UNODC) and the World Bank (WB) that provides policy analysis and proposal, case assistance and capacity building in developing countries to build anti-corruption and asset recovery systems.

- **Tools and Resources for Anti-Corruption Knowledge (TRACK)** – A web-based anti-corruption portal launched in 2011 by the UNODC with tools and resources for the private sector, academia and civil society. Resources include legal libraries, trainings and analytical tools related to anti-corruption and asset recovery.
- **Assessment of the Integrity and Capacity of the Justice System in Three Nigerian States** – A publication created in 2006 that presents statistics and data drawn from live interviews held with specific groups within the justice system.
- **Compendium of International Legal Instruments on Corruption, 2nd Edition** – A publication created in 2005 that contains all the major relevant international and regional treaties, agreements, resolutions and other instruments related to corruption.
- **Global Action Against Corruption: The Mérida Papers** – A publication highlighting the key topics addressed in the United Nations Office on Drugs and Crime in Merida, Mexico, in 2003, including, but not limited to, the following:
  - Preventive Measures against Corruption: the Role of the Private and Public Sectors
  - The Role of Civil Society and the Media in Building a Culture against Corruption
  - Legislative Measures to Implement the United Nations Convention against Corruption
  - Measures to Combat Corruption in National and International Financial Systems
  - International Group for Anti-Corruption Coordination: Report of the Fifth Meeting
- **Technical Guide to the United Nations Convention Against Corruption** – A publication created in 2009 by the UNODC and the United Nations Interregional Crime and Justice Research Institute (UNICRI) to promote the implementation of the United Nations Convention against Corruption (UNCAC) Convention, the first global legally binding instrument in the fight against corruption, which was adopted by the United Nations in 2003.

- Mutual Assistance and Other Criminal Matters
  - **United Nations Model Mutual Assistance in Criminal Matters Bill** (2000)
  - **United Nations Model Foreign Evidence Bill** (2000)
  - **United Nations Model Extradition (Amendment) Bill** (2000)
  - **United Nations Model Witness Protection Bill** (2000)

- **United Nations Model Legislation on Laundering, Confiscation and International Cooperation in Relation to the Proceeds of Crime** (1999)
- **United Nations Model Law on International Cooperation (Extradition and Mutual Legal Assistance) with regard to Illicit Traffic in Narcotic Drugs, Psychotropic Substances and Precursors**
- **United Nations Model Treaty on Extradition** (1990) and amendment, **United Nations International Cooperation in Criminal Matters** (1997)
- **United Nations Model Treaty on Mutual Assistance in Criminal Matters** (1990) and amendment, **United Nations Mutual Assistance and International Cooperation in Criminal Matters** (1998)

The United Nations has published reports related to organised crime, maritime crime and piracy, firearms, and other criminal activities. For further information, please visit the United Nations Office on Drug and Crime's website at www.unodc.org.

2903. What is the International Money Laundering Information Network (IMoLIN)?

The International Money Laundering Information Network (IMoLIN), established in 1998 by the United Nations, is a network of the following international organisations:

- Asia/Pacific Group on Money Laundering (APG)
- Caribbean Financial Action Task Force (CFATF)
- Commonwealth Secretariat, Council of Europe – MONEYVAL
- Eurasian Group (EAG)
- Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
- Financial Action Task Force (FATF)
- Financial Action Task Force of South America Against Money Laundering (GAFISUD)
- Intergovernmental Action Group Against Money Laundering in West Africa (GIABA)
- INTERPOL
- Organisation of American States (OAS/CICAD)

Key resources provided by IMoLIN include the following:

- **Anti-Money Laundering International Database (AMLID)** – A centralised resource center administered by the Law Enforcement, Organised Crime and Anti-Money-Laundering Unit (LEOCMLU) of the United Nations Office on Drugs and Crime (UNODC) that contains analyses of AML/CFT laws and regulations from its member organisations.
- **Legislations and Regulations** – List of legislation and regulations by country.
- **International Norms and Standards** – Model laws for common law and civil law systems.

- **Research and Analysis** – Publications from governments and international organisations.
- **Bibliography** – A list of books, articles and other publications issued by governments and international organisations addressing all aspects of anti-money laundering, countering the financing of terrorism, and governance.
- **Calendar of Events** – A list of current national, regional and international training events and conferences.
- **Technical Assistance** – Capacity-building resources, including fact sheets and trainings.

Egmont Group of Financial Intelligence Units

2904. What is a Financial Intelligence Unit (FIU)?

A financial intelligence unit (FIU) serves as the central agency to receive and analyse required AML/CFT reporting (e.g., suspicious transaction reporting, large currency transactions, disclosures of cross-border movement of currency and negotiable instruments) and disseminate guidance, statistics and feedback to relevant authorities in a secure and confidential process.

The Egmont Group of Financial Intelligence Units (Egmont Group) outlines four models for countries to develop their FIUs:

- **Judicial Model** – Agency established within the judicial branch; receives AML/CFT reports/information from the financial sector; uses judiciary power to seize funds, freeze assets/accounts, conduct interrogations, detain people and conduct searches;
- **Law Enforcement Model** – Agency that works alongside and supports existing law enforcement systems with jurisdictional authority to also investigate money laundering on its own;
- **Administrative Model** – Independent agency that coordinates AML/CFT efforts between the financial sector and judicial/law enforcement authorities; and
- **Hybrid Model** – Agency that combines elements of the aforementioned models.

The Financial Crimes Enforcement Network (FinCEN) is the FIU of the United States and is based on the hybrid model. For further guidance, please refer to the Financial Crimes Enforcement Network section.

2905. What is the Egmont Group of Financial Intelligence Units?

The Egmont Group, formed in 1995, has been the leading international association of FIUs. Over the years, member countries have met annually to discuss global issues of importance with regard to money laundering as well as terrorist financing. The Egmont Group acts as a conduit for information sharing and, when pertinent, passes information on to the corresponding law enforcement agency to investigate. The operating structure consists of the following:

- Heads of FIUs (HoFIUs)
- Egmont Committee

- Secretariat
- Working Groups
    - IT Working Group (ITWG)
    - Legal Working Group (LWG)
    - Operational Working Group (OpWG)
    - Outreach Working Group (OWG)
    - Training Working Group (TWG)
- Regional Groups
    - Africa
    - Americas
    - Asia
    - Europe
    - Oceania

2906. How does the Financial Action Task Force (FATF) address the establishment of FIUs?

FATF Recommendation 29 - Financial Intelligence Units, recommends that all jurisdictions establish FIUs and apply for membership with the Egmont Group.

2907. How does an FIU become a member of the Egmont Group?

An FIU becomes a member of the Egmont Group by completing the following:

- Submission of a Membership Application including the Egmont Group Questionnaire that includes contact details, interest from the unit, copies of AML/CFT legislation and other relevant documentation in English and at least two Sponsor FIUs;
- Multiple onsite visits resulting in a written assessment, Onsite Assessment Report (OAR), which focuses on the operational and legal aspects of the FIU.

The Outreach Working Group (OWG) and the Legal Working Group (LWG) lead discussions on the candidate's application, provide their recommendations at the annual meeting and a written commitment, if endorsed. Applicants may be invited to attend the Egmont Plenary session as an Observer FIU or Candidate FIU, depending on whether their application will be discussed in that session.

Membership has surpassed 150 countries and continues to grow.

2908. Can organisations participate in Egmont Group activities without being a member?

Yes. The Egmont Group works with observer organisations (e.g., FATF, International Monetary Fund [IMF], World Bank [WB]) and multiple international partner organisations (e.g., Basel Committee on

Banking Supervision, Wolfsberg Group, European Union). FIUs who have applied for membership may be invited to attend Egmont Plenaries as observers or candidates prior to becoming members.

2909. What is Egmont's Secure Web (ESW) system?

Egmont's Secure Web (ESW) system is a private network that allows member FIUs to interface with each other to access information related to ML/TF trends, analytical tools and technological developments. The ESW is administered by the Financial Crimes Enforcement Network (FinCEN), the FIU of the United States.

2910. What are the operational standards of the Egmont Group?

In 2013, the Egmont Group published the following charter and operational standards to provide member FIUs guidance on how to participate in information exchanges:

- Egmont Group of Financial Intelligence Units Charter
- Egmont Group of Financial Intelligence Units Operational Guidance for FIU Activities and the Exchange of Information

Topics covered include channels for information exchange, memorandums of understanding (MOUs) between FIUs, data protection and confidentiality and guidance for making and receiving requests and other FIU activities.

2911. Is there a mechanism to address member FIUs that are not in compliance with Egmont's charter and principles of information exchange?

Yes. The Support and Compliance Process was created to address non-compliant member FIUs. While it was designed to assist member FIUs to become compliant, Egmont will apply sanctions including, but not limited to, the following:

- Warnings
- Restrictions on participation in Egmont activities
- Bans from Egmont meetings and training sessions
- Suspension of ESW accounts
- Suspension

2912. What guidance has the Egmont Group provided?

Egmont has provided the following guidance:

- **Egmont Group Annual Report (2007 – 2015) –** Annual reports providing summaries and highlights from meetings, working group sessions, trainings, outreach programs and regional developments.
- **Egmont Group of Financial Intelligence Units Charter and Egmont Group of Financial Intelligence Units Operational Guidance for FIU Activities and the**

Exchange of Information – Created in 2013, this charter and publication provides operational standards for international cooperation and information exchange.

- **Egmont Group of Financial Intelligence Units Principles for Information Exchange Between Financial Intelligence Units** – A publication created in 2013 that provides binding principles for information exchange between FIUs. Topics covered include obligations for making and receiving requests, restrictive conditions for international cooperation and data protection and confidentiality.
- **Egmont Group of Financial Intelligence Units Support and Compliance Process –** A publication created in 2014 that provides guidance on the "Support and Compliance Process" mechanism that identifies member FIUs that are not in compliance with Egmont's charter and principles for information exchange.
- **Egmont Group Partnership with Observers and International AML/CFT Partners –** A publication created in 2013 that clarifies roles and partnerships by providing procedures to enhance cooperation between the Egmont Group and international organisations such as FATF, IMF, World Bank and the United Nations.
- **Enterprise-Wide STR Sharing: Issues and Approaches –** A publication created in 2011 that provides guidance on enterprisewide and cross-border sharing of suspicious transaction reports (STRs). Topics covered include survey results, risk and benefits of STR sharing and key considerations and approaches to facilitating STR sharing.
- **The Role of FIUs in Fighting Corruption and Recovering Stolen Assets** – An FIU can be an important element of fighting corruption-related offences, and preventing the laundering of illicit funds which stem from corruption activities. Published in 2012, this report details the results of a study aimed at increasing awareness of corruption and asset recovery among FIUs, and presents case scenarios and best practices. It also describes the position and the role of the FIU in the asset recovery process.
- **Enhancing International AML/CFT Information Exchange through Strengthening FIU Channels** – Published in 2011, this report introduces the concept of "diagonal" exchange of information through enhanced international cooperation, and focuses on the Egmont Group's ongoing efforts to strengthen international sharing of information in areas where current international standards do not call for, or may not fully support, cross-border sharing.
- **Statement of Purpose of the Egmont Group of Financial Intelligence Units** – A statement of purpose written for the organisation in June 1997 and revised as of June 2004. Full compliance with the Egmont definition of a financial intelligence unit (FIU) is an essential component of being admitted into the Egmont Group.
- **Principles for Information Exchange Between Financial Intelligence Units for Money Laundering and Terrorism Financing Cases** – Basic principles, written in June 2001, outlining how the exchange of information between FIUs should be conducted.

- **Interpretive Note Concerning the Egmont Definition of a Financial Intelligence Unit** – A document explaining the Egmont Group's stance on the definition of an FIU. The definition was originally stated in 1996 and amended in 2004 to include terrorism financing.
- **"Countering of Terrorism Financing" Complementary Interpretive Note** – A document created in 2004 intended to complement the Interpretive Note Concerning the Egmont Definition of an FIU, which further clarifies the definition of an FIU by also explaining the minimum requirements of an FIU to comply with the Egmont Group's definition of an FIU.
- **Executive Summary of The Final Report on Survey of FIU Governance Arrangements** – A document created by the Egmont Group and World Bank Project in January 2010 that summarises baseline information on governance arrangements among FIUs.
- **Best Practices for the Exchange of Information Between Financial Intelligence Units** – A document developed to enhance the exchange of information between FIUs by documenting principles that relate to the conditions for the exchange of information, the permitted uses of information, and confidentiality.
- **Information Paper on Financial Intelligence Units and the Egmont Group** – A brief paper published in 2004 describing the history and purpose of FIUs and the Egmont Group.
- **Egmont Meetings at a Glance** – A document that describes the main focus or outcomes of each of the Egmont Plenary Meetings, current as of August 2005.
- **International Bulletin** – A bulletin produced from time to time that outlines the current accomplishments and ongoing workings of the Egmont Group.
- **Library of Sanitised Cases** – A library of cases submitted by member FIUs of the Egmont Group, in which the information was sanitised so others can use the cases as training material to assist all FIUs and institutions with fighting the global problem of money laundering and terrorist financing. The library is broken down into categories such as Cross-Border Activities, Gambling, and Terrorist Financing.
- **FIUs in Action: 100 Cases from the Egmont Group** – A compilation of 100 sanitised cases published to assist FIUs and institutions with fighting the global problem of money laundering and terrorist financing, compiled by Egmont from submissions from member FIUs. These cases can be used as training material.
- **The Egmont Group – Financial Intelligence Units of the World –** A listing of all current member FIUs of the Egmont Group.

Other Key International Groups and Initiatives

2913. What is the Basel Committee on Banking Supervision?

The Basel Committee on Banking Supervision (BCBS) is a committee of central banks and bank supervisors and regulators from major industrialised countries that meets to discuss issues relating to banking supervision at the Bank for International Settlements (BIS) in Basel, Switzerland. BCBS was

formed in 1974 by the Governors of the central banks of the G10. BCBS operates under the expectation that member nations will take into account, and then implement, the guidance that comes out of these meetings. The goal of BCBS is to create uniform international standards of banking best practices.

2914. What key AML/CFT guidance has the Basel Committee provided?

The Basel Committee has provided the following key AML/CFT guidance:

- **Guidelines: Sound Management of Risks Related to Money Laundering and Financing of Terrorism** – This set of guidelines describes how banks should include risks related to money laundering and financing of terrorism within their overall risk management framework. These guidelines, published in January 2014, include cross-references to FATF standards to help banks comply with national requirements based on those standards.
- **Sound Management of Risks Related to Money Laundering and Financing of Terrorism** – A publication created in July 2013 that provides guidance on how financial institutions can manage risks related to money laundering and terrorist financing within their overall risk management framework (guidance supersedes previously issued guidance, Customer Due Diligence for Banks [October 2001] and Consolidated KYC Management [October 2004]).
- **Basel Committee: Banking Secrecy and International Cooperation in Banking Supervision** – A publication created in December 1981 that discusses the need to overcome bank secrecy impediments that hinder the flow of information between different foreign jurisdictions in an effort to establish an effective, internationally coordinated infrastructure to supervise banks.
- **Basel Committee: Prevention of Criminal Use of the Banking System for the Purpose of Money Laundering** – A publication created in December 1998 that encourages banks to implement effective procedures to properly identify customers with whom they are conducting business to prevent their institutions from being used to conduct criminal activity.
- **Basel Committee: Compliance and the Compliance Function** – A publication created in April 2005 that provides guidance on compliance risks (e.g., legal, regulatory, reputation, financial loss) and the compliance function, including responsibilities for compliance officers, senior management, boards of directors and the overall compliance culture.
- **Initiatives by the BCBS, IAIS and IOSCO to Combat Money Laundering and the Financing of Terrorism** – A joint note created in June 2003 between the Basel Committee on Banking Supervision (BCBS), International Association of Insurance Supervisors (IAIS), and the International Organisation of Securities Commissions (IOSCO) that discusses the initiatives taken by each sector to combat money laundering and terrorist financing. The first part of the note provides an overview of common AML/CFT standards applicable to all three sectors and assesses whether there are serious gaps or inconsistencies in approaches and recommendations. The second part of the note covers the relationships between the institutions and their customers, focusing on products or services particularly vulnerable to money laundering, how each committee has sought to address those vulnerabilities, and a description of ongoing and future work, broken out by each of the three sectors.

- **Customer Due Diligence for Banks** – A publication created in October 2001, establishing standards for Know Your Customer (KYC) programs to manage the reputational, operational, legal and concentration risks of banks and nonbank financial institutions and professional intermediaries (e.g., attorneys, accountants) effectively.
- **General Guide to Account Opening and Customer Identification** – A publication created in February 2003 as an attachment to "Customer Due Diligence for Banks," which was published in October 2001. This publication focuses on some mechanisms banks can use to develop an effective Customer Identification Program (CIP).
- **Consultative Document: General Guide to Account Opening** – This revised general guide to account opening, published in July 2015, aims to support banks in implementing the existing FATF standards and guidance, which requires the adoption of specific policies and procedures for account opening.
- **Sharing of Financial Records between Jurisdictions in Connection with the Fight against Terrorist Financing** – A publication created in April 2002 that focuses on the official gateways, such as financial intelligence units (FIUs), for cross-border information sharing as well as information flow from a financial entity to its head office or parent.
- **Survey of Developments in Electronic Money and Internet and Mobile Payments** – A publication created in March 2004 in cooperation with the Committee on Payment and Settlement Systems (CPSS) that focuses on two categories of emerging payment products and services: reloadable electronic money instruments and internet and mobile payments.
- **General Principles for International Remittance Services** – A publication created in January 2007 jointly with the World Bank (WB) that discusses the payment system aspect of remittances and how to safely and efficiently send and receive international payments. The January 2007 edition was an update to the original publication issued in March 2006.
- **Due Diligence and Transparency Regarding Cover Payment Messages Related to Cross-Border Wire Transfers –** A publication created in May 2009 that provides guidance for situations in which one or more intermediary banks are located in a jurisdiction other than where the bank of the originator and the bank of the beneficiary are located.

2915. What is the Wolfsberg Group of Banks?

The Wolfsberg Group of Banks (Wolfsberg Group) is an association of 11 member international banks that creates industry best practices. Formed in 2000, the member banks include Banco Santander, Bank of Tokyo-Mitsubishi UFJ, Barclays, Citigroup, Credit Suisse, Deutsche Bank, Goldman Sachs, HSBC, JPMorgan Chase, Société Générale and UBS. The group has produced work products in the areas of Know Your Customer (KYC), AML, CFT and anti-corruption best practices.

2916. What key AML/CFT guidance has the Wolfsberg Group provided?

Key AML/CFT publications issued by the Wolfsberg Group include, but are not limited to, the following:

- **Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption** (2015) – Guidance on developing, conducting and interpreting results of risk assessments that evaluate multiple financial crimes such as money laundering, terrorist financing, sanctions, bribery and corruption.
- **Wolfsberg Guidance on SWIFT Relationship Management Application (RMA)** Due Diligence (2016) – Guidance concerning minimum due diligence standards on SWIFT RMA arrangements (e.g., for non-customers, on-going due diligence).
- **Wolfsberg AML Principles for Correspondent Banking** (2014) – Guidance concerning the establishment and ongoing maintenance of correspondent banking relationships (updated 2002 guidance).
- **Wolfsberg Frequently Asked Questions on Correspondent Banking** (2014) – A follow-up guide to the Wolfsberg AML Principles for correspondent banking addressing frequently asked questions concerning correspondent banking based upon the Wolfsberg Group's views on current best practices and how it believes those practices should evolve over time (updated 2006 guidance).
- **Wolfsberg Guidance on Mobile and Internet Payment Services (MIPS) (2014) –** Guidance concerning the money laundering risks of mobile and internet payment services including credit, prepaid and stored value cards.
- **The Wolfsberg Statement Against Corruption** (2007) – A statement written to generally describe the Wolfsberg Group's and financial institutions' roles in dealing with corruption. It also identifies some measures that may be used by financial institutions to prevent corruption in their own operations and protect themselves against the misuse of their operations in relation to corruption.
- **Wolfsberg Statement – Guidance on a Risk-Based Approach for Managing Money Laundering Risks** (2006) – Guidance to assist institutions with managing money laundering risks and prevent the use of their institutions for criminal purposes; focuses on using a risk-based approach.
- **Wolfsberg Statement – Anti-Money Laundering Guidance for Mutual Funds and Other Pooled Investment Vehicles** (2006) – Guidance to assist mutual funds and other pooled investment vehicles with managing their money laundering risk.
- **Wolfsberg Statement on AML Monitoring, Screening and Searching** (2009) – This guidance supersedes the 2003 paper on the same topic. The statement provides more guidance on the design, implementation and ongoing maintenance of transaction monitoring frameworks for real-time screening, transaction monitoring and retroactive searches.
- **The Wolfsberg Group and the Clearing House Association: Cover Payments: Some Practical Questions Regarding the Implementation of the New Payments Messages** (2009) – Guidance issued by the Wolfsberg Group regarding the implementation of the new SWIFT payment messages for cover payments, the MT 202 COV, and the MT 205 COV.

- **Wolfsberg Statement on the Suppression of the Financing of Terrorism** (2002) – Guidance describing the role financial institutions have in preventing the flow of terrorist funds through the world's financial systems.
- **Wolfsberg AML Principles on Private Banking** (2012) – Guidance tailored toward assisting financial institutions with combating money laundering in the private banking industry.
- **Wolfsberg Frequently Asked Questions on Selected Anti-Money Laundering Issues in the Context of Investment and Commercial Banking** (2006) – Guidance addressing specific money laundering concerns in the investment and commercial banking industries.
- **Wolfsberg FAQs on Beneficial Ownership** (2012) – A guide addressing questions concerning "Beneficial Ownership" that arose from the Wolfsberg AML Principles on Private Banking.
- **Wolfsberg FAQs on Politically Exposed Persons** (2008) – A guide addressing frequently asked questions about politically exposed persons (PEPs).
- **Wolfsberg FAQs on Intermediaries** (2012) – A guide addressing frequently asked questions about intermediaries.
- **Wolfsberg AML Guidance on Credit/Charge Card Issuing and Merchant Acquiring Activities** (2009) – A guide addressing the vulnerabilities of credit/charge card issuing activities and merchant acquiring activities in and methods of managing these risks.
- **Wolfsberg Trade Finance Principles** (2011) – A guide on the vulnerabilities of trade finance and recommendations on methods for managing these risks.

2917. What is the World Bank?

The World Bank (WB), established in 1945, was founded to help countries recover from natural disasters, humanitarian crises and other conflicts that plague the developing world. The WB consists of five institutions:

- International Bank for Reconstruction and Development (IBRD)
- International Development Association (IDA)
- The International Finance Corporation (IFC)
- Multilateral Investment Guarantee Agency (MIGA)
- International Centre for Settlement of Investment Disputes (ICSID)

With nearly 190 member countries, the WB primarily works on reducing global poverty by the distribution of grants for development projects. The WB also has a group whose primary purpose is to curb money laundering and terrorist financing through FATF as its vehicle for change. In recent years, the WB has adopted FATF Recommendations for internal use.

2918. What key AML/CFT guidance has the WB provided?

Key AML/CFT publications issued by the WB include, but are not limited to, the following:

- **Making Remittances Work: Balancing Financial Integrity and Inclusion –** A publication created in 2014 that provides guidance on how to implement anti-money laundering and counter terrorist financing programs while balancing financial inclusion and economic development as it relates to remittances.
- **Protecting Mobile Money Against Financial Crimes: Global Policy Challenges and Solutions –** A publication created in 2011 that provides an overview of the mobile money market, associated money laundering and terrorist financing risks, potential mitigation techniques and the interplay between financial inclusion and compliance with global anti-money laundering and counter-terrorist financing standards.
- **Stolen Asset Recovery Initiative (StAR)** – A partnership between the WB and the United Nations Office on Drugs and Crime (UNODC) that provides policy analysis and proposal, case assistance and capacity building in developing countries to build anti-corruption and asset recovery systems.
- **Left Out of the Bargain: Settlements in Foreign Bribery Cases and Implications for Asset Recovery –** A publication created in 2014 that summarises global settlement practices as it relates to foreign bribery cases.
- **Barriers to Asset Recovery: An Analysis of the Key Barriers and Recommendations for Action –** A publication created in 2011 that provides an overview on the existing difficulties in stolen asset recovery actions and key recommendations.
- **Suspending Suspicious Transactions** – A publication created by the World Bank in partnership with the Egmont Group in 2013 about the power of Financial Intelligence Units (FIU) to postpone suspicious transactions.
- **Money Laundering and Terrorist Financing: A Practical Guide for Banking Supervisors** – A publication created in 2009 that summarises various models, suggested tools, and methodologies for developing comprehensive supervisory systems.
- **New Technologies, New Risks? Innovation and Countering the Financing of Terrorism** – A publication created in 2009 that details the vulnerabilities of value cards, mobile financial services, online banking/payments and digital currencies, and recommendations on developing more effective preventive measures.
- **Stolen Asset Recovery: Politically Exposed Persons, A Policy Paper on Strengthening Preventive Measures** – A publication created in 2009 that summarises key obstacles in identifying and mitigating the risks of politically exposed persons (PEPs) and recommendations on developing more effective preventive measures.
- **Stolen Asset Recovery: A Good Practices Guide on Non-Conviction Based (NCB) Asset Forfeiture** – A publication created in 2009 that provides guidance on Non-Conviction Based (NCB) forfeiture, a legal regime that provides for the seizure and forfeiture of the proceeds of serious crime, including corruption, without the need for a criminal conviction.

- **Correspondent Account KYC Toolkit: A Guide to Common Documentation Requirements** – A publication created in 2009 by the International Finance Corporation (IFC), the private sector arm of the World Bank Group, that provides information and guidance relating to the application process for opening a correspondent bank account or responding to an inquiry from a counterparty bank undertaking a Know Your Customer (KYC) compliance review.
- **Withdrawal from Correspondent Banking: Where, Why and What To Do About It** – This publication, published in November 2015, includes findings, conclusions and recommendations from the World Bank's survey of banking authorities and banks worldwide to examine the extent of withdrawal from correspondent banking, its drivers, and its implications for financial exclusion/inclusion.
- **Alternative Remittance Systems and Terrorism Financing: Issues in Risk Management** – A publication created in 2009 that summarises more than a hundred recommendations on issues relating to terrorist financing, including, but not limited to, new technologies, nonprofit organisations, informal remittance providers, and international cooperation.
- **Mobile Phone Financial Services Paper** – A publication created in 2008 that summarises fieldwork from seven economies on the vulnerabilities of mobile financial services and recommendations on methods for managing these risks.
- **Counter-Terrorism Implementation Task Force Report** – A publication created in 2009 that details the findings and recommendations of the meetings of the "United Nations Working Group on Tackling the Financing of Terrorism" task force led by the World Bank with the IMF and the UN Office on Drugs and Crime with support from INTERPOL, the Al-Qaida/Taliban Monitoring Team, and the Counter-Terrorism Committee.
- **Who Supports Violent Extremism in Developing Countries? Analysis of Attitudes Based on Value Surveys –** Drawing on information on attitudes toward extreme violence and other characteristics of 30,787 individuals from 27 developing countries around the world, and employing a variety of econometric techniques, this paper, published in June 2016, identifies the common characteristics among radicalised individuals, willing to justify attacks targeting civilians.
- **Financial Intelligence Units: An Overview** – A publication created in 2004 that provides examples from multiple countries on how to establish financial intelligence units (FIUs).
- **Effective Regimes to Combat Money Laundering and the Financing of Terrorism, Strengthening the Collaborative Process: Lessons Learned** – A publication created in 2004 that describes best practices for developing an effective AML/CFT infrastructure consistent with international standards.
- **The World Bank in the Global Fight Against Money Laundering and Terrorist Financing** – A publication created in 2003 that describes the magnitude and impact of money laundering and terrorist financing on the global financial system and the role of the World Bank in combating it.

- **Reference Guide to Anti-Money Laundering and Combating the Financing of Terrorism: Second Edition and Supplement on Special Recommendation IX** – A guide created in January 2006 that provides practical solutions to establishing a comprehensive AML/CFT infrastructure.
- **AML/CFT Regulation: Implications for Financial Service Providers that Serve Low-Income People** – A guide published in July 2005 that summarises the implications of the AML/CFT requirements for financial service providers working with low-income people and possible solutions to minimise adverse impacts.
- **Money Laundering in Cyberspace** – A document published in November 2004 that details the vulnerabilities and trends of internet-based payment mechanisms and recommendations on methods for managing these risks.
- **Bilateral Remittance Corridor Analysis (BRCA)** – A series of publications that focuses on payment corridors between two or more countries. The reports provide insight into the players (e.g., remittance senders and receivers), market dynamics, vulnerabilities, and regulatory frameworks of select remittance corridors.
- **Combating Money Laundering and the Financing of Terrorism: A Comprehensive Training Guide** – A seven-part training guide published in January 2009 on developing comprehensive institutional, legal, and regulatory frameworks for combating money laundering and terrorist financing consistent with international standards:
    - Volume 1: Effects on Economic Development and International Standards
    - Volume 2: Legal Requirements to Meet International Standards
    - Volume 3a: Regulatory and Institutional Requirements for AML/CFT
    - Volume 3b: Compliance Requirements for Financial Institutions
    - Volume 4: Building an Effective Financial Intelligence Unit
    - Volume 5: Domestic (Inter-Agency) and International Cooperation
    - Volume 6: Combating the Financing of Terrorism
    - Volume 7: Investigating Money Laundering and Terrorist Financing

2919. What is the International Monetary Fund?

The International Monetary Fund (IMF) is an international body like the World Bank. It oversees the global monetary system and offers aid and assistance to countries as situations arise. The IMF, along with the WB, have created the Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) program to help the global community better improve AML/CFT systems to prevent the flow of terrorist dollars into the global monetary infrastructure. This group works by providing technical assistance to countries in need.

2920. What is the Financial Sector Assessment Program (FSAP)?

The Financial Sector Assessment Program (FSAP) was established in 1999 by the IMF and the World Bank. The FSAP is a voluntary, comprehensive and in-depth analysis of a country's financial sector designed to help increase the effectiveness of efforts to promote the soundness of financial systems in member countries, including AML/CFT systems. Financial Stability Assessment Reports (FSARs) are published with the results of each country's assessment. In 2008, the **Offshore Financial Center (OFC) Assessment Program** was integrated into the FSAP Program. The OFC Assessment Program executes detailed assessments of the extent to which OFCs meet international standards.

Countries with financial sectors deemed "significantly important" are required to have FSAPs conducted every five years. The AML/CFT assessment may occur at the time of the FSAP or separately but is required to be completed within 18 months of the FSAP.

2921. What were the results of the most recent FSAP of the AML/CFT system of the United States?

The IMF published the most recent FSAP of the United States' AML/CFT system in July 2015. The assessment targeted a review of measures to prevent the abuse of legal arrangements (e.g., trusts) for money laundering/terrorist financing. The report detailed two main recommendations:

- Require the collection of beneficial ownership information, including trust and company service providers and lawyers and accountants providing these types of services; and
- Make tax crimes a predicate crime to money laundering.

2922. What key AML/CFT guidance has the IMF provided?

Key AML/CFT publications issued by the IMF include, but are not limited to, the following:

- **Islamic Finance and Anti-Money Laundering and Combating the Financing of Terrorism** (AML/CFT) – A publication released in February 2016 that explores the ML/TF risks associated with Islamic finance to help national regulators gain a better understanding of the specific risks associated with this form of financing and to develop an appropriate response.
- **Fiscal Consequences of Terrorism** – This publication released in October 2015 that provides an empirical analysis of how the frequency and severity of terrorism affect government revenue and expenditure during the period 1970–2013.
- **Review of the Fund's Strategy on Anti-Money Laundering and Combating the Financing of Terrorism** – A publication created in 2014 that addresses the revised AML/CFT standard and assessment framework, coverage of financial integrity issues in surveillance and financial sector assessment program (FSAP).
- **Anti-Money Laundering and Combating the Financing of Terrorism Inclusion in Surveillance and Financial Stability Assessments** – A publication created in 2012 that provides guidance on the inclusion of anti-money laundering and counter-terrorist financing

issues in surveillance and financial sector assessment programs (FSAP), specifically as they threaten the stability and integrity of financial systems.

- **Fiscal Transparency, Accountability, and Risk** – A publication created in 2012 that highlights fiscal transparency as a critical element of effective fiscal policymaking and risk management. The focus is on the ongoing efforts to enhance international standards for transparency and monitoring, and revitalising various efforts to prevent risk management shortcomings.
- **Money Laundering and Terrorism Financing: An Overview** – A publication created in 2005 that examines why and how criminal and terrorist organisations use financial institutions to move and store assets, and the legal and regulatory responses in developing preventive measures.
- **Recent Developments in International Monetary Fund Involvement in Anti-Money Laundering and Combating the Financing of Terrorism Matters** – A publication created in 2005 summarising recent developments in the fight against money laundering and terrorist financing, including, but not limited to, the expanded role of the IMF, the Offshore Financial Center (OFC) Program, the Financial Services Assessment Program (FSAP), and revisions to FATF's Forty plus Nine Recommendations.
- **Financial Sector Assessment Program (FSAP)** – The FSAP is a voluntary, comprehensive and in-depth analysis of a country's financial sector designed to help increase the effectiveness of efforts to promote the soundness of financial systems, including AML/CFT systems, in member countries which result in Financial System Stability Reports (FSSRs). In 2008, the Offshore Financial Center (OFC) Assessment Program was integrated into the FSAP Program. The OFC Assessment Program executes detailed assessments of the extent to which OFCs meet international standards.
- **Financial Intelligence Units: An Overview** – A publication created in 2004 that provides an overview of financial intelligence units (FIUs), including, but not limited to, information on how to establish an FIU, core functions and international assessments of FIUs.
- **The Impact of Terrorism on Financial Markets** – A publication created in 2005 that details how financial markets have reacted to terrorism.
- **Suppressing the Financing of Terrorism – A Handbook for Legislative Drafting** – A publication created in 2003 that summarises international measures to combat terrorist financing and provides guidance on topics such as criminalising the financing of terrorism; freezing, seizing and confiscating terrorist assets; establishing jurisdiction; international cooperation; alternative remittance systems; and nonprofit organisations.
- **Regulatory Frameworks for Hawalas and Other Remittance Systems** – A publication created in 2005 that summarises the regulatory frameworks for hawalas and other informal remittance systems. For additional guidance on informal value transfer systems (IVTS), please refer to the Money Services Businesses and Informal Value Transfer Systems sections.

2923. What is the International Organisation of Securities Commissions?

The International Organisation of Securities Commissions (IOSCO), established in 1983, is a global cooperative body recognised as the international standard setter for securities markets. With a membership that regulates more than 95 percent of the world's securities markets in over 100 jurisdictions, IOSCO is the primary international cooperative forum for securities market regulatory agencies.

2924. What key AML/CFT guidance has IOSCO provided?

Key AML/CFT publications issued by the International Organisation of Securities Commissions (IOSCO) include, but are not limited to, the following:

- **Anti-Money Laundering Guidance For Collective Investment Schemes** – Final Report (October 2005) – This publication lays out the principles endorsed by IOSCO to address the application of the client due diligence process in the securities industry and describes the FATF's Forty Recommendations on combating money laundering and the financing of terrorism.
- **Initiatives by the BCBS, IAIS and IOSCO to Combat Money Laundering and the Financing of Terrorism** (January 2005) – This report offers guidance to address vulnerabilities in combating money laundering and the financing of terrorism in the banking, insurance and securities sectors.
- **Report on Money Laundering** – This report, created in 1992, summarises the growing concerns of money laundering in the securities sector and recommendations to combat money laundering including, but not limited to, the FATF's Forty Recommendations.
- **Reports on Various Topics**:
    - Special Purpose Entities (SPEs):
        - Special Purpose Entities (2007)
        - Report on Special Purpose Entities, Joint Forum (IOSCO, BCBS and IAIS) (2009)
    - Due Diligence/Beneficial Ownership:
        - Principles on Client Identification and Beneficial Ownership for the Securities Industry (2004)
        - Resolution on Principles for Record Keeping, Collection of Information, Enforcement Powers and Mutual Cooperation (1997)
    - Cross-Border Cooperation/Information Sharing:
        - Principles Regarding Cross-Border Supervisory Cooperation – Final Report (2010)
        - Multi-jurisdictional Information Sharing – Final Report (2007)
        - A Resolution Concerning Cross-Border Transactions (1995)

- **Internet-Based Activities**: Report on Securities Activity on the Internet (Three Part Series: I, II and III) (1998, 2001 and 2003 respectively)

2925. What is Transparency International?

Transparency International (TI), founded in 1993, is a global civil society organisation with more than 100 chapters. Its mission is to fight against corruption by bringing together relevant players from government, civil society, business and media.

2926. How does one become a member of TI?

TI offers two methods of becoming a member:

- **National Chapters –** Locally established, independent chapters that partner with TI to promote and realise its anti-corruption goals.
- **Individual Members –** Individuals who are appointed as members.

Currently, there are over 100 National Chapters and over 30 Individual Members.

2927. How does TI ensure its members are in compliance with its values and principles?

National Chapters are reviewed every three years for compliance by the Membership Accreditation Committee. National Chapters face suspension or disaccreditation for continual noncompliance with TI's values and principles as summarised in the "Statement of Vision, Values and Guiding Principles of Transparency International." For example, in September 2014, the French division of TI suspended the membership of a major international bank for concealing several billion dollars of transactions with sanctioned countries (e.g., Sudan, Cuba, Iran) over an eight-year period.

Individual members are also reviewed by the Membership Accreditation Committee. Noncompliant individual members face suspension or expulsion.

2928. What key AML/CFT and anti-corruption guidance has TI provided?

Key AML/CFT and anti-corruption publications and resources issued or recommended by TI include, but are not limited to, the following:

- **Gateway: Corruption Assessment Toolbox –** A database of diagnostic tools and topic guides related to measuring corruption and identifying gaps in anti-corruption programs.
- Indices, Surveys and Assessments:
    - **The Corruption Perceptions Index** (CPI), launched in 1995, measures the perceived level of public-sector corruption in 180 countries and territories around the world based on multiple surveys. The CPI shows a country's ranking (score is based on a scale of 1 to 10, with 10 being the least corrupt), the number of surveys used to determine the score, and the confidence range of the scoring. CPI reports are published annually. In 2013, Denmark, New Zealand, Finland, Sweden, Norway, Singapore and Switzerland ranked as the least corrupt; Somalia, North Korea,

Afghanistan, Sudan, South Sudan, Libya and Iraq ranked as the most corrupt; the United States ranked as the 19th least corrupt country out of 180 jurisdictions.

  - **The Bribe Payers' Index** (BPI), launched in 1999, assesses the supply side of corruption and ranks corruption by source country and industry sector. BPI reports have been released in 2002, 2006, 2008 and 2011.
  - **The Global Corruption Barometer** (GCB) is a public opinion survey, launched in 2003, that assesses the general public's perception and experience of corruption in more than 100 countries. The latest GCP survey was released in 2013.
  - **National Integrity System Assessments** (NIS) country reports present the results of the NIS assessment in the form of a comprehensive analysis of the anti-corruption provisions and capacities in a country, including recommendations for key areas of anti-corruption reform. In 2012, TI published "Money, Politics, Power: Corruption Risks in Europe" which summarised the findings of 25 National Integrity System assessments carried out across Europe in 2011.

- **Working Papers and Global Corruption Reports** includes a series of reports on various topics related to corruption and anti-corruption practices including, but not limited to, the following:
  - Transparency in Corporate Reporting: Assessing Emerging Market Multinationals (2016)
  - Whistleblowing Overview Series (Various Countries) (2016) (Jordan, Palestine, Tunisia, Lebanon, Egypt, Morocco, Yemen)
  - Fighting Corruption, Demanding Justice – Impact Report (2016)
  - Tax Systems: A Channel for Corruption or A Way to Fight It? (2015)
  - Just for Show? Reviewing G20 Promises on Beneficial Ownership (2015)
  - Technical Guide: Implementing the G20 Beneficial Ownership Principles (2015)
  - Exporting Corruption: Progress Report 2015: Assessing Enforcement of the OECD Convention on Combating Foreign Bribery (2015)
  - Integrity of Public Officials in EU Countries: International Norms and Standards (2015)
  - Policy Brief: Closing Banks to the Corrupt: The Role of Due Diligence and PEPs (2014)
  - Anti-Corruption Kit: 15 Ideas for Young Activists (2014)
  - 2015 and Beyond: The Governance Solution for Development (2013)
  - Business Principles for Countering Bribery: A Multi-Stakeholder Initiative Led by Transparency International (2013)
  - Corporate Responsibility and Anti-Corruption: The Missing Link? (2010)

  - Making Government Anti-Corruption Hotlines Effective (2009)
  - Corruption and Local Government (2012)
  - Corruption in the [Middle East and North Africa] MENA Region: A Declining Trend or More of the Same? (2008)
  - Corruption and Sport: Building Integrity and Preventing Abuses (2009)
  - Recovering Stolen Assets: A Problem of Scope and Dimension (2011)
  - Corruption in the Land Sector (2011)
  - Corruption and Human Trafficking (2011)
  - Corruption and Public Procurement (2010)
  - Corruption and (In)security (2008)
  - Accountability and Transparency in Political Finance (2008)
  - Education (2013)
  - Climate Change (2011)
  - Corruption and the Private Sector (2009)
  - Corruption in Judicial Systems (2007)
  - Corruption and Health (2006)
  - Political Corruption (2004)
- **Policy Positions** includes a series of publications that provide guidance in developing anti-corruption policies, including, but not limited to, the following:
  - Controlling Corporate Lobbying and Financing of Political Activities (2009)
  - Building Corporate Integrity Systems to Address Corruption Risks (2009)
  - Making Anti-Corruption Regulation Effective for the Private Sector (2009)
  - Countering Cartels to End Corruption and Protect the Consumer (2009)
  - Strengthening Corporate Governance to Combat Corruption (2009)
  - Political Finance Regulations: Bridging the Enforcement Gap (2009)
  - Effectively Monitoring the United Nations Convention against Corruption (UNCAC) (2011)
  - Standards on Political Funding and Favours (2009)
- **Policy Briefs** including, but not limited to, the following:
  - Regulating Luxury Investments: What Dirty Money Can't Buy (2014)
  - Leaving the Corrupt at the Door: From Denial of Entry to Passport Sales (2014)

  - Ending Secrecy to End Impunity: Tracing the Beneficial Owner (2014)

- The **Anti-Corruption Research News** provides users with insights and activities in anti-corruption research on knowledge gaps and emerging risks, curriculum development, jobs, funding opportunities and research events on a quarterly basis.
- The **Anti-Corruption Plain Language Guide** provides standardised definitions for key terms commonly used by the anti-corruption movement.

RESOURCES

Supplemental New York FAQ: Part 504: Transaction Monitoring and Filtering Program Requirements and Certifications

Although the primary focus of the AML FAQ is on federal laws and regulations and the expectations of federal regulators, we believe the enactment in 2016 by the New York Department of Financial Services (DFS) of a first of its kind certification program for transaction monitoring and filtering programs warrants its own discussion. The following questions and answers relate to Part 504 of the DFS's Superintendent's Regulations, Transaction Monitoring and Filtering Program Requirements and Certifications. Certain of the responses are likely to evolve once the DFS begins examining for compliance with Part 504 and receives the initial round of certifications.

2929. Why did the DFS propose and ultimately implement Part 504?

DFS was not satisfied with the actions being taken by the financial institutions it regulates to "detect, weed out and prevent illicit transactions." The December 1, 2015 press release that accompanied the proposed Part 504 regulation indicated that the DFS, as a result of investigations it had conducted over a four-year period, had uncovered "serious shortcomings in the transaction monitoring and filtering programs … and that a lack of robust governance, oversight, and accountability at senior levels … had contributed to these shortcomings."

2930. What types of institutions are covered by Part 504?

Part 504 applies broadly to two types of financial institutions:

DFS-regulated bank institutions: banks, trust companies, private bankers, savings banks and savings and loan associations chartered under New York Banking Law and all foreign bank branches and agencies licensed under New York Banking Law to conduct operations in New York.

DFS-regulated nonbank institutions: check cashers and money transmitters licensed under New York Banking Law.

2931. When is Part 504 effective?

Part 504 became effective on January 1, 2017.

2932. When is the first Part 504 annual certification due?

The initial annual certification must be submitted by April 15, 2018 for the 2017 calendar year. Thereafter, annual certifications must be submitted by April 15 of each year for the prior calendar year.

2933. Is the certification for a point in time, i.e., as of a certain date, or for a set period?

The certification must cover the preceding calendar year.

2934. Who must submit the annual certification?

Part 504 allows for the annual certification to be submitted either by the board of directors (which is defined as the governing body or functional equivalent) or by a senior officer which can be an individual or individuals responsible for the management, operations, compliance and/or risk management of a covered institution.

2935. For the New York branch or agency of a foreign bank, can the senior officer be an individual(s) from head office rather than a representative(s) of the branch or agency?

Since the foreign bank branch or agency and the head office are the same legal entity, presumably individual(s) from head office could be the certifying senior officer(s) if they are responsible for the management, operations, compliance and/or risk management of the branch or agency. Unless transaction monitoring or filtering programs are directed from head office, however, such remote individuals may not have sufficient knowledge or understanding of the branch or agency's programs to feel comfortable certifying.

2936. What specifically must be included in the certification?

The final Part 504 rule includes a format (Attachment A) which must be used for the annual certification. Specifically, the board of directors or senior officer(s) must certify that:

- The board of directors or senior officer(s) has reviewed documents, reports, certifications and opinions of such officers, employees, representatives, outside vendors and other individuals as necessary to provide the certification.
- The board of directors or senior officer(s) has taken all steps necessary to confirm that the New York regulated institution has a Transaction Monitoring and Filtering Program (e.g., a sanctions screening program) that complies with the Program requirements; and
- To the best of the board's or senior officer's knowledge, the Transaction Monitoring and Filtering Program of the regulated institution for the prior year complies with the Program requirements.

2937. What does Part 504 require?

Part 504 requires covered institutions to:

- Develop and maintain customised, risk-based transaction monitoring and filtering programs;
- Certify annually to the DFS that the institution is in compliance with Part 504 requirements; and
- Develop and document remediation plans, for self-identified areas, systems or processes that require material improvement and make this information available to the DFS upon request.

2938. What are the key components of a customised, risk-based transaction monitoring program?

Section 504.3 of Part 504 requires that a customised, risk-based monitoring program include, at a minimum, the following attributes:

- Be based on the risk assessment of the institution;
- Reflect all applicable current BSA/AML laws, regulations and alerts, as well as any relevant information available from the institution's related programs and initiatives, such as "know your customer due diligence," "enhanced customer due diligence" or other relevant areas, such as security, investigations and fraud prevention;
- Map BSA/AML risks to the institution's businesses, products, services, and customers/counterparties;
- Utilise BSA/AML detection scenarios that are based on the institution's risk assessment with threshold values and amounts set to detect potential money laundering or other suspicious activities;
- Include an end-to-end, pre- and post-implementation testing of the Transaction Monitoring Program, including governance, data mapping, transaction coding, detection scenario logic, model validation, data input and program output, as well as periodic testing;
- Include easily understandable documentation that articulates the institution's current detection scenarios and the underlying assumptions, parameters, and thresholds;
- Include investigative protocols detailing how alerts generated by the Transaction Monitoring Program will be investigated, the process for deciding which alerts will result in a filing or other action, who is responsible for making such a decision, and how investigative and decision-making processes will be documented; and
- Be subject to an ongoing analysis to assess the continued relevancy of the detection scenarios, the underlying rules, threshold values, parameters, and assumptions.

2939. What are the key components of a customised, risk-based filtering program?

Similar to the requirements for a transaction monitoring program, a customised, risk-based filtering program should include, at a minimum, the following attributes:

- Be based on the risk assessment of the institution;
- Be based on technology or tools for matching names and accounts, in each case based on the institution's particular risks, transaction and product profiles;
- Include an end-to-end, pre- and post-implementation testing of the Watch List Filtering Program, including data mapping, an evaluation of whether the watch lists and threshold settings map to the risks of the institution, the logic of matching technology or tools, model validation, and data input and Watch List Filtering Program output;
- Utilises watch lists that reflect current legal or regulatory requirements;
- Be subject to ongoing analysis to assess the logic and performance of the technology or tools for matching names and accounts, as well as the watch lists and the threshold settings to see if they continue to map to the risks of the institution; and

- Include easily understandable documentation that articulates the intent and the design of the program tools or technology.

2940. Are there requirements in Part 504 that apply to both transaction monitoring and filtering programs?

There are a number of overarching requirements that apply to both programs. These include:

- Identification of all relevant data sources;
- Validation of the integrity, accuracy and quality of data on which the programs rely;
- Data extraction and loading processes to ensure complete and accurate transfer of data for automated systems;
- Governance and management oversight;
- Robust vendor selection process and ongoing vendor management;
- Appropriate funding;
- Qualified personnel to execute the programs; and
- Periodic training of all stakeholders with respect to the programs.

2941. What does a covered financial institution need to do to meet the compliance requirements of Part 504?

For a covered financial institution to submit a Part 504 certification with confidence, many different people and groups across the institution will need to be involved in the certification process. Key stakeholders may include, but not necessarily be limited to, individuals or departments responsible for:

- Program governance
- Risk assessment
- Know your customer
- Data and analytics
- Model validation
- Transaction monitoring and investigation
- Sanctions screening and adjudication
- Program monitoring
- Information technology
- Third-party risk management
- Internal audit

The most effective way for a covered financial institution to manage its compliance effort, especially in year one, is to form a Part 504 Project Management Office (PMO) with representatives of all affected areas. The PMO should develop a comprehensive, multi-phased, high-level project plan that includes identifying in-scope processes and technologies and their owners, gathering and testing supporting controls early enough to identify and remediate significant weaknesses, reviewing and signing-off on supporting documentation, and submitting the annual certification.

2942. What are some of the baseline documentation requirements for automated transaction monitoring and filtering systems?

Baseline document standards would include, but not necessarily be limited to:

- System selection due diligence, including vendor scorecards
- Vendor contract (establishing roles and responsibilities, training and ongoing level of support)
- System and data mapping (including rationale for any exclusions)
- Rationale for rule/scenario selection and threshold setting
- User manuals/desktop procedures
- Staffing needs analysis
- Performance measurement standards
- Training documentation
- Model Governance Policy (including, but not limited to, requirements for ongoing tuning, change management, validation and business continuity)

2943. Are manual transaction monitoring and sanctions screening processes outside of the scope of Part 504?

Part 504 is aimed at ensuring that covered financial institutions have comprehensive transaction monitoring and filtering programs. Manual processes, to the extent they exist, should, therefore, be included to evidence program completeness.

2944. How should an institution test that Program controls are effective and the Program is operating as intended?

An institution can use a combination of different means for confirming that controls are effective. These could include monitoring performed by compliance, testing conducted by Internal Audit and/or special control reviews executed by other internal or external parties. However, covered institutions must remember that they must certify to the effectiveness of their Program for the entire preceding year so will likely want to schedule periodic control testing throughout the year or at least at different points in the year so they can confidently submit the certification.

2945. What should the role of internal audit be in the Part 504 compliance effort?

In many institutions, Internal Audit will play a lead role in performing the testing required to evidence that the institution is complying with its transaction monitoring and filtering program policies and procedures. Even before that, Internal Audit may be charged with ensuring that the institution has developed a comprehensive Part 504 project plan and for monitoring adherence to that project plan to ensure that the institution will be prepared to certify.

2946. Given the complexity of Part 504 and the breadth of different stakeholders likely to be involved in the compliance effort, how will the final certifier be comfortable signing off?

Covered institutions will need to develop a body of evidence to support compliance and certifiers will want to review this documentation carefully and perhaps seek the advice of third parties, e.g., Internal Audit or third-party advisers, on the sufficiency of the documentation. That said, however, many institutions are likely to model their Part 504 compliance programs after Sarbanes-Oxley Act compliance programs, which typically rely on a sub-certification process in which all key stakeholders are required to certify compliance in their respective areas and the final certifier relies not only on the documentation developed, but also on the attestations of these responsible parties. Ultimately, the final certifier remains responsible for the accuracy of the certification.

2947. What constitutes a "material improvement" to an area, system or process?

"Material improvement" is not defined in the regulation. Absent further guidance from the DFS, it is reasonable to think that a material improvement is one that, if it is not made, may undermine the effectiveness of the transaction monitoring or filtering program. For example, known deficiencies in the extent or functioning of detection scenarios might warrant material improvement, while opportunities to enhance generally satisfactory policies and procedures may be viewed as an enhancement opportunity that can be carried out in the normal course of business.

2948. How does Part 504 differ from what the federal regulators expect of their supervised institutions?

Many facets of Part 504 are contained in existing federal regulatory guidance including, but not limited to FRB (SR 11-7) and OCC (OCC 2011-12) *Sound Practices for Model Risk Management*, the FFIEC *BSA/AML Examination Manua*l and FFIEC *IT Examination Handbook*.

What makes Part 504 different is, first and foremost, it is a regulation, not guidance, which means that the consequences for noncompliance may be more direct and severe. Additionally, Part 504, in its expansiveness, requires covered institutions to demonstrate the linkage among program elements in a more comprehensive way than federal regulators have typically required, whereby material weaknesses in any one program element may jeopardise the overall effectiveness of the program.

2949. What are likely to be the significant Part 504 challenges faced by covered financial institutions?

Challenges are likely to vary significantly across covered financial institutions, but may include the following:

- Nonavailability of current and complete data mapping from all relevant source systems to transaction monitoring and filtering systems;
- Inability to explain historical decisions to exclude certain source system data (e.g., certain products, transaction types) from transaction monitoring and filtering systems;
- No or inadequate testing of data completeness and integrity;
- Lack of alignment between the covered financial institution's AML and sanctions risk assessments and transaction monitoring and filtering systems, respectively, e.g., not all products and services covered by the AML risk assessment are included in the transaction monitoring program;
- Lack of robust automated systems;
- Insufficient documentation supporting the selection, initial calibration, testing and ongoing use, tuning and validation of transaction monitoring and filtering systems;
- Inadequate ongoing third-party risk management of vendor-provided systems;
- Inadequate policies and procedures for disposition of AML and sanctions alerts;
- Inadequate numbers of sufficiently trained staff to ensure timely and well-supported adjudication of transaction monitoring alerts and sanction "hits"; and
- Non-existent or poor management reporting.

2950. Are foreign bank branches and agencies likely to encounter any unique challenges?

For foreign bank branches and agencies that have self-contained transaction monitoring and filtering programs, i.e., they have unique systems that are not part of a global installation or are unique instances of a global installation, the challenges should be the same as for domestic institutions.

Foreign banks that rely on global transaction monitoring and filtering systems that were selected and are governed by head office (or another office of the foreign bank) may be additionally challenged in demonstrating their understanding of the systems; that the systems meet the unique needs of the branch or agency; and in providing the documentation expected by DFS to evidence the selection, installation, ongoing tuning, validation, and data integrity of the systems deployed.

2951. Are money transmitters and check cashers likely to encounter any unique challenges?

Many money transmitters and check cashers have small compliance departments and rely more on informal processes and outsourcing to meet their compliance needs. Such institutions may be especially challenged to meet the documentation standards implicit in Part 504.

2952. What should a financial institution do if it identifies gaps in its transaction monitoring and/or filtering program?

If an institution identifies a gap in its transaction monitoring or filtering program, it will first need to decide whether the gap represents a situation which requires a material improvement. If so, the institution should:

- Document the gap and how it was identified;
- Develop and implement a remediation plan for addressing the gap; and
- Make available to the DFS, upon request, information on the gap and the related remediation efforts.

Any gaps that require material improvement that remain unresolved at the time of certification will affect the institution's ability to certify to its compliance program; therefore, progress toward redressing any significant gaps should be closely monitored.

2953. What should an institution do if it identifies gaps that it does not consider significant or requiring material improvement?

Less significant gaps or process improvements should still be addressed, but these can be handled in the normal course of business and do not require development of a specific remediation plan as is necessary for gaps requiring material improvement.

2954. What does an institution do when it needs to submit a certification but knows that it has outstanding gaps that require material improvement?

The certification form (Attachment A) does not explicitly allow for institutions to qualify their certifications. However, since it would be ill-advised for an institution to submit a certification which it knows to be inaccurate, the certifier will likely want to annotate the certification to include outstanding gaps that require material improvements and the status of remediation efforts. The institution should consult with counsel on the best way to handle this disclosure.

2955. What are the consequences for failing to comply with Part 504?

Failure to comply with Part 504 subjects a financial institution and responsible parties to the full range of enforcement authorities available to the DFS. This includes, under existing law, holding individuals criminally liable for violations.

2956. Are there any strategic alternatives available to avoid having to comply with Part 504?

Regulated institutions can consider relocating and converting their license to another state or converting to a national/federal charter. However, any such decision should be subject to a thorough cost-benefit analysis and institutions considering either of these alternatives should know that regulators may not accept/approve charter conversion applications from institutions experiencing regulatory problems.

2957. How can a financial institution reduce the ongoing Part 504 compliance effort in future years?

For most financial institutions, Part 504 compliance in year one will be structured as a project. The keys to reducing the compliance effort in future years will be to mine all the lessons learned in year one (what worked well and what didn't) and to transform the project into an ongoing process which can be embedded into the institution's operations.

2958. What are some of the important considerations for transforming a project to a process?

Considerations will vary based on how an institution structured its initial project plan, but may include:

- Resetting the foundation to eliminate steps that did not provide value;
- Adjusting timing of certain steps to recognise interdependencies, achieve efficiencies, and facilitate the process;
- Refining the governance structure and clarifying responsibilities and accountability; and
- Acting on the improvement opportunities that were identified as part of accumulating the "lessons learned."

Key U.S. AML/CFT and Sanctions Laws and Regulations

In addition to our direct experience working with companies on AML/CFT projects, both in the United States and other jurisdictions, we used a variety of resources to respond to the questions posed. These included regulatory publications, issuances and guidance published by other governmental and law enforcement agencies, industry publications, and media reports. The following chart identifies some of the key resources used.

Specific guidance is further detailed within various sections of this guide.

31 U.S.C. §§ 5311-5314, 5316-5326, 5328-5332; 12 USC 1829b; 12 USC 1951-1959	Bank Secrecy Act (BSA)
31 U.S.C. § 5311	Declaration of purpose
31 U.S.C. § 5312	Definitions and application
31 U.S.C. § 5313	Reports on domestic coins and currency transactions (CTR)
31 U.S.C. § 5314	Records and reports on foreign financial agency transactions
31 U.S.C. § 5316	Reports on exporting and importing monetary instruments (CMIR)
31 U.S.C. § 5317	Search and forfeiture of monetary instruments
31 U.S.C. § 5318	Compliance, exemptions and summons authority
31 U.S.C. § 5319	Availability of reports
31 U.S.C. § 5320	Injunctions
31 U.S.C. § 5321	Civil penalties
31 U.S.C. § 5322	Criminal penalties
31 U.S.C. § 5323	Rewards for informants
31 U.S.C. § 5324	Structuring transactions to evade reporting requirement prohibited

31 U.S.C. § 5325	Identification required to purchase certain monetary instruments
31 U.S.C. § 5326	Records of certain domestic coin and currency transactions
31 U.S.C. § 5328	Whistleblower protections (Safe Harbor)
31 U.S.C. § 5329	Staff commentaries
31 U.S.C. § 5330	Registration of money transmitting businesses
31 U.S.C. § 5331	Reports relating to coins and currency received in nonfinancial trade or business (Form 8300)
31 U.S.C. § 5332	Bulk cash smuggling into or out of the United States
12 U.S.C. § 1829b	Retention of records by insured depository institutions
12 U.S.C. § 1951	Congressional findings and declaration of purpose
12 U.S.C. § 1952	Reports on ownership and control
12 U.S.C. § 1953	Recordkeeping and procedures
12 U.S.C. § 1954	Injunctions
12 U.S.C. § 1955	Civil penalties
12 U.S.C. § 1956	Criminal penalty
12 U.S.C. § 1957	Additional criminal penalty in certain cases
12 U.S.C. § 1958	Compliance
12 U.S.C. § 1959	Administrative procedure
Pub. L. 107-26	Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act): • Subtitle A: International Counter Money Laundering and Related Measures • Subtitle B: Bank Secrecy Act Amendments and Related Improvements • Subtitle C: Currency Crimes and Protection
Title III: Subtitle A: Section 302	Findings and purposes
Title III: Subtitle A: Section 303	4-year congressional review; expedited consideration
Title III: Subtitle A: Section 311	Special measures for jurisdictions, financial institutions, or international transactions of primary money laundering concern
Title III: Subtitle A: Section 312	Special due diligence for correspondent accounts and private banking accounts
Title III: Subtitle A: Section 313	Prohibition on United States correspondent accounts with foreign shell banks

Title III: Subtitle A: Section 314	Cooperative efforts to deter money laundering
Title III: Subtitle A: Section 315	Inclusion of foreign corruption offenses as money laundering crimes
Title III: Subtitle A: Section 316	Anti-terrorist forfeiture protection
Title III: Subtitle A: Section 317	Long-arm jurisdiction over foreign money launderers
Title III: Subtitle A: Section 318	Laundering money through a foreign bank
Title III: Subtitle A: Section 319	Forfeiture of funds in United States interbank accounts
Title III: Subtitle A: Section 320	Proceeds of foreign crimes
Title III: Subtitle A: Section 321	Financial institutions specified in Subchapter II of Chapter 53 of Title 31, United States Code
Title III: Subtitle A: Section 322	Corporation represented by fugitive
Title III: Subtitle A: Section 323	Enforcement of foreign judgments
Title III: Subtitle A: Section 324	Report and recommendation
Title III: Subtitle A: Section 325	Concentration accounts at financial institutions
Title III: Subtitle A: Section 326	Verification of identification (CIP)
Title III: Subtitle A: Section 327	Consideration of anti-money laundering record
Title III: Subtitle A: Section 328	International cooperation on identification of originators of wire transfers
Title III: Subtitle A: Section 329	Criminal penalties
Title III: Subtitle A: Section 330	International cooperation in investigations of money laundering, financial crimes and the finances of terrorist groups
Title III: Subtitle B: Section 351	Amendments relating to reporting of suspicious activities
Title III: Subtitle B: Section 352	Anti-money laundering programs (AML Programs)
Title III: Subtitle B: Section 353	Penalties for violations of geographic targeting orders and certain recordkeeping requirements and lengthening effective period of geographic targeting orders
Title III: Subtitle B: Section 354	Anti-money laundering strategy
Title III: Subtitle B: Section 355	Authorisation to include suspicions of illegal activity in written employment references
Title III: Subtitle B: Section 356	Reporting of suspicious activities by securities brokers and dealers; investment company study
Title III: Subtitle B: Section 357	Special report on administration of bank secrecy provisions
Title III: Subtitle B: Section 358	Bank secrecy provisions and activities of United States intelligence agencies to fight international terrorism
Title III: Subtitle B: Section 359	Reporting of suspicious activities by underground banking systems

Title III: Subtitle B: Section 360	Use of authority of United States executive directors
Title III: Subtitle B: Section 361	Financial Crimes Enforcement Network
Title III: Subtitle B: Section 362	Establishment of highly secure network
Title III: Subtitle B: Section 363	Increase in civil and criminal penalties for money laundering
Title III: Subtitle B: Section 364	Uniform protection authority for Federal Reserve facilities
Title III: Subtitle B: Section 365	Reports relating to coins and currency received in nonfinancial trade or business
Title III: Subtitle B: Section 366	Efficient use of currency transaction report system
Title III: Subtitle C: Section 371	Bulk cash smuggling into or out of the United States
Title III: Subtitle C: Section 372	Forfeiture in currency reporting cases
Title III: Subtitle C: Section 373	Illegal money transmitting businesses
Title III: Subtitle C: Section 374	Counterfeiting domestic currency and obligations
Title III: Subtitle C: Section 375	Counterfeiting foreign currency and obligations
Title III: Subtitle C: Section 376	Laundering the proceeds of terrorism
Title III: Subtitle C: Section 377	Extraterritorial jurisdiction
Title V: Section 505	Miscellaneous National Security Authorities
15 U.S.C. 1593 et seq.	Electronic Fund Transfer Act
18 U.S.C. §§ 1956 and 1957	Money Laundering Control Act of 1986 (MLCA)
Pub L. No. 100-690, 102 Stat. 4181 (codified as amended in scattered sections of the U.S.C.) (2012)	Anti-Drug Abuse Act of 1988
Pub L. No. 102-550, 106 Stat. 4044 (codified as amended in scattered sections of the U.S.C.) (2012)	Annunzio-Wylie Anti-Money Laundering Act of 1992
31 U.S.C. §§ 5301, note 5330 (2012)	Money Laundering Suppression Act of 1994 (MLSA)
31 U.S.C. §§ 5301, 5340-5341, 5351-5355 (2012)	Money Laundering and Financial Crimes Strategy Act of 1998
Pub L. No. 108-458, 118 Stat. 3638 (codified as amended in scattered sections of the U.S.C.) (2012)	Intelligence Reform and Terrorism Prevention Act of 2004
31 C.F.R. Chapter X	Financial recordkeeping and reporting of currency and foreign transactions
31 C.F.R. Chapter X § 1010.205(a)-(d)	Exempted anti-money laundering programs for certain financial institutions
31 C.F.R. Chapter X § 1010.314(a)-(c)	Structured transactions

31 C.F.R. Chapter X 1010.306(a)(1)-(e)	Filing of reports (CTR, CMIR, FBAR)
31 C.F.R. Chapter X 1010.306(a)(2)&(3); § 1010.306(d)-(e)	CTR exemption recordkeeping requirements
31 C.F.R. Chapter X § 1010.311(a)-(c)	Filing obligations for reports of transactions in currency
31 C.F.R. Chapter X § 1010.312	Identification requirements
31 C.F.R. Chapter X § 1010.313(a)-(b)	Aggregation multiple branches; multiple transactions – general
31 C.F.R. Chapter X § 1010.314	Structured transactions
31 C.F.R. Chapter X § 1010.330	Reports relating to currency in excess of $10,000 received in a trade or business (Form 8300)
31 C.F.R. Chapter X § 1010.340	Reports of transportation of currency or monetary instruments (CMIR)
31 C.F.R. Chapter X § 1010.350	Reports of foreign bank and financial accounts (FBAR)
31 C.F.R. Chapter X § 1010.360	Reports of transactions with foreign financial agencies
31 C.F.R. Chapter X § 1010.370	Reports of certain domestic coin and currency transactions
31 C.F.R. Chapter X § 1010.410	Records to be made and retained by financial institutions (funds transfer recordkeeping and transmittal requirements)
31 C.F.R. Chapter X § 1010.415	Purchases of bank checks and drafts, cashier's checks, money orders and traveller's checks
31 C.F.R. Chapter X § 1010.430 (a)(d)	Nature of records and retention period
31 C.F.R. Chapter X § 1010.440	Person outside the United States
31 C.F.R. Chapter X § 1010.520	Information sharing between federal law enforcement agencies and financial institutions (314(a))
31 C.F.R. Chapter X § 1010.540	Voluntary information sharing among financial institutions (314(b))
31 C.F.R. Chapter X § 1010.610	Due diligence programs for correspondent accounts for foreign financial institutions
31 C.F.R. Chapter X § 1010.620(a)-(e)	Due diligence programs for private banking accounts
31 C.F.R. Chapter X § 1010.630(a)-(f)	Prohibition on correspondent accounts for foreign shell banks; records concerning owners of foreign banks and agents for service of legal process
31 C.F.R. Chapter X § 1010.651	Special measures against Burma
31 C.F.R. Chapter X § 1010.652 (a)-(b)	Special measures against Myanmar Mayflower Bank and Asia Wealth Bank
31 C.F.R. Chapter X § 1010.653	Special measures against Commercial Bank of Syria
31 C.F.R. Chapter X § 1010.654	Special measures against VEF Bank
31 C.F.R. Chapter X § 1010.655	Special measures against Banco Delta Asia

31 C.F.R. Chapter X § 1010.670(a)-(f)	Summons or subpoena of foreign bank records; termination of correspondent relationship
31 C.F.R. Chapter X § 1010.710	Administrative rulings scope
31 C.F.R. Chapter X § 1010.711(a)-(e)	Submitting requests
31 C.F.R. Chapter X § 1010.712	Nonconforming requests
31 C.F.R. Chapter X § 1010.713(a)(b)	Oral communications
31 C.F.R. Chapter X § 1010.714	Withdrawing requests
31 C.F.R. Chapter X § 1010.715	Issuing rulings
31 C.F.R. Chapter X 1010.716(a)-(d)	Modifying or rescinding rulings
31 C.F.R. Chapter X § 1010.717(a)(b)	Disclosing information
31 C.F.R. Chapter X § 1010.810(a)-(g)	Enforcement
31 C.F.R. Chapter X § 1010.820(a)-(h)	Civil penalty
31 C.F.R. Chapter X § 1010.830	Forfeiture of currency or monetary instruments
31 C.F.R. Chapter X § 1010.840 (a)-(d)	Criminal penalty
31 C.F.R. Chapter X § 1010.850 (a)-(c)	Enforcement authority with respect to transportation of currency or monetary instruments
31 C.F.R. Chapter X § 1010.911	Summons-General
31 C.F.R. Chapter X § 1010.912(a)-(c)	Persons who may issue summons
31 C.F.R. Chapter X § 1010.913(a)&(b)	Contents of summons
31 C.F.R. Chapter X § 1010.914(a)-(c)	Service of summons
31 C.F.R. Chapter X § 1010.915(a)-(c)	Examination of witnesses and records
31 C.F.R. Chapter X § 1010.916	Enforcement of summons
31 C.F.R. Chapter X § 1010.917	Payment of expenses
31 C.F.R. Chapter X § 1010.920	Access to records
31 C.F.R. Chapter X § 1010.930(a)-(c)	Rewards for informants
31 C.F.R. Chapter X § 1010.940(a)&(b)	Photographic or other reproductions of Government obligations
31 C.F.R. Chapter X § 1010.950(a)-(f)	Availability of information
31 C.F.R. Chapter X § 1010.960	Disclosure
31 C.F.R. Chapter X § 1010.970(a)-(c)	Exceptions, exemptions, and reports
31 C.F.R. Chapter X § 1010.980	Dollars as including foreign currency

31 C.F.R. Chapter X § § 1020.100(d)(1); 1023.100(e) (1); 1010.100; 1020.210; 1023.210(a)(b); 1026.210(b)(1)&(2)	Anti-money laundering program requirements for financial institutions regulated by a federal functional regulator or a self-regulatory organisation, and casinos (AML Program)
31 C.F.R. Chapter X § 1020.100; 1020.220	Customer identification programs for banks, savings associations, credit unions, and certain non-federally regulated banks (CIP)
31 C.F.R. Chapter X § 1020.315(a)-(i)	Transactions of exempt persons
31 C.F.R. Chapter X § 1020.320(a)-(f)	Reports by banks of suspicious transactions (SAR)
31 C.F.R. Chapter X § 1020.410 (b)(c)	Additional records to be made and retained by banks
31 C.F.R. Chapter X § 1021.100	Special terms for casinos
31 C.F.R. Chapter X § 1021.210(a)	Requirements for casinos
31 C.F.R. Chapter X § 1021.210(b)	Compliance programs casinos
31 C.F.R. Chapter X § 1021.313	Aggregation - casinos
31 C.F.R. Chapter X § 1021.320(a)-(g)	Reports by casinos of suspicious transactions (SAR)
31 C.F.R. Chapter X § 1021.410 (a)-(c)	Additional records to be made and retained by casinos
31 C.F.R. Chapter X § 1022.420	Additional records to be maintained by providers and sellers of prepaid access
31 C.F.R. Chapter X § 1022.210(a)-(e)	Anti-money laundering programs for money services businesses (MSB) (AML Program)
31 C.F.R. Chapter X § 1022.320(a)-(f)	Reports by money services businesses (MSB) of suspicious transactions (SAR)
31 C.F.R. Chapter X § 1022.380(a)-(f)	Registration of money services businesses (MSB)
31 C.F.R. Chapter X § 1022.410 (a)-(c)	Additional records to be made and retained by currency dealers or exchangers
31 C.F.R. Chapter X § 1023.100; 1023.220	Customer identification programs for broker-dealers (CIP)
31 C.F.R. Chapter X § 1023.320(a)-(h)	Reports by brokers or dealers in securities of suspicious transactions (SAR)
31 C.F.R. Chapter X § 1023.410 (a)(b)	Additional records to be made and retained by brokers or dealers in securities
31 C.F.R. Chapter X § 1024.100; 1010.100; 1010.605	Customer identification programs for mutual funds (CIP)
31 C.F.R. Chapter X § 1024.210(a)(b);	Anti-money laundering programs for mutual funds (AML Program)
31 C.F.R. Chapter X § 1024.320(a)-(g)	Reports by mutual funds of suspicious transactions (SAR)
31 C.F.R. Chapter X § 1025.100; 1025.210(a)-(d):	Anti-money laundering programs for insurance companies (AML Program)
31 C.F.R. Chapter X § 1025.320(a)-(h)	Reports by insurance companies of suspicious transactions (SAR)

31 C.F.R. Chapter X § 1026.100; 1026.220	Customer identification programs for futures commission merchants and introducing brokers (CIP)
31 C.F.R. Chapter X § 1026.320(a)-(h)	Reports by futures commission merchants and introducing brokers in commodities of suspicious transactions (SAR)
31 C.F.R. Chapter X § 1027.100; 1027.210(a)-(c);	Anti-money laundering programs for dealers in precious metals, precious stones or jewels (AML Program)
31 C.F.R. Chapter X § X 1028.100; 1028.210 (a)(b)	Anti-money laundering programs for operators of credit card systems (AML Program)
31 C.F.R. Chapter X § X 1029.21	Anti-money laundering programs for loan or finance companies
31 C.F.R. Part 103, Appendix A to Subpart I of Part 103	Certification regarding correspondent accounts for foreign banks (foreign bank certification)
31 C.F.R. Part 103, Appendix B to Subpart I of Part 103	Recertification regarding correspondent accounts for foreign banks
31 C.F.R. Part 103, Appendix B to Part 103	Certification for purposes of Section 314(b) of the USA PATRIOT Act and 31 CFR 103.110
Pub. L. 111-195, 124 Stat. 1312 (codified as amended in scattered sections of the U.S.C.) (2010)	Comprehensive Iran Sanctions, Accountability, and Divestment Act of 2010 (CISADA)
50 U.S.C. §§ 1701-1707	International Emergency Economic Powers Act (IEEPA)
50 U.S.C. § 1701	Iran Sanctions Act of 1996 (ISA)
Pub. L. 112-158	Iran Threat Reduction and Syria Human Rights Act of 2012 (ITRSHRA)
Pub. L. 112-81	National Defense Authorisation Act for Fiscal Year 2012 (NDAA)
12 U.S.C. § 95a	Trading with the Enemy Act of 1917 (TWEA)
31 C.F.R. Part 500	Foreign Assets Control Regulations (OFAC)
31 C.F.R. Part 501	Reporting, Procedures and Penalties Regulations
31 C.F.R. Part 505	Regulations Prohibiting Transactions Involving the Shipment of Certain Merchandise Between Foreign Countries
31 C.F.R. Part 510	North Korea Sanctions Regulations
31 C.F.R. Part 515	Cuban Assets Control Regulations
31 C.F.R. Part 535	Iranian Assets Control Regulations
31 C.F.R. Part 536	Narcotics Trafficking Sanctions Regulations
31 C.F.R. Part 537	Burmese Sanctions Regulations
31 C.F.R. Part 538	Sudanese Sanctions Regulations (sanctions removed as of January 2017)
31 C.F.R. Part 539	Weapons of Mass Destruction Trade Control Regulations

31 C.F.R. Part 540	Highly Enriched Uranium (HEU) Agreement Assets Control Regulations
31 C.F.R. Part 541	Zimbabwe Sanctions Regulations
31 C.F.R. Part 542	Syrian Sanctions Regulations
31 C.F.R. Part 543	Côte d'Ivoire Sanctions Regulations
31 C.F.R. Part 544	Weapons of Mass Destruction Proliferators Sanctions Regulations
31 C.F.R. Part 545	Taliban (Afghanistan) Sanctions Regulations
31 C.F.R. Part 546	Darfur Sanctions Regulations
31 C.F.R. Part 547	Democratic Republic of the Congo Sanctions Regulations
31 C.F.R. Part 548	Belarus Sanctions Regulations
31 C.F.R. Part 549	Lebanon Sanctions Regulations
31 C.F.R. Part 551	Somalia Sanctions Regulations
31 C.F.R. Part 552	Yemeni Sanctions Regulations
31 C.F.R. Part 553	Central African Republic Sanctions Regulations
31 C.F.R. Part 554	Burundi Sanctions Regulations
31 C.F.R. Part 558	South Sudan Sanctions Regulations
31 C.F.R. Part 560	Iranian Transactions Regulations (ITR)
31 C.F.R. Part 561	Iranian Financial Sanctions Regulations (IFSR)
31 C.F.R. Part 562	Iranian Human Rights Abuses Sanctions Regulations
31 C.F.R. Part 566	Hizballah Financial Sanctions Regulations
31 C.F.R. Part 570	Libyan Sanctions Regulations
31 C.F.R. Part 575	Iraqi Sanctions Regulations
31 C.F.R. Part 576	Iraq Stabilisation and Insurgency Sanctions Regulations
31 C.F.R. Part 585	Federal Republic of Yugoslavia (Serbia and Montenegro) and Bosnian Serb-controlled Areas of the Republic of Bosnia and Herzegovina Sanctions Regulations
31 C.F.R. Part 586	Federal Republic of Yugoslavia (Serbia and Montenegro) Kosovo Sanctions Regulations
31 C.F.R. Part 587	Federal Republic of Yugoslavia (Serbia and Montenegro) Milosevic Sanctions Regulations
31 C.F.R. Part 588	Western Balkans Stabilisation Regulations
31 C.F.R. Part 589	Ukraine Related Sanctions Regulations

31 C.F.R. Part 590	Transnational Criminal Organisations Sanctions Regulations
31 C.F.R. Part 591	Venezuela Related Sanctions Regulations
31 C.F.R. Part 592	Rough Diamonds Control Regulations
31 C.F.R. Part 593	Former Liberian Regime of Charles Taylor Sanctions Regulations
31 C.F.R. Part 594	Global Terrorism Sanctions Regulations
31 C.F.R. Part 595	Terrorism Sanctions Regulations
31 C.F.R. Part 596	Terrorism List Governments Sanctions Regulations
31 C.F.R. Part 597	Foreign Terrorist Organisations Sanctions Regulations
31 C.F.R. Part 598	Foreign Narcotics Kingpin Sanctions Regulations
31 U.S.C. §§ 5361-5367	Security and Accountability For Every Port Act of 2006, Title VII: Unlawful Internet Gambling Enforcement Act of 2006 (UIGEA)
31 C.F.R. Part 132	Prohibition on funding of unlawful Internet gambling
26 U.S.C. §§ 1471-1474	Hiring Incentives to Restore Employment Act (HIRE): Title V: Subtitle A: Foreign Account Tax Compliance Act (FATCA)
17 C.F.R. § 240.17a-8	Records to be Made by Certain Exchange Members, Brokers and Dealers
17 C.F.R. § 405.4	Financial Recordkeeping and Reporting of Currency and Foreign Transactions by Registered Government Securities Brokers and Dealers
17 C.F.R. § 240.10b5-1	Trading “On the Basis of” Material and Non-public Information in Insider Trading Cases
17 C.F.R. § 240.10b5-2	Duties of Trust or Confidence in Misappropriation Insider Trading Cases
17 C.F.R. § 240.17a-3	Records to be Made by Certain Exchange Members, Brokers and Dealers
17 C.F.R. § 240.17a-4	Records to be Preserved by Certain Exchange Members, Brokers and Dealers
15 U.S.C. 1681 et seq.	Fair Credit Reporting Act
Pub. L. 114-22	Justice for Victims of Trafficking Act of 2015 (JVTA)

For additional information on the United States Code (USC), refer to http://uscode.house.gov/ and for the Code of Federal Regulations (CFR), refer to www.ecfr.gov.

Key U.S. Enforcement Actions and Settlements

Depository Institutions

Deutsche Bank AG: On May 26, 2017, the Federal Reserve Board (FRB) issued Deutsche Bank AG (DBUSA) a cease and desist order as well as a civil monetary penalty (CMP) in the amount of US$41 million for failures in compliance with the Bank Secrecy Act (BSA) and anti-money laundering (AML) and counter financing of terrorism (CFT) laws	The FRB identified the following: • Failure to maintain an effective AML Program to comply with BSA and AML/CFT laws • Insufficient senior management oversight and controls • Deficiencies in transaction monitoring capabilities preventing proper assessment for "billions of dollars in potential suspicious transactions" for which inaccurate or incomplete information was obtained from the DBUSA's foreign affiliates • Failure to staff the compliance function and train AML/CFT compliance personnel adequately • Insufficient procedures for independent testing procedures and quality assurance controls • Failure to report and escalate significant matters related to compliance risks to U.S. senior management • Deficiencies in the AML/CFT risk assessment processes, including failure to clearly define parameters regarding acceptable risks associated with specific types of customers or businesses • Inadequate measures to ensure that payment messages for cross-border funds transfers to and from the United States comply with applicable international and interagency standards for cross-border payments • Inadequate policies, procedures and controls to ensure that DBUSA collect, analyse, and retain complete and accurate customer information for all account holders
Banamex USA (BUSA): On May 18, 2017, BUSA entered into a non-prosecution agreement (NPA) with the Money Laundering and Asset Recovery Section of the U.S. Department of Justice (DOJ) and paid a US$140 million CMP to the Federal Deposit Insurance Corporation (FDIC) for wilful violations of AML/CFT laws and regulations. Three executives also paid CMPs ranging from US$30,000 to US$90,000.	The DOJ identified the following: • Failure to maintain an effective AML Program to comply with BSA and AML/CFT laws • Deficiencies in transaction monitoring capabilities that failed to monitor "millions of remittance transactions it processed to Mexico in partnership with money services businesses (MSBs)"; manual transaction monitoring program was limited, running two rules/scenarios that generated paper reports with inadequate investigation process • Failure to provide appropriate staff and resources to the AML/CFT compliance function, even after expanding MSB business into new territories • Failure to file Suspicious Activity Reports (SARs) on suspicious remittance transactions to Mexico consistent with known typologies (e.g., human smuggling, fraud, drug trafficking)
Branch Banking and Trust Company (BB&T): On January 25, 2017, the FDIC issued a cease and desist order for significant deficiencies in its firmwide AML and risk management program	The FDIC identified the following: • Failure to maintain an effective AML Program commensurate with BB&T's risk profile • Inadequate risk management program that failed to address BB&T's compliance risks in an effective and timely manner across the firm (e.g., across lines of business, support units, legal entities)

Intesa Sanpaolo S.p.A. New York Branch: On December 15, 2016, the New York State Department of Financial Services (DFS) issued a consent order to Intesa Sanpaolo S.p.A. and Intesa Sanpaolo S.p.A. New York Branch with a CMP of US$235 million.	DFS cited compliance failures at the New York branch over the last several years arising from deficiencies in the implementation and oversight of the transaction monitoring system of the New York branch, including: • Alert clearing process that deviated from documented procedures (e.g., AML Officer and compliance staff began reviewing and "clearing" significant volumes of keyword-based alerts without loading them into the case management system, as expressly required by written policy). • The algorithms designed to conduct key word searches contained programming errors. • As a result of these failures, the DFS alleged that the branch failed to review at least 17,000 alerts, totalling approximately US$16.6 billion in transactions during 2014 alone (equalling approximately 13 percent of the alerts that the system was designed to capture). • At least 6,600 Society for Worldwide Interbank Financial Telecommunications (SWIFT) messages, totalling at least US$319 million, processed by Intesa during 2005-2006 period that bore strong indicia of possible shell company activity. Of this amount, Intesa processed at least US$130 million through the New York branch without appropriate review or investigation. • From approximately 2002 to 2006, Intesa used non-transparent practices to process payments on behalf of Iranian clients and other entities.
Agricultural Bank of China New York Branch: On November 4, 2016, the New York State Department of Financial Services (DFS) issued a consent order to the Agricultural Bank of China Limited and the Agricultural Bank of China New York Branch with a CMP of US$215 million.	The DFS cited deficiencies in transaction monitoring, the Branch's risk assessment and policies, procedures and processes necessary to promote sustainability of the AML/CFT compliance program, including: • U.S. dollar transactions conducted through the Branch did not receive the important and necessary scrutiny required by state law concerning economic sanctions and AML/CFT compliance. • The Branch was specifically cautioned that its transaction monitoring systems were inadequate for its existing risks and disregarded the DFS's warning that it should not expand USD clearing until it had improved its AML/CFT compliance function. • The Branch failed to report to the DFS concerns raised by the Branch chief compliance officer (CCO) about suspicious transactions and improperly curtailed the CCO's independence after the CCO raised these concerns. • The Branch's transaction methods were not sufficiently transparent. • The Branch developed an "unmanageable" backlog of nearly 700 transaction monitoring alerts that needed to be investigated fully.
Mega International Commercial Bank Co. LTD- New York Branch: On August 19, 2016, the New York State Department of Financial Services issued a consent order to Mega international Commercial Bank Co. LTD New York Branch for BSA/AML deficiencies. There was a CMP of US$180 million.	The DFS identified the following: • The branch's AML/CFT policies and procedures were inadequate and inconsistent in transaction monitoring, customer on-boarding and OFAC compliance. Procedures did not incorporate regulatory guidance for reviews of CDD, EDD and diligence concerning PEPs. • The branch's AML/CFT risk assessment and methodology lacked a thorough review of branch customers, products, services and geographic locations served. • Surveillance monitoring filter criteria and thresholds were not periodically reviewed. Branch management was unable to explain the validation process or justification of the selection of the criteria being used. • The branch did not perform adequate reviews of the bank's affiliates' correspondent banking activities at the branch. • DFS identified suspicious transactions transferred between Mega Bank's New York and Panama branches that were not identified and reported. • The compliance and operational functions were comingled as a result of the dual conflicting responsibilities of certain compliance personnel.

Merchants Bank of California: On February 27, 2017, the Office of the Comptroller of the Currency (OCC) identified violations of consent orders the bank entered into on June 23, 2010 and June 26, 2014 by Merchants Bank of California (Merchants). The OCC assessed a US$1 million CMP for the violations. The Financial Crimes Enforcement Network (FinCEN) assessed a CMP of US$7 Million.	Among the violations of the 2010 Consent Order were failures relating to deficiencies in revising and implementing Merchants' BSA compliance program. Specifically the OCC identified: "an inadequate risk assessment process, inadequate system of internal controls, inadequate suspicious activity monitoring and reporting process, and inadequate customer due diligence and enhanced due diligence programs," including: • Failure to conduct CDD for high risk customers; failing to implement appropriate risk management controls for remote deposit capture services (RDCS) • Deficiencies in independent compliance testing dating to 2014; failure to appoint a dedicated AML compliance officer from August 2014 to April 2015 and a lack of sufficient support and authority for AML/CFT compliance leaders • Poorly focused AML/CFT training to Merchants' employees • Failures of CDD for foreign correspondent banking customers • Failures in Suspicious Activity Reporting (SARs) including numerous cases of suspicious activities going unreported
Gibraltar Private Bank and Trust Company (Gibraltar): On February 25, 2016, both the OCC and FinCEN issued enforcement actions against Gibraltar. OCC issued a Cease and Desist Order and CMP in the amount of US$2.5 million.	OCC examiners found that Gibraltar failed to comply with the terms of a 2010 Consent Order by maintaining an "ineffective BSA/AML Compliance Program" that lacked appropriate internal controls relating to reporting SARs. FinCEN found that Gibraltar: • Serviced high-risk customers without effectively monitoring their respective accounts, lacking adequate monitoring techniques, poor KYC and record keeping and an ineffective customer AML/CFT risk rating methodology that prevented/obscured numerous red flags. • Despite the knowledge of its deficiency by management, Gibraltar failed to undertake needed improvements in AML/CFT training compliance. • Failed to perform CDD and KYC requirements. In sum, FinCEN determined that Gibraltar lacked key capabilities to analyse and interpret customer transactions and identify suspicious activity. When suspicious activity was identified it was reported late: "During the period of 2009 to 2013, Gibraltar failed to detect and timely report 120 instances of suspicious activity involving nearly US$558 million in suspicious activity" including hundreds of millions of dollars in transactions relating to a US$1.2 billion Ponzi scheme run by Gibraltar client Scott W. Rothstein. Separately, on March 15, 2016, the former chief compliance officer for Gibraltar, Charles Sanders, was issued a Consent Order and CMP for US$2500. OCC found that "the Bank failed to timely file suspicious activity reports on a set of accounts for a customer who was later convicted of crimes relating to an illegal Ponzi scheme. The Bank's Bank Secrecy Act (BSA) Officer investigated this activity and agreed with the contents of those reports, but he failed to ensure the Bank filed timely suspicious activity reports, causing the Bank to be in violation of laws and regulations, including 12 C.F.R. §163.180."
Stearns Bank, N.A. (Stearns): On April 18 2016 Stearns Bank, N.A. was issued both a consent order with a CMP in the amount of US$1 million as well as a separate cease and desist order for remediation of AML/CFT compliance failures.	OCC found that "beginning in March 2010, the bank became aware of suspicious transactions associated with the manipulation and fabrication of accounts receivables and factoring invoices. The bank failed to adhere to its internal policies and procedures and failed to file timely SARs."

Bethex Federal Credit Union: On December 15, 2016 FinCEN assessed a CMP in the amount of US$500 Thousand against Bethex Federal Credit Union (BFCU) which, as of December 2016, was undergoing liquidation by the National Credit Union Administration (NCUA).	FinCEN identified a number of deficiencies mostly relating to BFCU's provision of banking services to several commercial money services businesses (MSBs). Specific findings included: • BCFU neither appointed a qualified AML compliance officer nor developed an adequate system of internal controls to maintains AML/CFT compliance • Failed to conduct or conducted inadequate risk assessments for domestic and foreign MSBs, including MSBs in several high-risk countries • Failed to perform adequate CDD on MSB clients including failure to collect routine KYC data and failing to implement systematic analysis and develop understanding of client MSBs' business transactions • Failed to put in place sufficient staff to adequately monitor voluminous MSB transactions • Filed SARs late and with poor data and case narratives

For further guidance, please refer to the Enforcement Actions section.

Broker-Dealers

Raymond James & Associates, Inc. (RJA) and Raymond James Financial Services, Inc. (RJFS): On May 8, 2016, Financial Industry Regulatory Authority (FINRA) announced a US$17 Million CMP for AML/CFT compliance violations. Additionally, Linda L Busby, RJA's AML compliance officer from 2002 to the first quarter of 2013, was assessed a fine of US$25 thousand and suspended from association with any FINRA member for three months.	Assessment by FINRA identified several areas of violative conduct including: • Failure to adequately resource and staff AML/CFT compliance operations with as few as 8 dedicated analysts to review transactions across millions of accounts • Failure to establish appropriate written procedures and AML/CFT guidelines or develop a unified AML/CFT compliance process • Deficiency in developing specific AML/CFT strategies tailored to each firm's respective business • A lack of adequate data reporting to identify red flags and a failure to investigate red flags that were identified • A failure to conduct CDD with respect to certain foreign customer correspondent accounts to include accepting improper Foreign Financial Institution Questionnaires (FFIQs) or sometimes not collecting FFIQs at all.
Credit Suisse Securities (USA) LLC: On December 5, 2016, FINRA announced an assessment of a US$16.5 million fine against Credit Suisse Securities (USA) LLC (CSSU) for AML/CFT compliance deficiencies.	FINRA found the following: • CSSU's automated surveillance system was poorly calibrated and often adequate data was not fed to the automated system • Potentially suspicious trading activity was not reported to AML/CFT compliance for further investigation • CSSU lacked adequate procedural guidelines for identifying, monitoring, and reporting suspicious behaviour relating to CSSU's microcap brokerage business leading to "an illegal distribution of at least 55 million unregistered shares of securities" • CSSU failed to conduct required CDD and EDD for foreign correspondent banking customers.
Albert Fried & Company: On June 1, 2016, the U.S. Securities and Exchange Commission (SEC) issued a cease and desist order as well as assessed a CMP of US$300 thousand against Albert Friend and Company (AFC) for failure to file SARs for suspicious activity.	The SEC cited Albert Friend and Company (AFC) for failure to file SARs for suspicious activity with regards to high volume microcap securities trading by some of its clients: “Albert Fried failed to sufficiently evaluate or monitor its customers trading for suspicious activity and its actual practices did not comport with its documented procedures. Albert Fried failed to file SARs as required by Section 17(a) of the Exchange and Rule 17a-8” despite clear red flags.

Brickell Global Markets (Brickell): On February 4, 2016, Brickell Global Markets, formerly E.S. Financial Services was issued a cease and desist order and assessed a CMP in the amount of US$1 million for AML/CFT violations largely relating to deficiencies in CDD and maintaining an effectual Customer Identification Program (CIP) by the SEC.	Brickell failed to properly identify the beneficial owners of various sub-accounts of a Central American Bank for which Brickell maintained a brokerage account. These beneficial account owners "interfaced directly with [Brickell's] registered representatives to solicit securities trading advice and to request account maintenance, securities orders and execution through the Central American Bank account" without Brickell properly identifying and assessing AML/CFT risks posed by these clients. As part of this Consent Order, Brickell agreed to, among other things, hire a third-party auditor to review and assess its CIP/AML/CFT compliance program, undertake any suitable recommendations the auditor might suggest and demonstrate suitable compliance with AML/CFT regulations to the SEC.

For further guidance, please refer to the Enforcement Actions section.

Money Services Businesses

Western Union Financial Services Inc. (WUFSI) Englewood, Colorado: On January 19, 2017, WUFSI agreed to a settlement of US$184 million with FinCEN. This CMP will be fully satisfied by WUFSI's payment to the DOJ for US$586 million	Prior to 2012, WUFSI wilfully violated the AML/CFT requirements by failing to implement an effective risk based AML/CFT compliance program and file SARs accordingly. The U.S. Department of Justice (DOJ) will collect US$586 million from WUFSI. The DOJ has stated that the funds collected through civil asset forfeiture will be used for restitution of victims of fraud. FinCEN's US$184 million settlement will be satisfied with WUFSI payment to the DOJ.
MoneyGram International Inc. (MoneyGram): In December 2012, MoneyGram entered into a Deferred Prosecution Agreement (DPA) with the DOJ with a forfeiture of US$100 million for aiding and abetting wire fraud and failing to maintain an effective AML Program.	Despite thousands of customer complaints and red flags raised by concerned personnel with regard to mass marketing and phishing schemes by foreign agents, MoneyGram's sales executives allegedly refused to terminate agents suspected of involvement in these fraudulent scams. Often targeting the elderly, scams ranged from individuals posing as relatives in need, false promises of prize money, false offers for deeply discounted items and false employment offers. Each scam required victims to send funds through MoneyGram. Reports of fraud by customers grew from nearly 1,600 instances in 2004 to almost 20,000 in 2008, totalling to at least US$100 million. MoneyGram agreed to retain an independent corporate monitor to oversee implementation of its corrective action plan to address deficiencies in its AML Program including, but not limited to, the lack of an enterprisewide AML Program, lack of alignment of senior management incentives with compliance obligations, inadequate compliance resources, and inadequate due diligence program and termination policy for high-risk agents. Initially, former MoneyGram compliance officer, Thomas E. Haider, faced a personal fine of up to US$5 million for "wilful inaction" in his AML/CFT compliance responsibilities, but ultimately settled for a fine of US$250,000 and a three-year injunction, barring him from any compliance employment with any money transmitter in May 2017. To date, the "Haider Settlement" is the largest public civil AML enforcement action against an individual.

For further guidance, please refer to the Enforcement Actions section.

OFAC Settlements

Zhongxing Telecommunications Equipment Corporation (ZTE): On March 7, 2017, ZTE agreed to a settlement of US$100,871,266 for 251 apparent violations of the Iranian Transactions and Sanctions Regulations (ITSR) administered by the Office of Foreign Assets Control (OFAC)	According to the settlement findings, from approximately January 2010 to March 2016, ZTE's management implemented a company-wide plan that utilised third-party companies to conceal and facilitate ZTE's illegal business with Iran. ZTE engaged in the following: • The exportation, sale, or supply, directly or indirectly, from the United States of goods to Iran or the Government of Iran • The re-exportation of controlled U.S.-origin goods subject to the Export Administration Regulations (EAR) from a third-country with knowledge that the goods were intended specifically for Iran or the Government of Iran; and • Activity that evaded or avoided, attempted and/or conspired to violate and/or caused violations of the prohibitions set forth in the ITSR.
United Medical Instruments Inc. (UMI): On February 28, 2017, UMI agreed to a settlement of US$515,400 for 56 alleged violations of the ITSR	According to the settlement findings, from approximately December 5, 2007 to April 30, 2009, UMI made sales of medical imaging equipment with knowledge or reason to know that the goods were intended specifically for supply or re-exportation to buyers located in Iran, and when it facilitated the sales of medical imaging equipment from a company located in the United Arab Emirates to Iran.
Toronto-Dominion Bank (TD Bank): On January 13, 2017, TD Bank agreed to a settlement for US$516,105 for 167 apparent violations	According to the settlement findings: • TD Bank failed to screen import-export letters of credit for TD Bank's Canadian customers prior to processing related transactions through the U.S. financial system. • TD Bank maintained several accounts for, and processed transactions to or through the United States on behalf of, a Canadian company owned by a Cuban company. • According to documentation available to TD Bank, a customer was listed as a sales agent for an entity on OFAC's List of Specially Designated Nationals and Blocked Persons (SDN) List and located in Iran. Between December 1, 2008 and March 28, 2012, TD Bank processed 39 transactions totalling US$515,071.20 to or through the United States on behalf of this customer in apparent violation of ITSR. • Separately, TD Bank maintained accounts on behalf of 62 customers who were Cuban nationals residing in Canada
American International Group, Inc. (AIG): On June 26, 2017, AIG agreed to a settlement of US$148,698 for 555 apparent violations of OFAC Sanctions	According to the settlement findings, from approximately November 20, 2007 to September 3, 2012, AIG engaged in a total of 555 transactions totalling approximately US$396,530 in premiums and claims for the insurance of maritime shipments of various goods and materials destined for, or that transited through, Iran, Sudan, or Cuba and/or that involved a blocked person.

For further guidance, please refer to the Enforcement Actions and Office of Foreign Assets Controls and International Sanctions Programs sections.

Key U.S. Terrorism Cases

"**Unabomber**." The Unabomber cases stretched from 1976 to 1995 and occurred in various cities in the United States. The information included here is from the indictment issued by the U.S. District Court for the Eastern District of California and does not cover all of Kaczynski's bombings.	• **Number of deaths/injuries:** Three deaths/over 20 injured
	• **Method of Attacks**: Mailed and hand-delivered 16 homemade bombs
	• **Alleged Causes**: According to Kaczynski's published manifesto, his causes included, but were not limited to, the following:
	  ○ Anti-modern technology and industrial society
	  ○ Anarchist
	  ○ Anti-leftist
	• **Suspect:** Theodore Kaczynski (United States), code-named "Unabomber" by the FBI for his targets on universities and airlines
	• **Method of Capture**: Tip from Kaczynski's brother after publishing of "Unabomber's" 35,000-word manifesto in the Washington Post and The New York Times in 1995.
	• **Charges included, but were not limited to, the following:**
	  ○ Transporting an Explosive in Interstate Commerce with Intent to Kill
	  ○ Mailing an Explosive Device with Intent to Kill or Injure
	  ○ Using a Destructive Device During and in Relation to a Crime of Violence
	  ○ Kaczynski also was investigated in 2011 for possible involvement in the 1982 Tylenol poisonings (capsules laced with potassium cyanide) that killed seven people in the Chicago-area
	• **Sentence**: Life imprisonment

World Trade Center (WTC) Bombing, (New York, New York, February 1993). The information included here comes from the indictment issued by the United States District Court for the Southern District of New York for the WTC Bombing.	• **Deaths/Injuries**: Six deaths/over 1,000 injured
	• **Methods of Attack:** Van with a 1,000+ lb. homemade bomb abandoned in lower-level parking garage under World Trade Center
	• **Alleged Causes/Affiliation**:
	  ○ Avenge the sufferings of the Palestinian people
	  ○ Protest U.S. support of Israel
	  ○ Protest U.S. military intervention in the Middle East
	• **Suspects:**
	  ○ Ramzi Yousef (Pakistan) (accused "mastermind," nephew to Khalid Sheikh Mohammed (Pakistan), accused "mastermind" of 9/11 attacks)
	  ○ Eyad Ismoil (Jordan)
	  ○ Mohammad Salameh (Palestine)
	  ○ Abdul Yasin (Iraq)
	  ○ Mahmoud Abouhalima (Egypt)
	  ○ Ahmed Ajaj (Palestine)
	  ○ Nidal Ayyad (Palestine)
	  ○ Seven suspects allegedly linked through sheik Omar Abdel Rahman (Egypt), also known as "the blind sheikh," who was later convicted for seditious conspiracy for various planned attacks against U.S. interests and died in prison in 2017
	• **Method of Capture:** Vehicle identification number (VIN) from bombing wreckage lead to renter, Mohammad Salameh; subsequent worldwide FBI investigation lead to capture of additional five suspects; seventh suspect, Abdul Yasin, remains at large.
	• **Charges included, but were not limited to, the following:**
	  ○ Conspiracy to Commit Offense or to Defraud United States
	  ○ Use of Arson or Explosives When a Labor Dispute is Involved
	  ○ Maliciously damages or destroys, or attempts to damage or destroy, by means of fire or an explosive, any building, vehicle, or other personal or real property in whole or in part owned or possessed by, or leased to, the United States

	○ Transports or receives, or attempts to transport or receive, in interstate or foreign commerce any explosive with the knowledge or intent that it will be used to kill, injure, or intimidate any individual or unlawfully to damage or destroy any building, vehicle, or other real or personal property ○ Destruction of Motor Vehicles or Motor Vehicle Facilities ○ Penalty When Death Results ○ Interstate and Foreign Travel or Transportation in Aid of Racketeering Enterprises • **Sentence**: Life imprisonment
Oklahoma City (OKC) Bombing (Oklahoma City, Oklahoma, April 1995). The information included here was sourced from the indictment issued by the United States District Court for the Western District of Oklahoma against Timothy McVeigh and Terry Nichols and the plea agreement for Michael Fortier.	• **Number of deaths/injuries:** 168 deaths/nearly 700 injured • **Method of Attack**: Truck with a homemade bomb parked in front of a federal building in downtown Oklahoma City • **Alleged Cause**: Anti-government individuals retaliating for FBI's handling of the 51-day standoff with the Branch Davidians also known as the Waco Siege (1993). • **Suspects**: Timothy McVeigh, Terry Nichols and Michael Fortier (all United States) • **Methods of Capture**: The VIN of a truck was recovered from the wreckage and traced to a body shop that lead to the identification of the renter, Timothy McVeigh. Within 90 minutes of the bombing, McVeigh was already in jail, arrested on an unrelated charge after being pulled over by a state trooper for a missing license plate. Subsequent FBI investigation lead to Terry Nichols and Michael Fortier, who knew about the bomb plot and received a reduced charge for his testimony against McVeigh and Nichols. Charges included, but were not limited to, the following: • **McVeigh/Nichols:** ○ First Degree Murder ○ Conspiracy to Use a Weapon of Mass Destruction ○ Use of Weapon of Mass Destruction ○ Destruction by Explosive ○ Maliciously Damages or Destroys, or Attempts to Damage or Destroy, by Means of Fire or an Explosive, Any Building, Vehicle, or Other Personal or Real Property in Whole or in Part Owned or Possessed by, or Leased to, the United States • **Fortier:** ○ Conspiracy to Commit Offense or to Defraud the United States ○ Transport or Ship in Interstate or Foreign Commerce, Any Stolen Firearm or Stolen Ammunition, Knowing or Having Reasonable Cause to Believe that the Firearm or Ammunition Was Stolen ○ Materially False, Fictitious, or Fraudulent Statement or Representation ○ Misprision of Felony (i.e., concealing and not making known to a person in civil authority his/her knowledge of the commission of a felony cognisable by a court of the United States) • **Sentences:** ○ McVeigh: death sentence, executed in 2001 ○ Nichols: life imprisonment ○ Fortier: 12-year prison sentence

Centennial Olympic Park Bombing (Atlanta, Georgia, July 1996). The information included here was sourced from the indictment issued by the United States District Court for the Northern District of Georgia, Atlanta Division, against Eric Robert Rudolph	• **Deaths/Injuries**: One death/over 100 injured
	• **Method of Attacks**:
	  ○ Centennial Olympic Park Bombing: Pipe bombs in a backpack left unattended in Centennial Olympic Park in Atlanta, Georgia; backpack was discovered by a security guard; due to evacuation, casualties were minimised
	  ○ Atlanta Clinic: Two bombings of an abortion clinic in Sandy Spring, Georgia
	  ○ Otherside Lounge: Two bombings of a lesbian nightclub in Atlanta, Georgia
	• **Alleged Cause**: Anti-abortion
	• **Suspect:** Eric Robert Rudolph (United States)
	• **Method of Capture:** After the bombings at the Atlanta Clinic and the Otherside Lounge, an FBI investigation lead to naming Rudolph as a prime suspect in 1998. In 2003, Rudolph was apprehended by a police officer on routine patrol.
	• **Charges included, but were not limited to, the following:**
	  ○ Bombing at Centennial Olympic Park
	  ○ First Bombing at the Atlanta Clinic
	  ○ Second Bombing at the Atlanta Clinic
	  ○ First Bombing at the Otherside Lounge
	  ○ Second Bombing at the Otherside Lounge
	  ○ Carrying and Use of Destructive Device
	  ○ Transportation of Explosive Used in Olympic Park Bombing
	  ○ Transportation of Explosives Used in Atlanta Clinic Bombings
	  ○ Transportation of Explosives Used in Otherside Lounge Bombings
	  ○ 911 Bomb Threat Call
	  ○ Atlanta “Army of God” Letters (threatening letters claiming responsibility for bombings)
	  ○ Birmingham “Army of God” Letters (threatening letters claiming responsibility for bombings)
	• **Sentence:** Life imprisonment

Amerithrax or Anthrax Attacks (Multiple cities, United States, September – October, 2001). The included information is from the FBI’s Amerithrax Investigative Summary (2010).	• **Deaths/Injuries**: Five deaths/17 sickened/31 tested positive for exposure/10,000 deemed “at risk” for exposure underwent antibiotic prophylaxis
	• **Method of Attack:** Letters laced with Bacillus anthracis spore powder (anthrax) mailed to several high-profile individuals including two members of the U.S. Congress, Tom Daschle and Patrick Leahy, and three media organisations, NBC (addressed to Tom Brokaw) and the New York Post in New York and the National Enquirer/American Media Inc. (AMI) in Florida.
	• **Suspects:**
	  ○ Bruce E. Ivins (United States) (microbiologist and biodefense researcher for the United States Army Medical Research Institute of Infectious Diseases [USAMRID] who initially assisted in the investigation, committed suicide in July 2008)
	  ○ Dr. Steven Hatfill (United States) (physician, former biodefense researcher for USAMRID; exonerated in 2008)
	• **Alleged Cause:** To garner support to continue Ivins’ lifelong work to develop an anthrax vaccine**.**
	• **Method of capture:** None: Ivins committed suicide. In February 2010 the FBI and the United States Postal Inspection Service (USPIS) concluded Ivins acted alone and closed the Amerithrax investigation.
	• **Charges:** None: In the summer of 2008 the charge was going to be Use of Weapon of Mass Destruction but Ivins committed suicide before the indictment was issued; the FBI and USPIS concluded Ivins acted alone and closed the Amerithrax investigation.
	• **Sentence**: None, see above.

September 11 (9/11) Attacks (New York, New York; Arlington County, Virginia; Shanksville, Pennsylvania, September 11, 2001). This information is from the indictments issued by the United States District Court Southern District of New York and Eastern District for Virginia for the 9/11 attacks.	• **Deaths/Injuries:** Nearly 3,000 deaths/unknown number of injuries (direct and subsequent)
	• **Method of Attacks:** Four hijacked airplanes (American Airlines Flight 11, American Airlines Flight 77, United Airlines Flight 93 and United Airlines Flight 175) aimed at three different targets including the World Trade Center, the Pentagon and Washington, D.C.
	• **Alleged Causes/Affiliations:**
	  ○ Al Qaeda
	  ○ United States viewed as an "infidel" because it was not governed in a manner consistent with Islamic interpretations
	  ○ United States provided support to other infidel governments and institutions (e.g., Saudi Arabia, Egypt, Israel, United Nations)
	  ○ Retaliation for United States military intervention in the Middle East (e.g., Gulf War) and Somalia in the early 1990s
	• **Suspects:**
	  ○ Facilitators/Financiers/Defendants:
	  ▪ Khalid Sheikh Mohammed (Pakistan) (alleged "mastermind" behind 9/11 attack) (also known as Mukhtar, Mukhtar al-Baluchi, Al-Mukh, Abdulrahman Abdullah al-Ghamdi, Salem Ali)
	  ▪ Walid Bin Attash (Yemen) (also known as Khallad Bin Attash, Saleh Saeed Mohammed Bin Yousaf, Tawfiq Muhammad Salih Bin Rashid, Silver)
	  ▪ Ramzi Bin al-Shibh (Yemen) (also known as Abu Ubaydah, Ahad Abdollahi Sabet)
	  ▪ Ali Abdul Aziz Ali (Pakistan) (also known as Aliosh, Ali A, Isam Mansur, Ammar al-Baluchi, Hani)
	  ▪ Mustafa al-Hawsawi (Saudi Arabia) (also known as Hashem Abdulrahman, Hashem Abdollahi, Mustafa Ahmed, Zaher, Khal)
	  ▪ Zacarias Moussaoui (France) (also known as Shaqil, Abu Khalid al Sahrawi)
	  ○ Actors:
	  ▪ Mohammed Atta (Egypt) (pilot of United Airlines Flight 175 that struck North Tower of World Trade Center)
	  ▪ Marwan al Shehhi (United Arab Emirates [UAE]) (pilot of American Airlines Flight 77 that struck South Tower of World Trade Center)
	  ▪ Hani Hanjour (Saudi Arabia) (pilot of American Airlines Flight 77 that struck the Pentagon)
	  ▪ Ziad Jarrah (Lebanon) (pilot of United Airlines Flight 93 that crashed in Shanksville)
	  ▪ Abdul Aziz al Omari (Saudi Arabia)
	  ▪ Wail al Shehri (Saudi Arabia)
	  ▪ Waleed al Shehri (Saudi Arabia)
	  ▪ Satam al Suqami (Saudi Arabia)
	  ▪ Fayez Banihammad (United Arab Emirates [UAE])
	  ▪ Ahmed al Ghamdi (Saudi Arabia)
	  ▪ Hamza al Ghamdi (Saudi Arabia)
	  ▪ Mohand al Shehri (Saudi Arabia)
	  ▪ Nawaf al Hazmi (Saudi Arabia)
	  ▪ Salem al Hazmi (Saudi Arabia)
	  ▪ Khalid al Mihdhar (Saudi Arabia)
	  ▪ Majed Moqed (Saudi Arabia)
	  ▪ Saeed al Ghamdi (Saudi Arabia)
	  ▪ Ahmad al Haznawi (Saudi Arabia)
	  ▪ Ahmed al Nami (Saudi Arabia)

	• **Method of Capture:** All actors were killed in the attacks. Additional suspects were identified through multiple investigations conducted by the FBI and others.
	• **Charge(s) included, but were not limited to, the following**:
	  ○ Conspiracy to Commit Acts of Terrorism Transcending National Boundaries
	  ○ Acts of Terrorism Transcending National Boundaries
	  ○ Conspiracy to Commit Violent Acts and Destroy Aircraft
	  ○ Violence on and Destruction of Aircraft
	  ○ Conspiracy to Commit Aircraft Piracy
	  ○ Conspiracy to Destroy Aircraft
	  ○ Aircraft Piracy
	  ○ Conspiracy to Use Weapons of Mass Destruction
	  ○ Murder of United States Officers and Employees
	  ○ Destruction of the Twin Towers
	  ○ Al Qaeda Conspiracy to Kill Americans
	  ○ Conspiracy to Destroy Property
	• **Sentence**: All actors were killed in the attacks. Some suspected facilitators and financiers were detained and at least one (Khalid Sheikh Mohammed) was tried in a military commission that began in 2008.

Shoe Bomber (Miami, Florida, December 2001). This information is from the indictment issued by the United States District Court District of Massachusetts against shoe bomber, Richard Colvin Reid.	• **Deaths/Injuries:** None (failed attack attempted two months after 9/11 attacks)
	• **Method of Attack:** Bombs hidden in shoes of passenger on American Airlines Flight 63 from Miami to Paris
	• **Alleged Cause/Affiliation:** Al-Qaeda
	• **Suspect**: Richard Colvin Reid (United Kingdom) (also known as Abdul Raheen, Abu Ibrahim)
	• **Method of Capture:** Other passengers on plane subdued Reid as he was attempting to ignite a fuse on his shoe; landed in East Boston, Massachusetts
	• **Charge(s) included, but were not limited to, the following**:
	  ○ Attempted Homicide
	  ○ Attempted Murder
	  ○ Attempted Use of a Weapon of Mass Destruction
	  ○ Placing Explosive Device on an Aircraft
	  ○ Attempted Destruction of an Aircraft
	  ○ Interference with Flight Crew Members and Attendants
	  ○ Using Destructive Device During and in Relation to a Crime of Violence
	  ○ Attempted Wrecking of Mass Transportation Vehicle
	• **Sentence**: Life imprisonment

Beltway Sniper Attacks (multiple cities, United States, October 2002). This information is from the indictment issued by the Circuit Court of Fairfax County against Lee Boyd Malvo and the criminal complaint issued by the U.S. District Court for the District of Maryland against John Allen Muhammad.	• **Deaths/Injuries:** 10 deaths/3 injuries
	• **Method of Attacks:** Bushmaster XM-15 semiautomatic rifle used to shoot victims in multiple cities around the Washington, D.C. area (e.g., Baltimore, Rockville, Wheaton, Kensington, Maryland)
	• **Alleged Cause/Affiliation:** According to various reports, possible affinity for the “Islamic jihad”
	• **Suspects**:
	  ○ John Allen Muhammad (United States) (also known as John Allen Williams, Wayne Weeks, Wayne Weekley)
	  ○ Lee Boyd Malvo (Jamaica) (also known as John Lee Malvo)
	• **Method of Capture:** After anonymous calls were made to law enforcement with information about another shooting in Montgomery, Alabama, the FBI conducted ballistics testing and were lead to Muhammad and Malvo as suspects; after releasing descriptions of the suspects and their car, calls from concerned citizens lead the FBI to Muhammad and Malvo at a rest station in Myersville, Maryland.

	• **Charges included, but were not limited to, the following:**
	  ○ Capital Murder
	  ○ Use of a Firearm During the Commission of a Crime of Violence, Causing Death of a Person
	  ○ Conspiracy to Commit Offenses Against the United States
	  ○ Conspiracy to Affect Interstate Commerce by Extortion and Threats of Physical Violence
	  ○ Interstate Transportation in Aid of Racketeering
	  ○ Discharging a Firearm in a School Zone
	• **Sentences:**
	  ○ Muhammad: Death sentence; executed in 2009
	  ○ Malvo: Life sentence

Boston Marathon Bombing (Boston, Massachusetts, April 2013). This information is from a criminal complaint issued by the United States District Court for the District of Massachusetts against Dzhokhar Tsarnaev.	• **Deaths/Injuries:** 3 deaths/over 200 injuries
	• **Method of Attack:** Two knapsacks with bombs detonated near the finish line of the Boston Marathon
	• **Alleged Cause/Affiliation:** According to several reports, the brothers were not affiliated with a terrorist organisation but were religiously motivated in their protest of U.S. wars in Afghanistan and Iraq.
	• **Suspects**:
	  ○ Dzhokhar Tsarnaev (Kyrgyzstan) (also known as Jahar Tsarnaev)
	  ○ Tamerlan Tsarnaev (Kyrgyzstan)
	• **Methods of Capture**:
	  ○ Within a few days of the bombing, Tamerlan Tsarnaev was shot and killed by police.
	  ○ Dzohokhar Tsarnaev was apprehended the following day by police with multiple injuries to his head, neck, legs and hand.
	• **Charges included, but were not limited to, the following**:
	  ○ Use of a Weapon of Mass Destruction
	  ○ Malicious Destruction of Property Resulting in Death
	• **Sentence:** Death penalty

Ricin letters (Multiple cities, United States, April 2013). The information included here is from the affidavit issued by the United States District for the Northern District of Mississippi against James Everett Dutschke.	• **Deaths/Injuries:** 0 deaths/0 injuries
	• **Method of Attack:** Three letters laced with ricin mailed to two politicians, Barack Obama and Roger Wicker, and judge, Sadie Holland
	• **Alleged Cause:** Personal vendettas against perceived rivals
	• **Suspects**:
	  ○ James Everett Dutschke (United States)
	  ○ Paul Kevin Curtis (United States) (exonerated in April 2013)
	• **Method of Capture:** Curtis tipped FBI to Dutschke as a possible suspect; FBI investigation confirmed Dutschke involvement leading to his subsequent arrest.
	• **Charges included, but were not limited to, the following**: Prohibitions with Respect to Biological Weapons
	• **Sentence**: According to various news outlets, Dutschke was sentenced to 25 years in prison in 2014.

Emanuel African Methodist Episcopal (AME) Church Shooting (Charleston, South Carolina, June 2015). The information provided here is from the indictment issued by the United States District Court for the District of South Carolina, Charleston Division, against Dylann Roof.	• **Deaths/Injuries:** Nine deaths/1 injury
	• **Method of Attack:** Shooting with a Glock, model 41, .45 calibre pistol
	• **Alleged Cause:** To initiate a race war with African Americans
	• **Suspect**: Dylann Roof (United States)
	• **Method of Capture:** Following a tip from a concerned citizen, police apprehended Roof in Shelby, North Carolina, approximately 250 miles from Charleston.
	• **Charges included, but were not limited to, the following**:
	  ○ Hate Crime Act Resulting in Death
	  ○ Hate Crime Act Involving an Attempt to Kill
	  ○ Obstruction of Exercise of Religion Resulting in Death
	  ○ Obstruction of Exercise of Religion Involving an Attempt to Kill and Use of a Dangerous Weapon
	  ○ Use of a Firearm to Commit Murder During and in Relation to a Crime of Violence
	• **Sentence**: Life imprisonment

San Bernardino Mass Shooting (San Bernardino, California, December 2015). The information provided here is from a memorandum issued by the Office of Inspector General of the Department of Homeland Security on the "San Bernardino Incident."	• **Deaths/Injuries:** 14 deaths/22 injuries
	• **Method of Attack:** Shooting with .223 assault rifles
	• **Alleged Cause:** Potential inspiration by foreign terrorist organisations
	• **Suspects**:
	  ○ Syed Rizwan Farook (United States)
	  ○ Tashfeen Malik (Pakistan/Saudi Arabia)
	• **Method of Capture:** Farook and Malik were pursued by police after the attack and killed in a shootout.
	• **Charges**: None; Farook & Malik were killed by police shortly after the shooting.
	• **Sentence**: None, see above.

Pulse Nightclub Shooting (Orlando, Florida, June 2016). The information provided here is according to the FBI's investigative update regarding Pulse Nightclub Shooting.	• **Deaths/Injuries:** 49 deaths/53 injuries • **Method of Attack:** Shooting with Sig Sauer MCX rifle and a 9mm handgun • **Alleged Cause:** In calls with Orlando Police Department (OPD) Crisis Negotiation Team, Mateen identified himself as an Islamic soldier and called for the end of bombing in Syria and Iraq; according to 911 transcripts, Mateen pledged allegiance to "Abu Bakr al-Baghdadi of the Islamic State." • **Suspect:** Omar Mateen (United States) • **Method of Capture:** Killed by police at Pulse Nightclub • **Charges**: None; Mateen was killed by police shortly after the shooting. • **Sentence:** None**,** see above.

Key Terms and Concepts

The 13599 List	The list of Persons Identified as Blocked Solely Pursuant to Executive Order 13599 includes persons that meet the definition of "Government of Iran" or "Iranian financial institution" as set forth in Part 560 of the Iranian Transactions and Sanctions regulations that are not blocked but are subject to other restrictions limiting transactions/trade. For further guidance on Iranian sanctions, please refer to the Country- and Regime-Based Sanctions Programs section.
Account	"Account" is defined differently for various types of institutions (e.g., bank, broker-dealer and casino). For example, for depository institutions, an "account" is a formal relationship in or through which financial transactions or services are provided. Examples of products and services where a formal relationship would normally exist include deposit accounts, extensions of credit, a safe deposit box or other safekeeping services, and cash management, custodian or trust services. For other definitions of "account," please see the Broker-Dealers in Securities and Casinos and Card Clubs sections.
Alert	Within the context of a transaction monitoring program, an "alert" is an indicator of unusual or potentially suspicious activity based on such factors as expected activity thresholds, account history, customer types, product types and geography in an automated monitoring system. An "alert" may be generated from a transaction monitoring system or via internal referrals, subpoenas, and 314(a) and 314(b) matches. Regardless of its source, an alert is not necessarily an automatic indicator of suspicious activity. For further guidance, please refer to the sections: Transaction Monitoring, Investigations and Red Flags and Investigating Potential Matches.
Alternative value transfer systems	Alternative value transfer systems refer to nontraditional value transfer systems outside of the conventional financial services system (e.g., banking), which can include, but are not limited to, the following: • Informal value transfer systems (IVTSs) • Black Market Peso Exchange (BMPE) • Reintegro • Virtual Currency Systems • Crowdfunding For additional guidance, please refer to the Alternative Value Transfer Systems section.
AML compliance officer	The AML compliance officer generally is responsible for developing and maintaining the AML Program, including policies and procedures; ensuring the timely and accurate filing of required reports; coordinating AML training (within the compliance department and with relevant employees); and acting as the liaison for AML/CFT-related matters with regulators. In addition, many AML compliance officers oversee the transaction monitoring function. Beyond these general points, the role of the AML compliance officer will vary by institution depending on its size and the availability of resources. In some instances, the AML compliance officer is responsible for OFAC compliance; in larger institutions, an OFAC compliance officer is responsible for OFAC compliance. Accordingly, the role of the AML compliance officer should be documented clearly in a job description. For additional guidance, please refer to the Section 352 Compliance Program section.

AML Program	At a minimum, Section 352 of the USA PATRIOT Act requires financial institutions to establish AML Programs, which previously included the following "four pillars": • Development of written internal policies, procedures and controls • Designation of an AML compliance officer • Ongoing AML employee-training program • Independent testing of the AML Program Since FinCEN issued the "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) in July 2016, a fifth pillar has been added to the AML Program: • Ongoing risk-based monitoring of customer activity and information with updates as necessary To distinguish the AML Program with "five pillars," this publication will use "AML/CFT Compliance Program" when referencing an expanded program that includes additional components (e.g., board of director and senior management support and oversight, risk assessments, customer identification program [CIP]). For further guidance, please refer to the AML/CFT Compliance Program and Section 352 – AML Program sections.
Anti-Bribery and Corruption (ABC) Compliance Program	An effective ABC Compliance Program includes the following 10 components: • Commitment from senior management and a clearly articulated statement of anti-corruption culture and policy to prevent bribery; • Code of conduct and compliance policies and procedures, specific to payments (e.g., gifts, hospitality, facilitation payments); • Oversight, accountability, autonomy and resources; • Risk assessment; • Training and continuing advice; • Incentives to prevent bribery and disciplinary measures for noncompliance and violations of the law; • Third-party anti-corruption due diligence program (e.g., risk scoring, questionnaires, written agreements, certifications, training); • Confidential reporting (e.g., whistleblower) and internal investigations of suspected instances of bribery and corruption; • Continuous improvement: periodic testing and review of the anti-bribery program; and • Mergers and acquisitions: pre-acquisition due diligence and post-acquisition integration. For further guidance, please refer to the Drug Trafficking section.
Armored car service (ACS)	Armored car services (ACS), a subset of common carriers of currency also referred to as "cash in transit" (CIT) operators, are "secured transporters of valuable goods, including currency for various third parties including, but not limited to, financial institutions, the Federal Reserve, the U.S. Mint and private companies. Goods may be transported via cars, airplanes and couriers." ACSs may also act as servicing agents for financial institutions (e.g., count and sort currency and coins). For additional guidance, please refer to the Common Carriers of Currency and Armored Car Services section.
Artificial intelligence (AI)	Artificial intelligence (AI) is a branch of software engineering that focuses on automatically making decisions for the problem at hand based on the decisions made in the past for the same problem. For further guidance, please refer to the Future of AML/CFT Technology section.

Automated Clearing House (ACH) Transactions	Automated Clearing House (ACH) transactions are commonly utilised for direct deposits of payroll, government benefits and tax refunds and payments of consumer bills (e.g., mortgages, utility bills, insurance premiums). The most significant growth in the use of ACH transactions has occurred with nonrecurring payments including, but not limited to, the following: • Accounts receivable conversion (ARC) • Point-of-purchase (POP) • Internet-initiated (WEB) • Telephone-initiated (TEL) • Re-presented check (RCK) entries For additional guidance, please refer to the Automated Clearing House Transactions section.
Automated teller machine (ATM)	An automated teller machine (ATM) is an electronic banking device that can be used by customers without the aid of a representative (e.g., teller) for the following types of services: • Accessing account information (e.g., balance inquiry, account statements) • Withdrawing and/or depositing funds (e.g., cash, monetary instruments) • Transferring funds between linked accounts • Bill payment For additional guidance, please refer to the Owners/Operators of Privately Owned Automated Teller Machines section.
Bank Secrecy Act (BSA)	The key U.S. AML/CFT law is the Bank Secrecy Act (BSA) (also known as the Financial Recordkeeping of Currency and Foreign Transactions Act of 1970), which was significantly amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act). The BSA was the first major money laundering legislation in the United States. It was designed to deter the use of secret foreign bank accounts and provide an audit trail for law enforcement by establishing regulatory reporting and recordkeeping requirements to help identify the source, volume and movement of currency and monetary instruments into or out of the United States or deposited in financial institutions. For additional guidance, please refer to the Bank Secrecy Act section.
Bearer negotiable instruments (BNI)	BNIs are defined by FATF as “monetary instruments in bearer form such as: traveller’s checks; negotiable instruments (including checks, promissory notes and money orders) that are either in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; incomplete instruments (including checks, promissory notes and money orders) signed, but with the payee’s name omitted.” For further guidance, please refer to the Financial Action Task Force section.
Bearer share	“Bearer shares” are negotiable instruments that accord ownership in a corporation to the person who possesses the bearer share certificate. For further guidance, please refer to the Beneficial Owners section.
Beneficial owner	As defined by FinCEN’s notice of proposed rulemaking (NPRM) on “Customer Due Diligence Requirements for Financial Institutions,” a “beneficial owner” is a natural person, not another legal entity, who meets the following criteria: Ownership prong – Is one of up to four, who owns, directly or indirectly, 25 percent or more of the equity interest in a legal entity customer; and Control prong – Exercises significant managerial control (e.g., a C-suite executive) over the legal entity. For further guidance, please refer to the Beneficial Owners section.

Beneficial Ownership Rule	FinCEN issued the final rule "Customer Due Diligence Requirements for Financial Institutions" (Beneficial Ownership Rule) in 2016, which requires financial institutions currently subject to Customer Identification Program (CIP) requirements to identify and verify the identity of beneficial owners with 25 percent or greater ownership or significant control of legal entity customers. However, the Beneficial Ownership Rule does not change Section 312 requirements. The Beneficial Ownership Rule uses a two-prong concept – ownership and effective control – by defining a "beneficial owner" as a natural person, not another legal entity, who meets the following criteria: • **Ownership prong** – Each individual, up to four, who owns, directly or indirectly, 25 percent or more of the equity interest in a legal entity customer; and • **Control prong** – At least one individual who exercises significant responsibility to control, manage or direct (e.g., a C-suite executive, managing member, general partner, president, treasurer) the legal entity. In cases where an individual is both a 25 percent owner and meets the control definition, that same individual can be defined as a beneficial owner under both prongs. From an industry perspective, the second prong improves upon the definition in the advanced notice of proposed rulemaking (ANPR) issued in 2012. The earlier definition would have required the identification of the individual who had "greater responsibility than any other individual." For further guidance, please refer to the Beneficial Owners section.
Bitcoin	Bitcoin is a form of cryptocurrency, which is defined by FATF as "… launched in 2009, was the first decentralised convertible virtual currency, and the first cryptocurrency. Bitcoins are units of account composed of unique strings of numbers and letters that constitute units of the currency and have value only because individual users are willing to pay for them. Bitcoins are digitally traded between users with a high degree of anonymity and can be exchanged (purchased or cashed out) into US dollars, Euros, and other fiat or virtual currencies. Anyone can download the free, open-source software from a website to send, receive, and store bitcoins and monitor Bitcoin transactions. Users can also obtain Bitcoin addresses, which function like accounts, at a Bitcoin exchanger or online wallet service. Transactions (fund flows) are publicly available in a shared transaction register and identified by the Bitcoin address, a string of letters and numbers that is not systematically linked to an individual. Therefore, Bitcoin is said to be 'pseudoanonymous.' …" For further guidance, please refer to the Virtual Currency Systems and Participants section.
Black Market Peso Exchange (BMPE)	The "Black Market Peso Exchange (BMPE)" is an intricate trade-based money laundering (TBML) system in which transnational criminal organisations (TCOs) (e.g. Colombian drug cartels) sell drug-related U.S.-based currency to money brokers (e.g. peso brokers) in a foreign country (e.g., Colombia) who, in turn, "exchange" the illicit U.S. currency for a foreign currency (e.g., Colombian pesos) through a series of transactions involving multiple financial institutions that support legitimate international trade between foreign importers and U.S. exporters. For further guidance, please refer to the sections: Black Market Peso Exchange and Informal Value Transfer System.
Blockchain	A blockchain is a distributed database (information distributed over a network of computers rather than located on a single or multiple servers) that maintains a continuously growing list of ordered records called blocks. Bitcoin and similar cryptocurrencies first used blockchain technology, but there are many applications of this technology that can be used to support AML/CFT compliance. By design, blockchains are intended to be immutable once information is recorded. Blockchain could play a significant role in streamlining the KYC process if used as KYC repositories where information could be used by eligible, participating financial institutions, thereby eliminating the need for customer outreach. The KYC data is unique, and it is impossible to create two conflicting entries into this system. For additional guidance, please refer to the Future of AML/CFT Technology section.

Bribery	Bribery is the offering or giving of "something of value" in order to induce the recipient to abuse his or her position in some way for the benefit of the bribe payer or the person or entity on whose behalf the bribe is being offered or paid. Bribes can come in as anything of value (e.g., cash payments, gifts, jobs or internships). For further guidance, please refer to the Anti-Bribery and Corruption Compliance Programs section.
Broker-dealer in securities	A broker-dealer is a person or company that is in the business of buying and selling securities – stocks, bonds, mutual funds, and certain other investment products – on behalf of its customers (as broker), for its own account (as dealer), or both. Individuals who work for broker-dealers – the sales personnel whom most people call brokers – are technically known as registered representatives. For additional guidance, please refer to the Broker-Dealers in the Securities section.
BSA Reports	Depending on the type of financial institution involved, the following are reports mandated by the BSA: • Currency Transaction Report (CTR) – For further guidance, please refer to the Currency Transaction Reports section. • Designation of Exempt Person (DOEP) – For further guidance, please refer to the CTR Exemptions and the Designation of Exempt Person Form and Filing of DOEP sections. • Report of Cash Payments Over US$10,000 Received in Trade/Business, FinCEN Form 8300 – For further guidance, please refer to the Form 8300 section. • Suspicious Activity Reports (SAR) – For further guidance, please refer to the Suspicious Activity Reports section. • Report of Foreign Bank and Financial Accounts (FBAR) – For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section. • Report of International Transportation of Currency or Monetary Instruments (CMIR), FinCEN Form 105 – For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section. • Registration of Money Services Businesses (RMSB) – For further guidance, please refer to the Registration of Money Services Businesses section.
Currency (cash)	"Currency" is defined differently for Currency Transaction Reports (CTRs) and Form 8300 reporting requirements. For CTRs, currency means the coin and paper money of the United States or any other country, which is circulated and customarily used and accepted as money. For Form 8300 purposes, "currency" is defined as: • U.S. and foreign coin and currency received in any transaction • A cashier's check, money order, bank draft or traveller's check having a face amount of US$10,000 or less received in a designated reporting transaction, or received in any transaction in which the recipient knows that the instrument is being used in an attempt to avoid reporting requirements For further guidance, please refer to the sections: Currency Transactions, Currency Transaction Reports and Form 8300.
Currency Transaction Report (CTR)	A "Currency Transaction Report (CTR)" is a report filed by certain types of financial institutions for cash currency transactions of more than US$10,000 in one business day. Multiple transactions must be treated as a single transaction (aggregated) if the financial institution has knowledge that they are by or on behalf of the same person and result in cash-in or cash-out totalling more than US$10,000 in any one business day. For further guidance, please refer to the Currency Transaction Reports section.

Customer	"Customer" is defined differently for various types of institutions (e.g., depository institution, broker-dealer and casino). For example, for depository institutions, a customer is any person who opens a new account or enters into another formal relationship after October 1, 2003. "Person" in this context includes individuals, corporations, partnerships, trusts or estates, joint stock companies, joint ventures or other incorporated organisations or groups. For other definitions of customer, please see the Broker-Dealers in Securities and Casinos and Card Clubs sections.
Customer due diligence (CDD)	"Customer due diligence (CDD)" is information obtained for all customers. Information obtained for CDD should enable a financial institution to verify the identity of a customer and assess the risks associated with that customer. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.
Customer Identification Program (CIP)	The CIP is intended to enable the bank to form a reasonable belief that it knows the true identity of each customer. The CIP must include account opening procedures that specify the identifying information that will be obtained from each customer. It must also include reasonable and practical risk-based procedures for verifying the identity of each customer. Banks should conduct a risk assessment of their customer base and product offerings, and in determining the risks, consider: • The types of accounts offered by the bank. • The bank's methods of opening accounts. • The types of identifying information available. • The bank's size, location, and customer base, including types of products and services used by customers in different geographic locations. For further guidance, please refer to the Section 326 – Verification of Identification section.
Customer risk assessment	A "customer risk assessment" is a process that identifies the level of money laundering and terrorist financing risk inherent in a financial institution's customer base, either on an individual customer or customer segment basis. For further guidance, please refer to the Customer Risk Assessment section.
Customer risk profile	"Customer risk profile" is defined as "the information gathered about a customer to develop the baseline against which customer activity is assessed for suspicious transaction reporting." While the Beneficial Ownership Rule does not explicitly require covered financial institutions to risk rate each customer and update this profile on an ongoing basis, it does expect institutions to understand the ML and TF risks posed by their customers and be able to demonstrate their understanding. For further guidance on risk assessments, please refer to the Risk Assessments section.
Cyber-Related Sanctions Program	Established by Executive Order 13694 – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities and Executive Order 13757 – Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities, the Cyber-Related Sanctions Program blocks the property and property interests of individuals and entities involved in "significant malicious cyber-enabled activity" that resulted in or materially contributed to a significant threat to the national security, foreign policy or economic health or financial stability of the United States. Designees have been identified as persons who have been responsible for or complicit in, or have engaged in, directly or indirectly, any of the following: • Harmed, or otherwise significantly compromised the provision of services by a computer or network of computers that supports one or more entities in a critical infrastructure sector; • Caused a significant disruption to the availability of a computer or network of computers;

	• Caused a significant misappropriation of funds or economic resources, trade secrets, personal identifiers or financial information for commercial or competitive advantage or private financial gain; • Engaged in the receipt or use for commercial or competitive advantage or private financial gain, or by a commercial entity, outside the United States of trade secrets misappropriated through cyber-enabled means, knowing they have been misappropriated, where the misappropriation of such trade secrets is reasonably likely to result in or materially contribute to a significant threat to the national security, foreign policy or economy of the United States; • Tampered with, altered or caused a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions; • Materially assisted, sponsored or provided financial, material or technological support for, or goods or services to or in support of the aforementioned acts; or • Owned or controlled property or interests, acted or purported to act directly or indirectly for or on behalf of Specially Designated Nationals (SDN) as designated by the Cyber-Related Sanctions Program. The Cyber-Related Sanctions Program is implemented under 31 CFR 578 – Cyber-Related Sanctions Regulations. OFAC intends to publish more comprehensive regulations to provide additional guidance (e.g., key definitions, licensing policy). For additional guidance, please refer to the Cyber-Related Sanctions Program section.
Cyber-event	A "cyber-event" is defined by the Financial Crimes Enforcement Network (FinCEN) as "an attempt to compromise or gain unauthorised electronic access to electronic systems, services, resources or information." For additional guidance, please refer to the Cyber Events and Cybersecurity section.
Cybersecurity	"Cybersecurity" is defined by the National Institute of Standards and Technology (NIST) as "the ability to protect or defend the use of cyberspace from cyber attacks." For additional guidance, please refer to the Cyber Events and Cybersecurity section.
Date of detection	The "date of detection" that triggers the time period for filing a SAR begins when the financial institution, during its review of transaction or account activity or because of other factors, knows, or has reason to suspect, that the activity or transactions under review meet one or more of the definitions of suspicious activity. For further guidance on the date of detection, please see the SAR Filing Time Frame and Date of Initial Detection section.
Dealers in Precious Metals, Precious Stones and Jewels	A "dealer in precious metals, precious stones and jewels" is defined as anyone engaged as a business in the purchase and sale of covered goods that purchase and sell US$50,000 or more of "covered goods" (e.g., gold, silver, jewels) in the preceding year and is required to maintain an AML Program. For further guidance, please refer to the Dealers in Precious Metals, Precious Stones and Jewels section.
Denied Persons List (DPL)	A list of individuals and entities that have been denied export privileges. No exporter may participate in an export or re-export transaction subject to an Export Administration Regulation (EAR) with a person or entity whose export privilege has been denied by the BIS. For additional guidance, please refer to the Other U.S. and International Sanctions Programs and Trade Finance Activities sections.
Deposit broker	A deposit broker is an individual or a firm that, for a fee, places customers' deposits with insured depository institutions.

Depository institution	"Depository institutions" include banks, savings associations, thrift institutions and credit unions.
De-risking	"De-risking" often refers to a financial institution's policy to exit from a high-risk activity to reduce its inherent risk profile. For further guidance, please refer to the Risk Assessments section.
Designation of exempt persons (DOEP)	CTR exemptions are designations filed by eligible financial institutions that alleviate the requirement for filing CTRs when "exempted" customers conduct (deposit or withdraw) transactions in currency that exceed US$10,000 in one business day. Financial institutions can designate exempt customers by filing the Designation of Exempt Persons (DOEP), FinCEN Report 110, with FinCEN. For additional guidance, please refer to the CTR Exemptions and the Designation of Exempt Persons Form.

Designated nonfinancial businesses and professions (DNFPBs)	FATF defines designated nonfinancial businesses and professions (DNFBPs) as the following:
	• Casinos (including online casinos)
	• Real estate agents
	• Dealers in precious metals
	• Dealers in precious stones
	• Lawyers, notaries, other independent legal professionals and accountants
	  ○ Refers to sole practitioners, partners or employed professionals within professional firms; it is not meant to refer to professionals who are employees of other types of businesses, nor to professionals working for government agencies who already may be subject to measures that would combat money laundering and terrorist financing
	• Trust and company service providers
	  ○ Refers to all persons or businesses who are not covered elsewhere under the Recommendations, and which, as a business, provide any of the following services to third parties:
	  ▪ Acting as a formation agent of legal persons
	  ▪ Acting as (or arranging for another person to act as) a director or secretary of a company, a partner of a partnership, or a similar position in relation to other legal persons
	  ▪ Providing a registered office, business address or accommodation, correspondence or administrative address for a company, a partnership or any other legal person or arrangement
	  ▪ Acting as (or arranging for another person to act as) a trustee of an express trust
	  ▪ Acting as (or arranging for another person to act as) a nominee shareholder for another person

Drug trafficking	The United Nations (U.N.) defines "drug trafficking" as "a global illicit trade involving the cultivation, manufacture, distribution and sale of substances which are subject to drug prohibition laws." The Office of Foreign Assets Control (OFAC) defines "narcotics trafficking" as "any activity undertaken illicitly to cultivate, produce, manufacture, distribute, sell, finance or transport, or otherwise assist, abet, conspire, or collude with others in illicit activities relating to narcotic drugs, including, but not limited to, cocaine." For further guidance, please refer to the Drug Trafficking section.
E-cash	"E-cash," also known as "e-wallets" or "e-money," is a digital representation of currency (e.g. legal tender, in circulation, accepted as a medium of exchange in

	the country of issuance) that can be stored and retrieved in several forms, including computer-based, mobile telephone-based and prepaid cards. For further guidance, please refer to the Electronic Banking and Digital Value section.
Elder abuse	"Elder abuse" generally refers to intentional or negligent actions taken by a caregiver or other person presumed to be in a position of trust who causes harm or a serious risk of harm to a vulnerable, older adult. It can be a single act or a series of actions that causes harm or distress to an older person and may include physical, psychological or financial abuse, as well as neglect. For further guidance, please refer to the Elder Financial Abuse section.
Elder financial abuse	"Elder financial abuse" involves the exploitation of a relationship with an elder or dependent adult in order to steal, embezzle or improperly use the person's money, property or other resources. The exploitation may occur by deception, coercion, misrepresentation, undue influence or theft, and can include deprivation of money and/or property. For further guidance, please refer to the Elder Financial Abuse section.
Electronic banking	"Electronic banking," or "e-banking," is a broad term used to describe financial services provided to customers through various electronic delivery mechanisms or channels. Examples of e-banking include, but are not limited to, the following: • Automated teller machine (ATM) transactions; • Online account opening and banking transactions; • Mobile banking; • Telephone banking; and • Remote deposit capture (RDC) services. For further guidance, please refer to the Electronic Banking and Digital Value section.
Email account compromise (EAC)	Email account compromise is a scheme that targets a victim's personal accounts; victims may overlap with BEC victims as the scheme expands beyond the business activity of companies. Financial services professionals (e.g., attorneys, accountants, realtors) are frequent targets. For further guidance, please refer to the Cyber Events and Cybersecurity section.
Enforcement action	Regulators have a range of enforcement tools available to address AML Program deficiencies and violations of AML/CFT laws and regulations. These "enforcement actions" include: • Commitment Letters • Memorandums of Understanding (MOUs) • Formal Agreements • Consent Orders or Order to Cease and Desist (C & D) • Civil Money Penalties • "Death Penalty" For further guidance, please refer to the Enforcement Actions section.
Enhanced due diligence (EDD)	"Enhanced due diligence (EDD)" refers to additional information that would be collected for those customers deemed to be of higher risk. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.

Enterprisewide risk assessment	An "enterprisewide risk assessment" is an exercise intended to identify the aggregate ML and TF risks facing an organisation that may not be apparent in a risk assessment focused on a line of business, legal entity, or other assessment unit. In other words, it is the big picture view, or profile, of an organisation's ML/TF risks that aggregates the results of other risk assessment exercises in order to quantify and relate the total risks for the organisation to the established risk appetite and tolerance for the enterprise. For further guidance, please see the Enterprisewide Risk Assessment section.
Expected activity	"Expected activity" describes anticipated activity from a particular customer or account type, including types, amounts, geographical locations where transactions are done and frequencies of transactions; unlike average activity which describes the mean activity historically conducted by a customer through an account. Expected activity provides a narrative for the types of activities that are deemed normal for a particular customer or account. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence sections.
Fiat currency	"Fiat currency" is another term used to describe "real" currency that is government-issued. Similarly, in its report "Virtual Currencies: Key Definitions and Potential AML/CFT Risks," FATF defines "virtual currency" as a "digital representation of value that can be digitally traded and functions as: • A medium of exchange; and/or • A unit of account; and/or • A store of value that does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction." For further guidance, please refer to the Virtual Currencies section.
Financial inclusion	"Financial inclusion" generally refers to the availability of financial services at affordable costs to disadvantaged and lower income segments of the economy.
Financial institution	The term "financial institution" is defined differently for various regulations (e.g., USA PATRIOT Act, identity theft). The definition in the USA PATRIOT Act includes: • Insured banks • Commercial banks • Trust companies • Private banks • Agency or branch of a foreign bank in the United States • Credit unions • Thrift and saving institutions • Broker-dealers registered or required to register with the SEC • Securities/commodities broker-dealers • Futures commission merchants (FCM), introducing brokers (IB), commodity pool operators (CPO) and commodity trading advisers (CTA) registered or required to register under the Commodity Exchange Act (CEA) • State-licensed or Indian casinos with annual gaming revenue of more than US$1 million • Investment bankers • Investment companies • Currency exchanges • Issuer or seller of traveller's checks, money orders or similar instruments • Licensed sender of money or any other person who engages as a business in the transmission of funds, formally or informally • Operators of credit card systems

	• Insurance companies • Dealers in precious metals, precious stones or jewels • Pawnbrokers • Loan or finance companies [e.g., nonbank residential mortgage lenders or originators [RMLOs]) • Travel agencies • Telegraph companies • Businesses engaged in vehicle sales, including automobile, airplane and boat sales • Persons involved in real estate closings and settlements • The U.S. Postal Service • Agencies of the federal government or any state or local government, carrying out a duty or power of a business described in the definition of a "financial institution" • Any business or agency which engages in any activity which the Secretary of the Treasury determines, by regulation, to be an activity which is similar to, related to, or a substitute for any activity in which any of the above entities are authorised to engage (e.g., housing government-sponsored enterprises [GSEs]) • Any other business designated by the Secretary of the Treasury whose cash transactions have a high degree of usefulness in criminal, tax or regulatory matters For further guidance, please refer to the sections: USA PATRIOT Act Basics and BSA Basics.
Foreign Sanctions Evaders List (FSE List)	The "Foreign Sanctions Evaders List (FSE List)" includes persons engaged in conduct relating to the evasion of OFAC sanctions with respect to Iran, Syria, anti-terrorism and non-proliferation of weapons of mass destruction (WMDs). For further guidance, please refer to the OFAC Sanctions Listings section.
Form 8300	"Form 8300 (Cash Over 10K Received in Trade/Business)" should be completed and submitted to the Internal Revenue Service (IRS) if a person engaged in trade or business who, in the course of that trade or business, receives more than US$10,000 in single or multiple related transactions in currency or covered monetary instruments that are either received in a "designated reporting transaction" or in a transaction in which the recipient knows the monetary instrument is being used to try to avoid the reporting of the transaction. For further guidance, please refer to the Form 8300 section.
Free trade zones	"Free trade zones" are designated areas within countries that offer a free trade environment with minimal regulation. According to FATF, free trade zones are now located in over 130 countries. Financial institutions may consider conducting enhanced due diligence on parties and transactions associated with free trade zones. For further guidance, please refer to the Trade Finance Activities section.
Funds transfer	The term "funds transfer" means a series of transactions, beginning with the originator's payment order, made for the purpose of making payment to the beneficiary of the order. Funds transfers governed by the Electronic Funds Transfer Act of 1978 as well as any other funds transfers made through an ACH, ATM or a point-of-sale (POS) system are excluded from this definition. For further guidance, please refer to the Funds Transfers section.
Funds Transfer Recordkeeping Requirement	The basic requirements of the Funds Transfer Recordkeeping Requirement vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution, beneficiary institution). For each funds transfer of US$3,000 or more, the originating institution must obtain and retain the following information relating to the payment order: • The name and address of the originator

	• The amount of the payment order
	• The execution date of the payment order
	• Any payment instructions received from the originator with the payment order
	• The identity of the beneficiary's bank
	• As many of the following items as are received with the payment order:
	  ○ The name of the beneficiary
	  ○ The address of the beneficiary
	  ○ The account number of the beneficiary
	  ○ Any other specific identifier of the beneficiary
	Nonbank financial institutions (NBFIs) also must retain any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.
	For each funds transfer of US$3,000 or more that the financial institution accepts as an intermediary or beneficiary institution, the institution must retain a record of the payment order (e.g., original record, microfilm).
	This recordkeeping requirement for funds transfers and transmittals of funds is implemented under regulation 31 C.F.R. 1010.410 – Records to be Made and Retained by Financial Institutions.
	For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.

Funnel account	FinCEN defines a "funnel account" as "an individual or business account in one geographic area that receives multiple cash deposits, often in amounts below the cash reporting threshold, and from which the funds are withdrawn in a different geographic area with little time elapsing between the deposits and withdrawals." For further guidance, please refer to the Bulk Shipments of Currency and Bulk Cash Smuggling section.
Futures Commission Merchant (FCM)	A "futures commission merchant (FCM)" is a person or entity registered, or required to register, as an FCM with the Commodity Futures Trading Commission (CFTC) under the Commodity Exchange Act (CEA), except a person who registers pursuant to 4(f)(a)(2) of the CEA. FCMs conduct transactions in the futures market in a manner similar to that of brokers in the securities market. For further guidance, please refer to the Futures Commission Merchants and Introducing Brokers in Commodities section.
Geographic risk assessment	A "geographic risk assessment" is an exercise intended to identify the inherent ML/TF risks of the international and domestic jurisdictions in which a financial institution and its customers conduct business. For further guidance, please refer to the Geographic Risk Assessment section.
Geographic Targeting Order (GTO)	A "Geographic Targeting Order (GTO)" gives the U.S. Treasury Department, and in some instances states, the authority to require a financial institution or a group of financial institutions or companies in a geographic area to file additional reports or maintain additional records above and beyond ordinary AML/CFT requirements for (e.g., less than US$10,000 for CTRs). GTOs are used to collect information on individuals/entities suspected of conducting transactions under reportable thresholds. For further guidance, please refer to the Bulk Shipments of Currency and Bulk Cash Smuggling section.

GHRAVITY E.O.	On April 22, 2012, the U.S. president signed Executive Order 13606 – Blocking the Property and Suspending Entry Into the United States of Certain Persons With Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology (GHRAVITY E.O.). The GHRAVITY E.O. requires U.S. persons to block all property and interests in property of persons designated by the Secretary of the Treasury, in consultation with or at the recommendation of the Secretary of State, who: • Have operated, or directed the operation of, information and communications technology that facilitates computer or network disruption, monitoring or tracking that could assist in or enable serious human rights abuses by or on behalf of the government of Iran or the government of Syria; • Have sold, leased or otherwise provided, directly or indirectly, goods, services or technology to Iran or Syria likely to be used to facilitate such activities; • Have materially assisted, sponsored or provided financial, material or technological support for, or goods or services to or in support of, the activities described above or any person whose property and interests in property are blocked pursuant to this order; or • Have been owned or controlled by, or have acted or purported to act for or on behalf of, directly or indirectly, any person whose property and interests in property are blocked pursuant to the order. Entities that are 50 percent or more owned by persons blocked by the GHRAVITY E.O. are also blocked, regardless of whether such entities appear on the Annex or OFAC's SDN List. For further guidance, please refer to the Other U.S. and International Sanctions Programs section.
Government-sponsored enterprise (GSE)	A "government-sponsored enterprise (GSE)" is a financial services organisation created and regulated by the U.S. government (specifically, by Congress) and functioning to increase the availability and reduce the cost of credit to targeted sectors such as education, agriculture and home finance. GSEs that target home finance are called Housing GSEs. For further guidance, please refer to the Housing Government-Sponsored Enterprises section.
Hawala	"Hawala" is one type of informal value transfer system (IVTS). Hawala is an Arabic word that means "a bill of exchange or promissory note." For further guidance, please refer to the sections: Informal Value Transfer Systems and Money Services Businesses.
High Intensity Drug Trafficking Area (HIDTA)	"High Intensity Drug Trafficking Areas (HIDTAs)" are designated jurisdictions authorised in the Anti-Drug Abuse Act of 1988 to assist law enforcement with concentrating its efforts with drug control at the federal, state and local levels. Since the original designation of five HIDTAs in 1990, the program has expanded to 28 areas of the country, including, but not limited to, the following: • Appalachia (e.g., counties in Tennessee, Kentucky, Virginia and West Virginia) • New York/New Jersey • Rocky Mountain (e.g., counties in Colorado, Utah, Wyoming and Montana) • South Florida • Southwest Border (e.g., southern regions of California, Arizona, New Mexico and Texas) For further guidance, please refer to the Geographic Risk Assessment section.

High Intensity Financial Crimes Area (HIFCA)	"High Intensity Financial Crimes Areas (HIFCAs)" were designated in the Money Laundering and Financial Crimes Strategy Act of 1998 to assist law enforcement with concentrating its efforts in high-intensity money laundering zones at the federal, state and local levels. HIFCAs may be defined geographically; they also can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions. Examples include, but are not limited to, the following: • California (e.g., southern region, northern region) • Chicago • Southwest Border (e.g., Arizona, southern region of Texas) • New York/New Jersey • Puerto Rico • South Florida For further guidance, please refer to the Geographic Risk Assessment section.

High-Risk and Non-Cooperative Jurisdictions	High-Risk and Non-Cooperative Jurisdictions describe two primary groups:
	• Group 1: Jurisdictions with strategic AML/CFT deficiencies subject to a FATF call on its members and other jurisdictions to apply counter-measures to protect the international financial system from the ongoing and substantial money laundering and terrorist financing risks emanating from the jurisdictions; and
	• Group 2: Jurisdictions with strategic AML/CFT deficiencies that either:
	  ○ Have not made sufficient progress in addressing the deficiencies; or
	  ○ Have not committed to an action plan developed with FATF to address the deficiencies.
	For further guidance, please refer to the High-Risk and Non-Cooperative Jurisdictions section.

Horizontal risk assessment	A "horizontal risk assessment" is an exercise intended to identify systemic ML/TF risks of designated high-risk products/services and/or customers across an organisation regardless of which line of business or legal entity owns these activities or customers. For further guidance, please refer to the Horizontal Risk Assessment section.
Household	A "household" is generally defined as a grouping consisting of two or more distinct customers that share a common factor such as an address, phone number or business owner. For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags section.
Human smuggling	"Human smuggling," which is also known as migrant smuggling or alien smuggling. is defined by FinCEN as "acts or attempts to bring unauthorised aliens to or into the United States, transport them within the U.S., harbour unlawful aliens, encourage entry of illegal aliens, or conspire to commit these violations, knowingly or in reckless disregard of illegal status." For further guidance, please refer to the Human Trafficking and Migrant Smuggling section.
Human trafficking	FinCEN defines "human trafficking," which is also known as modern slavery, as the "act of recruiting, harbouring, transporting, providing or obtaining a person for forced labour or commercial sex acts through the use of force, fraud or coercion" For further guidance, please refer to the Human Trafficking and Migrant Smuggling section.
Identity Theft	Identity theft is defined as fraud committed or attempted using the identifying information of another person without authority.

Informal value transfer system (IVTS)	An "informal value transfer system (IVTS)" refers to any system, mechanism or network of people operating outside of the traditional financial system that receives money for the purpose of making the funds or an equivalent value payable to a third party in another geographic location, regardless of whether the funds are in the same form. For further guidance on these systems, please refer to the Informal Value Transfer Systems section.
Inherent risk	"Inherent risk" is the risk to an entity in the absence of any actions management might take (e.g., controls) to alter either the risk's likelihood or impact. For further guidance, please refer to the Risk Assessments section.
Insider abuse	"Insider abuse" generally refers to violations or attempted violations of laws, regulations or internal policies by employees (e.g., directors, officers) for personal gain. Insiders may have the knowledge and ability to evade internal controls designed to prevent money laundering and terrorist financing. For further guidance, please refer to the Know Your Employees section.
Insider trading	"Insider trading" refers to the buying and selling of stocks by corporate insiders (e.g., employees, directors). According to the SEC, there are two types of insider trading: • Legal insider trading – Conducted in accordance with securities laws and internal company policies that must be reported by the broker-dealer to the SEC (e.g., statement of ownership [initial, changes, deferred] on Forms 3, 4 and 5 respectively). • Illegal insider trading – Conducted in violation of securities laws (e.g., may involve a breach of fiduciary duty or violation of law such as "tipping" [e.g., disclosing material non-public information]). For further guidance, please refer to the Broker-dealers in Securities section.
Interbank account	An "interbank account" is an account owned by a financial institution that is held with another financial institution for the primary purpose of facilitating customer transactions (e.g., correspondent accounts, payable-through accounts [PTAs], concentration accounts). For further guidance, please refer to Section 319 – Forfeiture of Funds in United States Interbank Accounts.
Interdiction software	"Interdiction software," also known as filtering or screening software, is a tool that facilitates the comparison of separate sets of data (e.g., a customer database, list of individuals/businesses linked to illicit activity) for possible matches. Some vendors provide detailed background information for the individuals/entities, while others provide limited information (e.g., name, address). Interdiction software can involve screening customers, as well as transactions (e.g., wires, ACHs). For further guidance, please refer to the AML/CFT Technology section.
International Automated Clearing House Transaction (IAT)	An "international automated clearing house transaction (IAT)" is a standard entry class (SEC) code used to identify cross-border ACH transactions. For further guidance, please refer to the section: Automated Clearing House Transactions and IATs.

Internet gambling	Simply put, internet gambling is the online wagering of money or other value. Other terms used include online gambling and the more comprehensive term, remote gambling, which includes gambling through the use of remote communications such as the internet, smartphone, telephone, radio and television. Much of the legislation on gambling was enacted prior to the invention of the internet. In the United States, there is no common definition of internet gambling, so the legality or illegality of some activities must be determined based on the particular facts. Examples of activities considered as a type of internet gambling include, but are not limited to, the following: • Online poker; • Internet lottery; and • Simulated gambling in virtual multiplayer online games (MMOGs). For additional guidance, please refer to the Illegal Internet Gambling and Fantasy Sports Wagering section.
Introducing broker (IB)	An IB is any person or entity that is registered, or required to be registered, with the CFTC as an IB under the CEA, except a person who registers pursuant to 4(f)(a)(2) of the CEA. For additional guidance, please refer to the Futures Commission Merchants and Introducing Brokers in Commodities section.
Investigation	An "investigation" is the review of transactions/conduct, which may have been identified in routine monitoring or brought to an institution's attention by regulators or law enforcement, in order to classify the alert as a "false positive" or a "true positive," which will require further analysis and could result in the filing of a SAR. For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags section.
Investment adviser	The Investment Advisor Act of 1940 defines an "investment adviser" as "any person who, for compensation, engages in the business of advising others, either directly or through publications or writings, as to the value of securities or as to the advisability of investing in, purchasing, or selling securities, or who, for compensation and as part of a regular business, issues or promulgates analyses or reports concerning securities." For further guidance, please refer to the Registered Investment Advisers and Unregistered Investment Companies section.
Issuers and sellers of money orders and traveller's checks	An issuer is defined as "a person that issues money orders or traveller's checks that are sold in an amount greater than US$1,000 to any person on any day in one or more transactions." A seller is defined as "a person that sells money orders or traveller's checks in an amount greater than US$1,000 to any person on any day in one or more transactions." For additional guidance, please refer to the Issuers and Sellers of Money Orders and Traveller's Checks section.
Junket representative	A "junket representative" is the organiser of a group of well-known players; a "junket" who travel together for the purpose of gambling. For further guidance, please refer to the Casinos and Card Clubs section.
Kimberley Process Certificate Scheme (KPCS)	Launched in 2003, the "Kimberley Process Certificate Scheme (KPCS)" is an international program that implements certification requirements and other import/export controls to prevent the production and trade in rough diamonds that are used to finance violence in countries in conflict (e.g., Democratic Republic of the Congo, Cote d'Ivoire). These diamonds are also known as "conflict diamonds" or "blood diamonds." For further guidance, please refer to the Rough Diamond Trade Controls Sanctions Program section.

Know Your Customer (KYC) program	"Know Your Customer (KYC)," also referred to as an onboarding program or customer acceptance and maintenance program, generally refers to the steps taken by a financial institution to: • Establish the identity of a customer; • Understand the nature of a customer's activities (ultimately to be satisfied that the source of the customer's funds is legitimate); and • Assess the ML and TF risks associated with that customer. For further guidance, please refer to the Know Your Customer, Customer Due Diligence and Enhanced Due Diligence section.
Know Your Customer's Customer (KYCC)	While there is no U.S. law that requires it, in certain situations (e.g., where a financial institution provides clearing services for a correspondent), financial institutions may be expected to demonstrate an understanding of their customers' customers. This may be accomplished by conducting due diligence directly or indirectly by requesting information from the correspondent banking customer (e.g., respondent). This policy is known as Know Your Customer's Customer (KYCC) or Know Your Correspondent's Customer (KYCC). Due to the uncertainty around KYCC, many financial institutions have opted to de-risk by terminating high-risk correspondent accounts instead of managing the high compliance burden of such relationships. To counter de-risking activities, several agencies (e.g., U.S. federal banking regulators) have issued guidance that KYCC is not required under current AML/CFT laws and regulations. For additional guidance, please refer to the Correspondent Banking section.
Knowingly	"Knowingly" means actual knowledge or constructive knowledge (i.e., the person should have known) within the context of select Iranian and Syrian sanctions. For further guidance, please refer to the Iranian and Syrian Sanctions Overview section.
Look back	A look back is a regulator or self-directed review performed for a certain period and/or of a certain type of accounts or transactions to identify any usual or potentially suspicious activity that may have been previously overlooked. Regulators may require that a look back be performed if they conclude that a financial institution has a poorly designed or implemented transaction monitoring program. Self-directed look backs are often performed when a financial institution identifies a pattern of unusual or potentially suspicious activity and decides that it should conduct a more in-depth review to determine when the activity began and how pervasive it has been. For additional guidance, please refer to the Monitoring Guidance section.
Memorandum of Understanding (MOU)	A "Memorandum of Understanding (MOU)" is an agreement between a bank's board of directors and one or more regulatory agencies. The content of an MOU may be similar or identical to more formal enforcement actions, but MOUs are non-public documents and, similar to Commitment Letters, not legally binding. For further guidance, please refer to the Enforcement Action section.
Migrant Smuggling	See "Human Smuggling."

Model Validation and Model Governance	Model validation is an exercise conducted by an independent team (i.e., a team that does not directly own the model in question) to ascertain whether the subject model is working as intended. The effort involves execution of a battery of tests against data (e.g., transactions, customers, accounts), logic (e.g., scenario logic, risk rating calculation) and outputs (e.g., alerts, assigned risk scores) to ascertain whether the respective test results are in accordance with the expected test results. Model governance refers to the processes and frameworks by which an entity manages its models. These processes and frameworks include, but are not necessarily limited to: the roles and responsibilities of the board, management, and business units across the model life cycle; independent model validation; maintenance of a model inventory; standards for model documentation; change control management; access controls; ongoing monitoring programs; and model risk control requirements. For further guidance, please refer to the Model Validation section.
Micro structuring	"Micro structuring" is a form of structuring that involves breaking transactions into small amounts, typically ranging from US$500 to US$1,500, and more frequent depositing of currency into a higher number of bank accounts than is done in classic structuring schemes. For further guidance on micro structuring, please see the CTR Evasion section.
Monetary instrument	The definition of "monetary instruments" varies based on the specific AML/CFT requirement. For example, for the Report of International Transportation of Currency or Monetary Instruments (CMIR), monetary instruments are defined as: • Coin or currency of the United States or of any other country; • Traveller's checks in any form; • Negotiable instruments (e.g., checks, promissory notes, money orders) in bearer form, endorsed without restriction, made out to a fictitious payee, or otherwise in such form that title thereto passes upon delivery; • Incomplete instruments (including checks, promissory notes, and money orders) that are signed but on which the name of the payee has been omitted; and • Securities or stock in bearer form or otherwise in such form that title thereto passes upon delivery. For CMIRs, monetary instruments do not include: • Checks or money orders made payable to the order of a named person which have not been endorsed or which bear restrictive endorsements; • Warehouse receipts; or • Bills of lading. For the Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments, monetary instruments include: • Bank check or draft • Foreign draft • Cashier's check • Money order • Traveller's check For further guidance, please refer to the sections: Monetary Instruments, Report of International Transportation of Currency or Monetary Instruments (CMIR), Recordkeeping Requirements for the Purchase and Sale of Monetary Instruments.
Money laundering	"Money laundering" is the attempt to disguise the proceeds of illegal activity, so that it appears to come from legitimate sources or activities. For further guidance, please refer to The Fundamentals section.
Money or value transfer services	See "Money services business."

Money services business (MSB)	FinCEN defines a "money services business (MSB)" as "a person wherever located doing business, whether or not on a regular basis or as an organised or licensed concern, wholly or in substantial part within the United States, in one or more capacities" listed below: • Issuer or seller of money orders or traveller's checks • Check casher • Dealer in foreign exchange • Provider or seller of prepaid access • Money transmitter For further guidance, please refer to the Money Services Businesses section.
Money transmitter	A money transmitter is defined as the following: • Any person engaged in the transfer of funds • A person who provides money transmission services "Money transmission services" is defined as "the acceptance of currency, funds or other value that substitutes currency from one person and the transmission of currency, funds or other value that substitutes for currency to another location or person by any means." "By any means" includes money transmission through the following: • A financial agency or institution; • A Federal Reserve Bank or other facility of one or more Federal Reserve Banks, the Board of Governors of the Federal Reserve System or both; • An electronic funds transfer network; or • An informal value transfer system (IVTS). For further guidance, please refer to the Money Transmitters section.
Monitoring	"Monitoring" is a general term used to describe processes designed to detect and identify potentially suspicious activity. Monitoring is not limited to reviews of transaction activity. Potentially suspicious activity can be detected in other types of customer activities (e.g., provision of fraudulent or inaccurate documentation during account opening, enhanced due diligence reviews). Monitoring should be risk-based and ongoing. For further guidance, please refer to the Transaction Monitoring, Investigations and Red Flags section.
Mortgage fraud	Mortgage fraud is generally defined as any material misstatement, misrepresentation or omission relied upon by an underwriter or lender to fund, purchase or insure a loan. There are two types of mortgage fraud: fraud for housing/property and fraud for profit. The former typically involves misstatements about income, debt or property value by the borrower in order to qualify for a mortgage in which he/she usually intends to pay. The latter typically involves collusion among industry professionals involved in the mortgage process (e.g., mortgage brokers, real estate agents, appraisers, attorneys, title examiners) in order to qualify for a mortgage and generate a profit with no intention to pay the mortgage. Profits can be generated in multiple ways, such as by obtaining a mortgage and not paying it back or by flipping properties with inflated property values. In both types of mortgage fraud, lenders may extend credit that the lender would likely not have offered if the true facts were known. For additional guidance, please refer to the Mortgage Fraud section.

Mutual Evaluations	A mutual evaluation is an assessment of adherence to the FATF Recommendations. Through the mutual evaluation, FATF is able to perform an in-depth evaluation of a country's system for preventing criminal abuse of the financial system; it helps FATF to quantify each country's risk exposure to money laundering and terrorist financing, among other financial crimes. For additional guidance, please refer to the Mutual Evaluations: Methodology and Reports section.
Mutual Fund	A "mutual fund" is an open-ended investment company that is registered or required to register with the Securities and Exchange Commission (SEC) under Section 5 of the Investment Company Act. For further guidance, please refer to the Mutual Funds section.
Narcotics and bulk currency corridor	"Narcotics and bulk currency corridors" are established distribution channels or logistical highways for the transportation of narcotics and the illicit proceeds from the sale of narcotics. For further guidance, please refer to the Geographic Risk Assessment section.
National Security Letter (NSL)	"National Security Letters (NSLs)" are written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) office and other federal governmental authorities in counterintelligence and counterterrorism investigations to obtain the following: • Telephone and electronic communications records from telephone companies and internet service providers • Information from credit bureaus • Financial records from financial institutions For further guidance, please refer to Section 505 –- Miscellaneous National Security Authorities.
Nested relationship	A "nested" relationship occurs when a correspondent bank client provides services to other banks. Nested relationships may expose financial institutions to the risks of downstream correspondents about which the financial institution may have little knowledge. If undetected, the financial institution may provide services to correspondents for which services have been terminated. For further guidance, please refer to the Correspondent Banking section.
Nonbank financial institution (NBFI)	For purposes of this guide, "nonbank financial institutions (NBFIs)" include all entities excluding depository institutions that are considered financial institutions under the USA PATRIOT Act. For further guidance, please refer to the Nonbank Financial Institutions and Nonfinancial Businesses section.
Nondeposit investment product	Nondeposit investment products (NDIPs) include various types of investment products (e.g., securities, bonds, fixed or variable annuities, mutual funds) that may be offered by a financial institution directly through proprietary programs with subsidiaries or affiliates, or indirectly through third-party networking arrangements. Third-party networking arrangements may include relationships with third-party financial services corporations (e.g., investment firms, securities broker-dealers, insurance companies) to offer NDIP on the premises of the financial institution. These may include co-branded products and dual-employee arrangements where products are co-sponsored by the financial institution and a third-party institution, or third-party arrangements where a third-party institution leases space from the financial institution to offer its NDIPs independent of the hosting financial institution. For further guidance, please refer to the Nondeposit Investment Products section.

Nongovernmental organisation (NGO)	Nongovernmental organisations (NGOs) are organisations that are independent from government. Some are for-profit organisations, but the majority of NGOs are not-for-profits with a wide range of causes (e.g., human rights abuses, environmental degradation). For further guidance, please refer to the Charitable Organisations and Nongovernmental Organisations section.
Non-resident alien (NRA)	An alien is any person who is not a U.S. citizen. For tax purposes, the Internal Revenue Service (IRS) classifies aliens as either resident aliens or non-resident aliens (NRAs) based on (1) a Green Card test or (2) a Substantial Presence test. A non-resident alien is an alien who does not meet the Green Card test or the Substantial Presence test. For NRAs, only income that is generated from U.S. sources, excluding certain investments such as stocks, is subject to taxation. For further guidance, please refer to the Know Your Customer Types: Non-resident Aliens and Foreign Persons section.
Non-Specially Designated Nationals Palestinian Legislative Council List (NS-PLC List)	The "Non-Specially Designated Nationals Palestinian Council List (NS-PLC List)" is composed of members of the Palestinian Legislative Council who were elected on the party slate of Hamas or other designated foreign terrorists or terrorist organisations not named on the SDN List. For further guidance, please refer to the OFAC Sanctions Listings section.
OFAC Sanctions Compliance Program	Although OFAC does not dictate specific components of compliance programs, a financial institution is expected to implement a risk-based OFAC Sanctions Compliance Program that addresses adherence to sanctions, including, but not limited to screening against OFAC Sanctions Listings (e.g., Specially Designated Nationals and Blocked Persons List [SDN List]), reporting blocked and/or rejected transactions, and designating an individual responsible for OFAC compliance. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.
OFAC Sanctions Listings	As part of its enforcement efforts, OFAC publishes multiple lists of individuals and companies owned or controlled by, or acting for or on behalf of, the governments of targeted countries, collectively referred to as "OFAC Sanctions Listings" in this publication. OFAC Sanctions Listings include the following: • OFAC Specially Designated Nationals and Blocked Persons List (SDN List) • Non-SDN Palestinian Legislative Council List (NS-PLC List) • Foreign Sanctions Evaders List (FSE List) • Sectoral Sanctions Identifications List (SSI List) • List of Foreign Financial Institutions Subject to Part 561 (Part 561 List) • Non-SDN Iranian Sanctions Act (NS-ISA) List • List of Persons Identified as Blocked Pursuant to Executive Order 13599 (the 13599 List) For further guidance, please refer to the OFAC Sanctions Listings section.

OFAC Sanctions Programs	OFAC administers and enforces economic and trade sanctions against certain individuals, entities, foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. These programs are collectively referred to as OFAC Sanctions Programs and include, but are not limited to, the following: • Counter Terrorism Sanctions • Counter Narcotics Trafficking Sanctions • Cyber-Related Sanctions • Non-Proliferation Sanctions • Transnational Criminal Organisations Sanctions • Rough Diamond Trade Controls • Country- and Regime-Based Sanctions For further guidance, please refer to the OFAC Sanctions Programs section.
OFAC/Sanctions risk assessment	An "OFAC/Sanctions risk assessment" identifies an organisation's level of vulnerability to noncompliance with economic sanctions administered by OFAC. This is accomplished by evaluating, among other factors, the inherent risk of products and services, customer types and the geographic origin and destination of transactions, and the controls mitigating those risks. For further guidance, please refer to the Office of Foreign Assets Control/Sanctions Risk Assessment section.
Offshore financial center (OFC)	"Offshore financial centres (OFCs)" are jurisdictions that have a relatively large number of financial institutions engaged primarily in business with non-residents. For further guidance, please refer to the section: Business Entities: Shell Companies, Private Investment Companies and Others.
Operators of credit card systems	An operator of a credit card system is a business in the United States that administers a system for clearing and settling transactions in which the operator's credit card, whether acting as a credit card or debit card, is used to purchase goods or services or to obtain a cash advance, and authorises another entity to serve as an issuing or acquiring institution for the operator's credit card, which must be usable in the United States. Although there are many issuing and acquiring institutions, there are few operators of such systems in the United States (e.g., MasterCard, Visa). For further guidance, please refer to the Operators of Credit Card Systems section.
Part 561 List	The "List of Foreign Financial Institutions Subject to Part 561 (Part 561 List)" includes entities which have violated Iranian Financial Sanctions Regulations (IFSR) pursuant to the Comprehensive Iran Sanctions, Accountability, and Divestment Act (CISADA) (2010). For further guidance, please refer to the OFAC Sanctions Listings section.
Payable-through account (PTA)	A "payable-through account (PTA)," also known as a "pass through" or "pass-by" account, is an account maintained for a respondent that permits the respondent's customers to engage, either directly or through a subaccount, in banking activities (e.g., check writing, making deposits), usually in the United States. For further guidance, please refer to the Payable-Through Accounts section.
Participating Foreign Financial Institution (PFFI)	A participating foreign financial institution is an FFI that signs an FFI agreement with the IRS. See also "Foreign financial institution" (FFI) entry. For further guidance, please refer to the Foreign Account Tax Compliance Act section.

Pharming	"Pharming" is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by secretly redirecting users from legitimate websites to websites created by scammers. For further guidance, please refer to the Identity Theft and Identity Theft Prevention Program section.
Phishing	"Phishing" is a method of fraudulently obtaining identity or other sensitive information (e.g., passwords, security answers) by masquerading as a legitimate entity in an electronic communication (e.g., email, spyware). For example, an individual may receive an email that appears to be from his or her bank that requests identity and/or password information under the guise of "verification" purposes. For further guidance, please refer to the Identity Theft and. Identity Theft Prevention Program section.
Politically exposed person (PEP)	A "politically exposed person (PEP)" has been defined by multiple sources (e.g., USA PATRIOT Act, FATF and the Wolfsberg Group of Banks). Under the USA PATRIOT Act, a "politically exposed person" (PEP) is a senior foreign political figure, such as a current or former senior official in the executive, legislative, administrative, military or judicial branches of a foreign government (whether elected or not), a senior official of a major foreign political party, or a senior executive of a foreign government-owned commercial enterprise; a corporation, business or other entity formed by or for the benefit of any such individual; an immediate family member of such an individual; or any individual publicly known (or actually known by the financial institution) to be a close personal or professional associate of such an individual. For further guidance on PEPs, please see sections: Politically Exposed Persons and Enhanced Due Diligence for Private Banking Accounts.
Pouch activity	"Pouch activity," also known as "pouch services" or "cash letters," is the use of a courier to transport currency, monetary instruments, loan payments and other financial documents to a financial institution. Pouches can be sent by another financial institution or by an individual and are commonly offered in conjunction with correspondent banking services. For further guidance, please refer to the Pouch Activity section.
Predicate crimes/predicate offenses	The United States lists hundreds of specified unlawful activities (SUAs) including 20 of the 21 designated categories of predicate offenses recommended by FATF, including, but not limited to, the following: • Racketeering activity (e.g., any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter or dealing in a controlled substance or listed chemical as defined by the Controlled Substances Act), which is chargeable under state law and punishable by imprisonment for more than one year; • Terrorist financing; • Counterfeiting (e.g., currency, goods); • Fraud (e.g., securities fraud, wire fraud); • Slavery, trafficking in persons and alien smuggling; • Illegal arms sales (e.g., chemical weapons, nuclear material); and • Illegal gambling. Tax crimes are not SUAs, although tax evasion with income from legitimate sources is considered a predicate crime for money laundering in the United States, if intent to violate federal law can be proven. FATF's designated categories of predicate offenses to money laundering include the following: • Participation in an organised criminal group and racketeering • Terrorism, including terrorist financing • Trafficking in human beings and migrant smuggling • Sexual exploitation, including sexual exploitation of children • Illicit trafficking in narcotic drugs and psychotropic substances

	• Illicit arms trafficking • Illicit trafficking in stolen and other goods • Corruption and bribery • Fraud • Counterfeiting currency • Counterfeiting and piracy of products • Environmental crime • Murder, grievous bodily injury • Kidnapping, illegal restraint and hostage-taking • Robbery or theft • Smuggling (including in relation to customs and excise duties and taxes) • Tax crimes (related to direct taxes and indirect taxes) • Extortion • Forgery • Piracy • Insider trading and market manipulation For further guidance, please refer to the Key FATF Definitions with Comparisons to U.S. Definitions and Financial Action Task Force sections.
Prepaid access	"Prepaid access" is defined by FinCEN's final rule "Definitions and Other Regulations Relating to Prepaid Access" as the access to funds or the value of funds that have been paid in advance and can be retrieved or transferred at some point in the future through an electronic device or vehicle, such as a card, code, electronic serial number, mobile identification number or personal identification number. Prepaid access applies to a very broad range of prepaid services, including but not limited to open-loop prepaid access, closed-loop prepaid access, prepaid access given for the return of merchandise, many prefunded employee programs such as a Health Savings Account. For further guidance, please refer to the sections: Prepaid Access and Stored-Value, and Providers and Sellers of Prepaid Access.
Prepaid access provider	A "provider of prepaid access" is defined as the participant within a prepaid program that agrees to serve as the principal conduit for access to information from its fellow program participants. The participants in each prepaid access program (which may be one or more) must determine a single participant within the prepaid program to serve as the provider of prepaid access (provider). The provider also will be the primary contact and source of information for FinCEN, law enforcement and regulators for the particular prepaid program. For further guidance, please refer to the sections: Prepaid Access and Stored-Value and Providers and Sellers of Prepaid Access.
Prepaid access seller	A "seller of prepaid access" is defined as any person who receives funds or the value of funds in exchange for an initial or subsequent loading of prepaid access if: • That person either sells prepaid access offered under a prepaid program that can be used before the customer's identity can be captured (including name, address, date of birth and identification number) and verified; or • That person sells prepaid access (including closed-loop prepaid access) to funds that exceed US$10,000 to any person or entity (there is a limited exception for bulk sales) on any one day and has not implemented policies and procedures to reasonably prevent such sales. For further guidance, please refer to the sections: Prepaid Access and Stored-Value and Providers and Sellers of Prepaid Access.

Private banking account	A “private banking account” is defined in the USA PATRIOT Act as an account (or combination of accounts) maintained at a financial institution that meets the following criteria: • Requires a minimum aggregate deposit of funds or other assets of not less than US$1 million; • Is established on behalf of or for the benefit of one or more non-U.S. persons who are direct or beneficial owners of the account; and • Is assigned to, or is administered or managed by, in whole or in part, an officer, employee or agent of a financial institution acting as a liaison between the financial institution and the direct or beneficial owner of the account. For further guidance, please refer to the sections: Private Banking, Due Diligence for Private Banking Accounts and Enhanced Due Diligence for Private Banking Accounts.
Private investment company (PIC)	A “private investment company (PIC)” generally is a company formed by one or more individuals to own and manage his or her assets. Often established in offshore financial centres (OFCs) for tax reasons, PICs provide confidentiality and anonymity to the beneficial owners of the funds since the management of the PIC often rests with a third party not readily associated with the beneficial owner. For further guidance, please refer to the Business Entities: Shell Companies and Private Investment Companies section.
Proceeds of foreign corruption	“Proceeds of foreign corruption” are defined by Section 312 of the USA PATRIOT Act as assets or properties that are acquired by, through or on behalf of a senior foreign political figure through the following: • Misappropriation, theft or embezzlement of public funds; • The unlawful conversion of property of a foreign government; or • Acts of bribery or extortion. Properties into which any such assets have been transformed or converted also are covered under this definition. For further guidance, please refer to the Senior Foreign Political Figure section.
Product/service risk assessment	A “product/service risk assessment” is an exercise intended to identify the inherent ML/ TF risks of the products and services offered by a financial institution. For further guidance, please refer to the Product/Service Risk Assessment section.
Professional service provider	A “professional service provider,” also referred to as a “gatekeeper,” acts as an intermediary between its client and a third-party financial institution and may conduct or arrange for financial dealings and services on its client’s behalf (e.g., management of client finances, settlement of real estate transactions, asset transfers, investment services, trust arrangements). Examples of professional service providers include lawyers, notaries and accountants. For further guidance, please refer to the Professional Service Providers section.
Registered Deemed Compliant Foreign Financial Institution (RDCFFI)	A registered deemed compliant foreign financial institution (RDCFFI) must meet IRS definition requirements, agree to conditions and register with the IRS, and renew their IRS certification every three years. Examples of registered deemed-compliant FFIs might be non-reporting members of FFI groups, qualified investment vehicles and restricted funds. See also the FFI entry. For further guidance, please refer to the Foreign Account Tax Compliance Act section.

Registration of Money Services Businesses (RMSB)	Money services businesses (MSBs) must register with FinCEN by completing a "Registration of Money Services Business (RMSB)" within 180 calendar days after the date the business is established. MSBs must reregister every two years on or before December 31 using the same RMSB form. For further guidance, please refer to the Registration of Money Services Businesses section.
regtech	Regulatory Technology, or simply regtech, is a specific branch of fintech that focuses solely on the application of a technology framework to automate various regulatory business processes. Like fintech, regtech applies the same nimble, scalable, mobile-friendly solutions and rapid, low-cost deployment to improve risk management, transaction monitoring, regulatory compliance, reporting, data storage and analytics. It offers new ways of solving old problems by offering speed, security, and agility in complying with regulatory requirements. As such, financial institutions have good reasons to look forward to implementing the technology. Although regtech is still in its infancy and the market is very fragmented, it has the potential to replace many of the traditional manual and paper-based solutions which also tend to be resource-intensive, tying up both capital and IT capacity. Applied to AML/CFT compliance, a regtech real-time transaction monitoring solution can bridge communication gaps by consolidating and analysing data from disparate systems. Applied to know-your-customer (KYC) processes, regtech can be used to create a secure central data repository with reference data utilities to protect personally identifiable information. The technology also can monitor financial services regulations in every country and region within an institution's footprint, and report back to internal audit. Risk Reporting (Management Reporting) is also a feature that many financial institutions and regtech firms are improving by providing on demand and visual renditions of various static reports. For further guidance, please refer to the Future of AML/CFT Technology section.
Reintegro	"Reintegro" refers to a trade-based, reverse-BMPE laundering scheme that hinges on trade document manipulation and often includes the corruption of a bank employee or customs official. Unlike traditional BMPE activities that operate with goods (not funds) crossing the border, in reintegro transactions, peso exchange brokers repatriate drug proceeds by disguising them as payments for non-existent or overvalued goods using purchased export papers, similar to letters of credit, to make the payments appear legitimate. This is known as "reintegro" or "reintegrate papers." For further guidance, please refer to the Reintegro section.
Remote deposit capture (RDC)	"Remote deposit capture (RDC)" is the process by which a customer deposits a check or other monetary instrument into an account at a financial institution from a remote location via transmission of digital information or a scanned image to the financial institution rather than delivery of the physical check. RDC is used for domestic transactions and is more frequently being used to replace international pouch activities. For further guidance, please refer to the Remote Deposit Capture section.
Report of International Transportation of Currency or Monetary Instruments (CMIR)	The "Report of International Transportation of Currency or Monetary Instruments (CMIR)" is required to be filed by: • Each person who physically transports, mails or ships, or causes (or attempts to cause) to be physically transported, mailed or shipped, currency or other monetary instruments in an aggregate amount exceeding US$10,000 at one time from the United States to any place outside of the United States or into the United States from any place outside of the United States • Each person who receives U.S. currency or other monetary instrument(s) in an aggregate amount exceeding US$10,000 at one time, which has been transported, mailed or shipped from any place outside of the United States For further guidance, please refer to the Report of International Transportation of Currency or Monetary Instruments section.

Report of Foreign Bank and Financial Accounts (FBAR)	"Report of Foreign Bank and Financial Accounts (FBAR)," is a report that must be filed by a U.S. person who has a financial interest in, or signature or other authority over, any foreign financial accounts, including bank, securities or other financial accounts in a foreign country, which have a maximum value exceeding US$10,000 (alone or in aggregate) at any time during a calendar year. The report must be filed with the U.S. Department of the Treasury on or before June 30 of the following calendar year. For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section.
Resident Alien	An alien is any person who is not a U.S. citizen. For tax purposes, the Internal Revenue Service (IRS) classifies aliens as either resident aliens or non-resident aliens (NRAs) based on (1) a Green Card test or (2) a Substantial Presence test. Resident Alien: If the alien has a Green Card, also known as an alien registration receipt card, or if he or she was physically present in the United States for 31 days during the current year and 183 days during a three-year period that includes the current year and the two years immediately before that, the alien is then classified as a resident alien and his or her earned income is taxed like a U.S. citizen's earned income. For further guidance, please refer to the Know Your Customer Types: Non-resident Aliens and Foreign Persons section.
Residential mortgage lender or originator (RMLO)	A "residential mortgage lender" is defined as "the person to whom the debt arising from a residential mortgage loan is initially payable on the face of the evidence of indebtedness or, if there is no such evidence of indebtedness, by agreement, or to whom the obligation is initially assigned at or immediately after settlement." Individuals who finance the sale of their own dwelling or real property are not included in the definition of residential mortgage lender. A "residential mortgage originator" is defined as "a person who accepts a residential mortgage loan application or offers or negotiates terms of a residential mortgage." For further guidance, please refer to the Loan or Finance Companies/Nonbank Residential Lenders and Originators section.
Residual risk	"Residual risk" is the risk remaining after all controls have been applied to reduce the likelihood or impact of the risk. For further guidance, please refer to the Risk Assessments section.
Respondent bank	A "correspondent bank" (correspondent) is the financial institution providing the banking services. A "respondent bank" (respondent) is the financial institution utilising these account services, whether foreign or domestic. For further guidance, please refer to the sections: Correspondent Banking and Section 312 – Special Due Diligence for Correspondent Accounts and Private Banking Accounts.
Risk assessment	FATF defines a "risk assessment" as "a process based on a methodology, agreed by those parties involved, that attempts to identify, analyse and understand risks and serves as a first step in addressing them and making judgments" about identified risks. Risk assessments may be designed to measure the following on a line of business or at an enterprise level: • Inherent risks; • Controls or control environment (e.g., strengths/deficiencies in a compliance program); and • Residual risk. Examples of AML/CFT risk assessments include, but are not limited to, the following: • Enterprisewide Risk Assessment • Horizontal Risk Assessment • Line of Business/Legal Entity Risk Assessment

	• Geographic Risk Assessment • Product/Service Risk Assessment • Customer Risk Assessment • OFAC/Sanctions Risk Assessment For further guidance, please refer to the Risk Assessments section.
Risk assessment methodology	A risk assessment methodology is an institution's documented process and approach for conducting the risk assessment. A methodology document typically includes the following: • A detailed description of the procedures to follow in conducting the risk assessment; • The roles of responsible and accountable parties; • The scoring system(s) used along with definitions and weights; • Supporting data types and sources; • Frequency of updates; • Required approvals; and • Usage in shaping the compliance program. For further guidance, please refer to the Risk Assessment section.
Robotic process automation (RPA)	Robotic process automation is the ability of the system to capture relevant information, analyse that information and take appropriate action to move the task at hand to the next step in the respective business process. A practical application of robotic process automation is the ability to capture the publicly available information for a given alerted customer, populate it in the alert investigation form and discern whether the alert can be closed as false positive or needs to be moved to a human being for a detailed investigation. For further guidance, please refer to the Future of AML/CFT Technology section.
Rough Diamonds Trade Controls Sanctions Program	Established by the Clean Diamond Trade Act (CDTA), IEEPA, NEA, UNPA and Executive Order 13312 – Implementing the Clean Diamond Trade Act, OFAC's Rough Diamond Trade Controls Sanctions Program prohibits the import and export of rough diamonds from countries that do not participate in the Kimberley Process Certification Scheme (KPCS) and prohibits any transaction that evades or attempts to evade these prohibitions on or after July 30, 2003. The Rough Diamond Trade Control Sanctions Program is implemented under 31 C.F.R. Part 592 – Rough Diamonds Control Regulations. For further guidance, please refer to the Rough Diamond Trade Controls Sanctions Program section.
Safe Harbor	"Safe Harbor" is protection from civil liability to any financial institution, director, officer or employee that makes a suspicious transaction report under any federal, state or local law. A "bank, and any director, officer, employee or agent of any bank, that makes a voluntary disclosure of any possible violation of law or regulation to a government agency with jurisdiction, including a disclosure made jointly with another institution involved in the same transaction, shall be protected" under the Safe Harbor provision. For further guidance, please see the Safe Harbor section.
Sanctions	The U.S. uses the term "sanctions" to describe economic and trade sanctions against certain individuals, entities and foreign government agencies and countries whose interests are considered to be at odds with U.S. policy. These "sanctions" are administered by the Office of Foreign Assets Control (OFAC). Some organisations, such as FATF also use the term to describe penalties for non-compliance with AML/CFT laws and regulations (e.g., civil, criminal, administrative). For further guidance on economic and trade sanctions, please refer to the Office of Foreign Assets Control and International Sanctions Program section. For further guidance on penalties for noncompliance, please refer to the Enforcement Actions section.

Sectoral Sanctions Identifications List (SSI List)	The "Sectoral Sanctions Identifications List (SSI List)" includes designated persons operating in financial and energy sectors of the Russian economy who are subject to sanctions by OFAC. For further guidance, please refer to the OFAC Sanctions Listings section.
Senior foreign political figure	See "Politically exposed person."
Shell company	A "shell company" generally refers to an entity without a physical presence in any country. For further guidance, please refer to the Business Entities: Shell Companies and Private Investment Companies section.
Signature or other authority	"Signature or other authority" is defined as "the authority of an individual (alone or in conjunction with another individual) to control the disposition of assets held in a foreign financial account by direct communication (whether in writing or otherwise) to the bank or other financial institution that maintains the financial account." For further guidance, please refer to the Report of Foreign Bank and Financial Accounts section.
Simplified due diligence	Simplified due diligence is a term used in some jurisdictions (e.g., Europe) to describe abbreviated due diligence requirements that may be applied to select categories of customers. Simplified Due Diligence is not a principle that has specific meaning in the U.S., but it may be included in the KYC policy and procedures of foreign bank organisations (FBOs) doing business in the United States. For further guidance, please refer to the KYC Basics section.
Skimming	"Skimming" is a method of fraudulently obtaining and storing credit/debit card information through the use of computers or specialised card readers in order to re-encode the account information onto the magnetic strips of blank credit/debit cards, which then can be used to make purchases. For further guidance, please refer to the Identity Theft and Identity Theft Prevention Program section.
Smurfing	"Smurfing" is the attempt to evade CTR filing requirements and/or detection by conducting numerous transactions at different locations of either the same institution or different institutions. For further guidance on smurfing, please see the CTR Evasion section.
Special due diligence (SDD)	In the United States, special due diligence generally refers to due diligence prescribed by AML/CFT laws and regulations for select high-risk customers (e.g., foreign correspondents, private banking). SDD may include, but not be limited to, obtaining the following information as required by various sections of the USA PATRIOT Act: A Foreign Bank Certification, also known as a USA PATRIOT Act Certification, which requires foreign respondents to certify the following: • Physical presence/regulated affiliated status; • Prohibition of indirect use of correspondent accounts by foreign shell banks; and • Ownership status (for non-public institutions). For further guidance, please refer to the CDD vs. EDD & Other Due Diligence Requirements section.

Special Measures	Section 311 provides the U.S. Department of the Treasury broad authority to impose one or more of five Special Measures against foreign jurisdictions, foreign financial institutions (FFIs), classes of international transactions or types of accounts, if it determines that such jurisdictions, financial institutions, transactions or accounts are of primary money laundering concern. These Special Measures require a range of responses, from information requirements to outright prohibitions. They are as follows: • First Measure: Additional recordkeeping and reporting of certain financial transactions • Second Measure: The collection of information relating to beneficial ownership of accounts • Third Measure: The collection of information relating to certain payable-through accounts (PTAs) • Fourth Measure: The collection of information relating to certain correspondent accounts • Fifth Measure: The prohibition or imposition of conditions on opening or maintaining correspondent or payable-through accounts (PTAs) and notifying foreign respondents of applicable restrictions Section 311 is implemented for depository institutions under 31 C.F.R. 1010.650 – Special Measures under Section 311 of the USA PATRIOT Act and Law Enforcement Access to Foreign Bank Records. For further guidance, please refer to the USA PATRIOT Act - Analysis of Key Sections: Section 311- Special Measures section.
Special purpose vehicle (SPV)	A “special purpose vehicle (SPV),” also known as a special purpose entity (SPE), bankruptcy-remote entity, and orphan company, is a corporation, trust, partnership, or limited liability company that is created for a limited purpose, generally to isolate financial risk. An SPE may be owned by one or more other entities. For further guidance, please refer to the Business Entities: Shell Companies and Private Investment Companies section.
Specially Designated Nationals and Blocked Persons List (SDN List)	The “Specially Designated Nationals and Blocked Persons List (SDN List)” identifies individuals, groups and entities, such as terrorists and narcotics traffickers, designated under programs administered by the Office of Foreign Assets Control (OFAC) (e.g., Counter Terrorism Sanctions, Counter Narcotics Sanctions, Non-Proliferation Sanctions). For further guidance, please refer to the OFAC Sanctions Listings section.
Specified unlawful activity (SUA)	The United States lists hundreds of specified unlawful activities (SUAs) that are considered predicate crimes for money laundering, including, but not limited to, the following: • Racketeering activity (e.g., any act or threat involving murder, kidnapping, gambling, arson, robbery, bribery, extortion, dealing in obscene matter or dealing in a controlled substance or listed chemical as defined by the Controlled Substances Act), which is chargeable under state law and punishable by imprisonment for more than one year; • Terrorist financing; • Counterfeiting (e.g., currency, goods); • Fraud (e.g., securities fraud, wire fraud); • Slavery, trafficking in persons and alien smuggling; • Illegal arms sales (e.g., chemical weapons, nuclear material); and • Illegal gambling.

Standards of knowledge	When assessing whether an institution or its personnel are guilty of aiding and abetting money laundering or terrorist financing, the authorities consider, among other factors, the following "standards of knowledge": • Reckless Disregard – Careless disregard for legal or regulatory requirements and sound business practices • Wilful Blindness – Deliberate ignorance and failure to follow up in the face of information that suggests probable money laundering or illicit activity • Collective Knowledge – Aggregates/attributes the knowledge of employees to the employing company For further guidance, please refer to the Overview of AML/CFT Laws section.
Stored-Value Cards	"Stored-value cards," now known as prepaid cards, are funds or monetary value represented in digital electronic format and stored or capable of storage on electronic media in such a way as to be retrievable and transferable electronically. For further guidance, please refer to the sections: Prepaid Access and Stored-Value and Providers and Sellers of Prepaid Access.
Strict liability	As it relates to OFAC, "strict liability" means that the offender is liable even if it did not know that it violated a sanctions program. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.
Stripping	"Stripping" is when information is removed from payment information in order to prevent the funds transfer from being blocked or rejected when being screened for possible sanctions violations. For further guidance, please refer to the Office of Foreign Assets Control and International Sanctions Programs section.
Structuring	"Structuring" is the attempt to evade CTR filing requirements by breaking transactions into smaller amounts, typically just below the reportable threshold (e.g., US$9,999). For further guidance on structuring, please see the CTR Evasion section.

Substantial ownership	The Foreign Account Tax Compliance Act (FATCA) defines "substantial ownership" as:
	• "With respect to any corporation, any specified United States person which owns, directly or indirectly, more than 10 percent of the stock of such corporation (by vote or value),
	• With respect to any partnership, any specified United States person which owns, directly or indirectly, more than 10 percent of the profits interests or capital interests in such partnership, and
	• In the case of a trust:
	  ○ Any specified United States person treated as an owner of any portion of such trust under subpart E of part I of subchapter J of chapter 1, and
	  ○ To the extent provided by the Secretary in regulations or other guidance, any specified United States person which holds, directly or indirectly, more than 10 percent of the beneficial interests of such trust."
	For further guidance, please refer to the Foreign Account Tax Compliance Act.

Suspicious activity red flags	Suspicious activity red flags can be used to assist in identifying suspicious activity that may necessitate the filing of a SAR. For a list of examples of suspicious activity red flags, please refer to the Suspicious Activity Red Flags section.

Suspicious Activity Report (SAR)	A “Suspicious Activity Report (SAR),” is a report that documents suspicious or potentially suspicious activity (e.g., has no business purpose or apparent lawful purpose) attempted or conducted at or through a financial institution. For further guidance, please refer to the Suspicious Activity Reports section.
SWIFT	SWIFT stands for Society for Worldwide Interbank Financial Telecommunication. SWIFT is the infrastructure supporting both global correspondent banking and most domestic payment systems and Real-Time Gross Settlement (RTGS) networks involving over 11,000 financial institutions (e.g., banks, broker-dealers, investment managers) in more than 200 countries and territories. Participants also include corporate as well as market infrastructures (settlement and clearing organisations) in payments, securities, treasury and trade. Message types (MTs) are used to transmit financial information and instructions from one participating financial institution to another, also referred to as SWIFT FIN messages. Oversight is provided by central banks including the National Bank of Belgium, the Bank of England, the Bank of Japan and the U.S. Federal Reserve. For further guidance, please refer to the Cover Payments and SWIFT section.
Tax avoidance	Tax avoidance is the legal reduction or nonpayment of taxes. For further guidance, please refer to the Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act section.
Tax evasion	Tax evasion is the illegal reduction or nonpayment of taxes. For further guidance, please refer to the Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act section.
Tax fraud	Tax fraud is the intentional wrongdoing by the taxpayer with the specific purpose of evading taxes owed or believed to be owed and can result in both civil and criminal penalties. For further guidance, please refer to the Offshore Tax Evasion, Voluntary Tax Compliance Programs and Foreign Account Tax Compliance Act section.
Terrorism	“Terrorism” is often defined as an activity that involves a violent act or an act dangerous to human life, property or infrastructure that appears to be intended to: intimidate or coerce a civilian population; influence the policy of a government by intimidation or coercion; affect the conduct of a government by mass destruction, assassination, kidnapping or hostage taking. For further guidance, please refer to the Counter Terrorism Sanctions Program section.
Terrorist financing	“Terrorist financing” is a financial crime that uses funds to support the agenda, activities or cause of a terrorist organisation. The funds raised may be from legitimate sources, such as charitable organisations or donations from supporters, as well as criminal sources such as drug trade, weapons smuggling, fraud, kidnapping and extortion for illegal activities.
Third-party payment processors (TPPPs)	Third-party payment processors (TPPPs) provide payment-processing services to third-party business entities (e.g., banks, merchants). TPPPs include, but are not limited to, the following: • Funds transfer • Check clearing • Debit/credit cards processing • Automated teller machine (ATM) networks • Remote deposit capture (RDC) services • Automated clearing house (ACH) networks

	Financial institutions often utilise TPPPs as vendors to assist with their payment processing needs. Additionally, TPPPs may be customers of financial institutions that may use their accounts to conduct payment processing for their merchants' clients. For additional guidance, please refer to the Third-Party Payment Processors section.
Third-party transaction	A "third-party transaction" is defined as a transfer of funds to/from the account holder to/from an individual/entity that is different than the customer/account holder. It includes all types of transactions (e.g., wires, checks), regardless of direction (i.e., incoming, outgoing). "Third party" distinguishes the recipient/sender of the funds from the account holder. The individual/entity also can be a customer of the same financial institution, although the risk is greater when the individual/entity is not a customer of the financial institution, as the latter was not subject to the same customer acceptance procedures. For further guidance, please refer to the sections: Product/Service Risk Assessment and Know Your Customer's Customer.
Trade-Based Money Laundering (TBML)	"Trade-based money laundering (TBML)" refers to the process of disguising the proceeds of illegal activity and moving value through the use of trade transactions so that they appear to come from legitimate sources or activities. Examples of TBML include the Black Market Peso Exchange (BMPE) and Reintegro schemes. For further guidance, please refer to the sections: Trade Finance Activities and Informal Value Transfer Systems.
Trade Finance	"Trade finance" generally refers to the financial component of trade transactions executed between exporters from one country and importers from another country, which typically involves short-term financing to facilitate the import and export of goods. For further guidance, please refer to the Trade Finance Activities section.
Transaction monitoring system/software	Several different types of suspicious transaction monitoring software are currently available. Some of the most commonly used AML/CFT technologies include rules-based software; profiling software; and artificial intelligence (AI) software or predictive analysis. Some of the more sophisticated or mature vendors in the industry have incorporated all three types of software into their solutions. Rules-based software flags any transaction or activity that violates a business rule. These rules are typically modelled to detect known money laundering red flags as published by regulatory agencies and trade associations (e.g., Federal Financial Institutions Examination Council [FFIEC], Joint Money Laundering Steering Group [JMLSG], Wolfsberg Group of Banks, Financial Action Task Force [FATF]). Rules-based software can be customised over time through the addition and/or refinement of rules. Rules-based software is suitable for known patterns of suspicious activity (e.g., structuring, flow-through of funds). Profiling software uses a combination of predictive profiles developed from a customer's identification and customer due diligence (CDD)/enhanced due diligence (EDD) information, as well as historical transactions. Profiling software is designed to flag transactions that are out of profile by utilising means, standard deviations and thresholds. Profiling software is suitable for both known and unknown patterns of suspicious activity. In addition to leveraging the features of profiling software, artificial intelligence based systems take into account more upstream applications like KYC to make the process of data collection from multiple sources and systems "more intelligent." Additionally, these systems leverage prior knowledge and rules to link related entities, learn by remembering investigation results and applying them to the current dataset to determine whether an alert should be generated and if it does in fact need to be generated, determine the severity of the alert. For additional guidance please refer to the Monitoring, Investigating and Filing of Suspicious Activity Reports (SARs) section.

Transnational criminal organisation (TCO)	OFAC defines TCOs as a group of persons that "engages in an ongoing pattern of serious criminal activity involving the jurisdictions of at least two foreign states; and threatens the national security, foreign policy or economy of the United States." For further guidance please refer to the OFAC Sanctions Listings: Transnational Criminal Organisations Sanctions Program and Drug Trafficking sections.
Transnational criminal organisation (TCO) Sanctions Program	Established by IEEPA, NEA and Executive Order 13581 – Blocking Property of Transnational Criminal Organisations (2011), OFAC's Transnational Criminal Organisations (TCO) Sanctions Program blocks the property and property interests of individuals and entities determined to be significant transnational criminal organisations or to have provided material support for, or to be owned or controlled by, or to have acted on behalf of such organisations. The Executive Order states that the activities of the listed transnational criminal organisations threaten the stability of international political and economic systems and constitute an unusual and extraordinary threat to the national security, foreign policy and economic interests of the United States. TCO Sanctions are implemented under 31 C.F.R. Part 590 – Transnational Criminal Organisations Sanctions Regulations. For further guidance, please refer to the OFAC Sanctions Listings: Transnational Criminal Organisations Sanctions Program and Drug Trafficking sections.

Travel Rule	The Travel Rule refers to the requirement for financial institutions that participate in funds transfers of US$3,000 or more to pass along certain information about the funds transfer to the next financial institution involved in the funds transmittal.
	
	The requirements of the Travel Rule vary depending on the role the financial institution plays in the funds transfer (e.g., originating institution, intermediary institution).
	
	The originating financial institution must forward the following information to the next financial institution in the chain:
	
	• The name of the originator
	• The account number of the originator, if used
	• The address of the originator
	• The amount of the payment order
	• The execution date of the payment order
	• The identity of the recipient's financial institution
	• As many of the following items as are received with the payment order:
	  ○ Name of the recipient
	  ○ Address of the recipient
	  ○ Account number of the recipient
	  ○ Any other specific identifier of the recipient
	• Either the name and address or the numerical identifier of the originator's financial institution
	
	A financial institution serving as an intermediary must pass on the required information listed above, if received from the preceding financial institution, to the next financial institution in the chain. The intermediary, however, has no obligation to obtain information not provided by the preceding financial institution.
	
	For further guidance, please refer to the Funds Transfer Recordkeeping Requirement and the Travel Rule section.

Trust accounts	The FFIEC BSA/AML Examination Manual defines “trust accounts” as legal arrangements in which one party (the trustor or grantor) transfers ownership of assets to a person or financial institution (the trustee) to be held or used for the benefit of others. These legal arrangements include: • Broad categories of court-supervised accounts (e.g., executorships and guardianships) • Personal trusts (e.g., living trusts, trusts established under a will, charitable trusts) • Corporate trusts (e.g., bond trusteeships) For further guidance, please refer to the Trust and Asset Management Services section.
U.S. dollar drafts	A U.S. dollar draft is a bank draft or check denominated in U.S. dollars, which is offered by foreign financial institutions (FFIs) and drawn on a U.S. correspondent account of the FFI. For further guidance, please refer to the U.S. Dollar Drafts section.
U.S. Munitions List (USML)	The U.S. Munitions List (USML) is administered by the Directorate of Defense Trade Controls, Bureau of Political-Military Affairs within the State Department pursuant to the Arms Export Control Act of 1976 (AECA) and the International Traffic in Arms Regulations (ITAR), and is used to control the export of defence articles, services and related technologies. Examples of items on the USML list include, but are not limited to, the following: • Firearms, such as close assault weapons, combat shotguns, guns over calibre 0.50 and flamethrowers • Launch vehicles, guided missiles, ballistic missiles, rockets, torpedoes, bombs and mines • Explosives, propellants and incendiary agents • Armored combat ground vehicles, special naval equipment, fighter bombers, attack helicopters, unmanned aerial vehicles (UAV) • Military training equipment • Personal protective equipment, such as body armour, helmets and select face paints • Military electronics, such as radios and radar systems For further guidance, please refer to the Non-Proliferation Sanctions Program, OFAC Licensing and Trade Finance Activities sections.
USA PATRIOT Act	Following the terrorist activity of September 11, 2001, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act was signed into law by President George W. Bush on October 26, 2001, significantly amending the Bank Secrecy Act (BSA). The USA PATRIOT Act has 10 titles: • Title I: Enhancing Domestic Security Against Terrorism • Title II: Enhanced Surveillance Procedures • Title III: International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001 • Title IV: Protecting the Border • Title V: Removing Obstacles to Investigating Terrorism • Title VI: Providing for Victims of Terrorism, Public Safety Officers and Their Families • Title VII: Increased Information Sharing for Critical Infrastructure Protection • Title VIII: Strengthening the Criminal Laws Against Terrorism • Title IX: Improved Intelligence • Title X: Miscellaneous Title III, the International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001, deals with money laundering and terrorist financing. Title III made significant changes to U.S. money laundering regulations, imposed enhanced requirements for AML Programs, and significantly expanded the scope of coverage to nonbank financial institutions (NBFIs). It

	requires financial institutions to establish AML Programs that include policies, procedures and controls, designation of a compliance officer, training and independent review. In addition, it requires certain financial institutions to have customer identification procedures for new accounts and enhanced due diligence (EDD) for correspondent and private banking accounts maintained by non-U.S. persons. The USA PATRIOT Act Improvement and Reauthorisation Act of 2005 made permanent certain temporary provisions of the USA PATRIOT Act; increased civil and criminal penalties for terrorist financing and terrorist attacks on mass transportation systems and seaports (e.g., enhancements to death penalty procedures); included laundering through informal value transfer systems (IVTSs) (e.g., hawalas) within the federal definition of money laundering; implemented safeguards to protect civil liberties related to various provisions of the USA PATRIOT Act (e.g., National Security Letters [NSLs], roving surveillance orders, access to business records); and imposed additional measures to combat the trafficking of methamphetamine. For further guidance, please refer to the USA Patriot Act section.
Virtual Currency	"Virtual currency," as defined by FinCEN, is "a medium of exchange that operates like currency in some environments, but does not have all the attributes of real or fiat currency." "Fiat currency" is another term used to describe "real" currency that is government-issued. For further guidance, please refer to the Virtual Currency Systems and Participants section.
Weapons of mass destruction (WMDs)	Under Title 18 U.S. Code 2332a, a "weapon of mass destruction" (WMD) is defined as: • Any destructive device (e.g., explosive, incendiary or poison gas bomb, grenade, rocket, missile, mine); • Any weapon that is designed or intended to cause death or serious bodily injury through the release, dissemination or impact of toxic or poisonous chemicals or their precursors; • Any weapon involving a biological agent, toxin or vector (e.g., living organism or molecule capable of carrying a biological agent or toxin to a host); or • Any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. Nuclear, biological, chemical or radiological WMDs and their delivery systems (e.g., any apparatus, equipment, device, or means of delivery specifically designed to deliver or disseminate a biological agent, toxin or vector) are subject to sanctions by OFAC's Non-Proliferation Sanctions Program. For further guidance, please refer to the Non-Proliferation Sanctions Program section.
White list	A "white list" is a compilation of names that a financial institution has decided to exclude from sanctions screening. The white list typically evolves from false hits that the financial institution has experienced – names that are exact or partial matches to names on a sanctions list, but which the financial institution, through its due diligence, has determined are not true matches. For further guidance, please refer to the OFAC Basics and Customer and Transaction List Screening sections.

Acronyms

ABA	American Bankers Association
ACH	Automated Clearing House
ACS	Armored Car Service
ACSSS	American Council of State Savings Supervisors
AECA	Arms Export Control Act of 1976
AEDPA	Antiterrorism and Effective Death Penalty Act of 1996
AFMLS	Asset Forfeiture and Money Laundering Section, DOJ, Criminal Division
AI	Artificial Intelligence
AIE	Automatic Information Exchange
AIS	Automated Indicator Sharing
AMEX/ASE	American Stock Exchange
AML	Anti-Money Laundering
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
AMLID	Anti-Money Laundering International Database
ANF	Al-Nusrah Front
ANPR	Advanced Notice of Proposed Rulemaking
AOA	U.S. Administration on Aging
APA	U.S. Administrative Procedures Act
APG	Asia/Pacific Group on Money Laundering
APO	Army Post Office
APT	Advanced Persistent Threat
ATF	U.S. Bureau of Alcohol Tobacco and Firearms
ATM	Automated Teller Machine
ATP	Authorised Third Party
ATEST	Alliance to End Slavery and Trafficking
AUSA	Assistant U.S. Attorneys
BASCAP	Business Action to Stop Counterfeiting and Piracy
BCBS	Basel Committee on Banking Supervision

BCSC	National Bulk Cash Smuggling Center
BEC	Business Email Compromise
BEPS	Base Erosion and Profit Shifting
BHC	Bank Holding Company
BI	Business Intelligence
BIC	Bank Identifier Code
BIS	Bureau of Industry and Security
BIS	Bank for International Settlements
BJA	Bureau of Justice Assistance
BMPE	Black Market Peso Exchange
BNI	Bearer Negotiable Instrument
BOE	Bank of England
BPI	Bribe Payers Index
BPI-PA	Blocked Pending Investigation, Patriot Act
BSA	Bank Secrecy Act
BSAAG	Bank Secrecy Act Advisory Group
BXA	Bureau of Export Administration (now called Bureau of Industry and Security)
C & D	Cease and Desist
CBETF	Cross-Border Electronic Transmittal of Funds
CBI	Central Bank of Iran
CBP	Customs and Border Protection
CBT	Computer-Based Training
CBW	Chemical and Biological Weapons Control and Warfare Elimination Act of 1991
CCIPS	Computer Crime and Intellectual Property Section
CCL	The Commerce Control List
CCS	Commercial Crime Services
CDD	Customer Due Diligence
CDO	Chief Data Officer
CDTA	Clean Diamond Trade Act

CEA	Commodity Exchange Act
CFATF	Caribbean Financial Action Task Force
CFPB	Consumer Financial Protection Bureau
CFR	Code of Federal Regulations
CFTC	Commodity Futures Trading Commission
CIA	Central Intelligence Agency
CIP	Customer Identification Program
CISA	Cybersecurity Act of 2015 (aka Cybersecurity Sharing Act)
CISADA	Comprehensive Iran Sanctions, Accountability and Divestment Act
CMIR	Report of International Transportation of Currency or Monetary Instruments
CMP	Civil Money Penalty
COE	Council of Europe
CPA	Certified Public Accountant
CPD	Controlled Prescription Drugs
CPI	Corruption Perceptions Index
CPO	Commodity Pool Operator
CPRC	Consumer Payments Research Center (Federal Reserve Bank of Boston)
CRF	Criminal Referral Form
CRHA	Countering Russian Hostilities Act of 2017
CRR	Customer Risk Rating
CRS	Common Reporting Standard
CSA	Controlled Substances Act
CSBS	Conference of State Bank Supervisors
CSF	Cybersecurity Framework
CSV	Comma-Separated Values
CTA	Commodity Trading Adviser
CTR	Currency Transaction Report
CTS	Counterterrorism Section, Criminal Division
CTSC	California Transparency in Supply Chains Act

DBA	Doing Business As
DDA	Demand Deposit Account
DEA	Drug Enforcement Administration
DFAT	Australian Department of Foreign Affairs and Trade
DFS	New York State Department of Financial Services
DHS	Department of Homeland Security
DLT	Distributed Ledger Technology
DNFBP	Designated Non-financial Businesses and Professions
DOB	Date of Birth
DoD	U.S. Department of Defense
DOE	U.S. Department of Energy
DOEP	Designation of Exempt Person
DOJ	U.S. Department of Justice
DOL	U.S. Department of Labor
DOS	U.S. Department of State
DOS	Denial of Service
DOT	U.S. Department of the Treasury
DPA	Deferred Prosecution Agreement
DPL	Denied Persons List
EAA	Export Administration Act of 1979
EAC	Email Account Compromise
EAG	Expanded Affiliated Groups
EAG	Eurasian Group on Combating Money Laundering and Financing of Terrorism
EAR	Export Administration Regulation
EC	European Commission
EC3	European Cybercrime Centre
ECTF	Electronic Crimes Task Force
ED	U.S. Department of Education
EDD	Enhanced Due Diligence

EEOC	U.S. Equal Employment Opportunity Commission
EFT	Electronic Funds Transfer
EFTA	Electronic Funds Transfer Act of 1978
EIA	U.S. Energy Information Administration
EIFFE	Elder Investment Fraud and Financial Exploitation
EIN	Employer Identification Number
EPN	Electronic Payments Network
EPRS	European Parliamentary Research Service
ERISA	Employee Retirement Income Security Act
ESAAMLG	Eastern and Southern Africa Anti-Money Laundering Group
ESW	Egmont Secure Web
ETL	Extract Transform and Load
EU	European Union
FAQ	Frequently Asked Question
FARA	Foreign Agents Registration Act of 1938
FAST	Fiduciary Abuse Specialist Team
FATCA	Foreign Account Tax Compliance Act
FATF	Financial Action Task Force
FBAR	Report of Foreign Bank and Financial Accounts
FBI	Federal Bureau of Investigation
FBO	Foreign Banking Organisation
FCA	UK Financial Conduct Authority
FCM	Futures Commission Merchant
FCOs	Foreign consular offices
FCPA	Foreign Corrupt Practices Act
FCPIA	Federal Civil Penalties Inflation Adjustment Act of 1990
FCS	FINRA Contact System
FDAP	Fixed, Determinable, Annual or Periodical
FDIC	Federal Deposit Insurance Corporation

FFETF	Financial Fraud Enforcement Task Force
FFI	Foreign Financial Institution
FFIEC	Federal Financial Institutions Examination Council
FGO	Foreign Gateway Operator
FHFA	Federal Housing Finance Agency
FHL Bank	Federal Home Loan Bank
FI	Financial Institution
FICO	Financing Corporation
FinCEN	Financial Crimes Enforcement Network
FINRA	Financial Industry Regulatory Authority
FIU	Financial Intelligence Unit
FLETC	Federal Law Enforcement Training Center
FPO	Fleet Post Office
FRB	Federal Reserve Board
FSAP	Financial Sector Assessment Program
FSAR	Financial Stability Assessment Reports
FSB	Financial Stability Board
FSE	Foreign Sanctions Evaders
FSF	Financial Stability Forum
FSRB	FATF-Style Regional Bodies
FTC	Federal Trade Commission
FTO	Foreign Terrorist Organisation
FTZ	Foreign Trade Zones
GAESA	Grupo de Administración Empresarial
GAFISUD	Financial Action Task Force of South America Against Money Laundering
GAO	Government Accountability Office
GCB	Global Corruption Barometer
GDP	Gross Domestic Product

GHRAVITY E.O.	Blocking the Property and Suspending Entry into the United States of Certain Persons with Respect to Grave Human Rights Abuses by the Governments of Iran and Syria via Information Technology
GIABA	Groupe Inter-Gouvernemental D'action Contre Le Blanchiment En Afrique (Inter Governmental Action Group Against Money Laundering in West Africa)
GIFCS	Group of International Finance Centre Supervisors
GIIN	Global Intermediary Identification Number
GLBA	Graham-Leach-Bliley Act
GO	Gateway Operator
GPR cards	General purpose reloadable cards
GTFP	The Global Trade Finance Program
GSE	Government-sponsored enterprise
GTO	Geographic Targeting Order
HEAT	Health Care Fraud Prevention and Enforcement Action Team
HERO	Human Exploitation Rescue Operations Act of 2015
HEU	Highly Enriched Uranium
HHS	Department of Health and Human Services
HIDTA	High Intensity Drug Trafficking Area
HIFCA	High Intensity Financial Crime Area
HIFPA	Hizballah International Financing Prevention Act of 2015
HKMA	Hong Kong Monetary Authority
HMT	Her Majesty's Treasury
HOSSPs	Hawalas and Other Similar Service Providers
IAIS	International Association of Insurance Supervisors
IAT	International Automated Clearing House Transactions
IB	Introducing Broker
IBC	International Business Corporation
IBRD	International Bank for Reconstruction and Development
IC3	Internet Crime Complaint Center
ICC	International Chamber of Commerce
ICE	Immigration and Customs Enforcement

ICIJ	International Consortium of Investigative Journalists
ICRG	International Co-operation Review Group
ICSID	International Centre for Settlement of Investment Disputes
IDA	International Development Association
IEEPA	International Emergency Economic Powers Act
IFC	International Finance Corporation
IFCA	Iran Freedom and Counter-Proliferation Act
IFSR	Iranian Financial Sanctions Regulations
IEEPA	International Emergency Economic Powers Act
IGRA	Indian Gaming Regulatory Act of 1998
ILO	International Labour Office
IMF	International Monetary Fund
IMO	International Organisation for Immigration
INA	Immigration and Nationality Act
INCSR	International Narcotics Control Strategy Report
INL	Bureau of International Narcotics and Law Enforcement Affairs
INTERPOL	International Police Organisation
IOLTA	Interest on Lawyers' Trust Account
IOSCO	International Organisation of Securities Commissions
IoT	Internet of Things
IPT	Investor Protection Trust
IRBA	Independent Regulatory Board for Auditors
IRGC	Islamic Revolutionary Guard Corps
IRS	Internal Revenue Service
IRS-CI	Internal Revenue Service Criminal Investigation
IRS-SBSE	Internal Revenue Service – Small Business and Self-Employed Division
IRS-TEGE	Internal Revenue Service – Tax Exempt and Government Entities Division
ISA	Iran Sanctions Act of 1996
ISDCA	International Security and Development Cooperation Act of 1985

ISO	Independent Sales Organisation
IT	Information Technology
ITAR	International Traffic In Arms Regulations
ITPP	Identity Theft Prevention Program
ITR	Iranian Transaction Regulations
ITRSHRA	Iran Threat Reduction and Syria Human Rights Act of 2012
ITSR	Iranian Transactions and Sanctions Regulations
IVTS	Informal Value Transfer System
JADE	To Lantos Block Burmese Jade Act of 2008 (Juntas' Anti-Democratic Efforts)
JCPOA	Joint Comprehensive Plan of Action
JFIU	Joint Financial Intelligence Unit (Hong Kong)
JMLSG	Joint Money Laundering Steering Group
JOBS Act	Jumpstart Our Business Startups Act of 2012
JVTA	Justice for Victims of Trafficking Act
KARA	Kleptocracy Asset Recovery Rewards Act
KFR	Kidnapping for ransom
KPCS	Kimberley Process Certification Scheme
KRI	Key Risk Indicator
KYC	Know Your Customer
KYCC	Know Your Customer's Customer
LC	Letter of Credit
LE	Legal Entity
LLC	Limited Liability Company
LOB	Line of Business
LSSP	Lost and Stolen Securities Program
MAS	Monetary Authority of Singapore
MER	Mutual Evaluation Report
MF	Mossack Fonseca
MI	Management Information

MIGA	Multilateral Investment Guarantee Agency
ML	Money Laundering
MLCA	Money Laundering Control Act of 1986
MLSA	Money Laundering Suppression Act of 1994
MLTA	U.S. Money Laundering Threat Assessment
MMDA	Money Market Deposit Account
MONEYVAL	The Council of Europe Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (Formerly Pc-R-Ev)
MOU	Memorandum of Understanding
MSB	Money Services Business
MSRB	Municipal Securities Rulemaking Board
MT	Message Type
MTL	Multiple Transaction Logs
MTRA	Money Transmitter Regulators Association
MVTS	Money or Value Transfer Services
NACHA	The Electronic Payments Association (formerly National Automated Clearing House Association)
NAIC	National Association of Insurance Commissioners
NAICS	North American Industry Classification System
NAMSDL	National Alliance for Model State Drug Laws
NAPSA	National Adult Protective Services Association
NARCC	North American Regional Clearing Center
NASAA	North American Securities Administrators Association
NASCUS	National Association of State Credit Union Supervisors
NASD	National Association of Securities Dealers
NASDAQ	National Association of Securities Dealers Automated Quotations
NBFI	Nonbank Financial Institution
NBPCA	Network Branded Prepaid Card Association
NCCIC	National Cybersecurity Communications Integration Center
NCCT	Non-Cooperative Countries and Territories

NCEA	National Center on Elder Abuse
NCMEC	National Center for Missing and Exploited Children
NCPEA	National Committee for the Prevention of Elder Abuse
NCPG	National Council on Problem Gambling
NCTC	National Counterterrorism Center
NCUA	National Credit Union Administration
NDAA	National Defense Authorisation Act
NDIP	Nondeposit Investment Product
NDO	New Disclosure Opportunity
NDTA	National Drug Threat Assessment
NEA	National Emergencies Act
NFA	National Futures Association
NFC	Near field communication
NFFE	Nonfinancial Foreign Entities
NGA	National Geospatial – Intelligence Agency
NGO	Nongovernmental Organisation
NHTRC	National Human Trafficking Resource Center
NICCS	National Initiative for Cybersecurity Careers and Studies
NIGC	National Indian Gaming Commission
NIOC	National Iranian Oil Company
NIS	Nominee Incorporation Services
NIS	National Integrity System Assessments
NIST	National Institute of Standards and Technology
NKSPEA	North Korea Sanctions and Policy Enhancement Act of 2016
NMLRA	National Money Laundering Risk Assessment
NMLS	National Money Laundering Strategy
NNSA	National Nuclear Security Administration
NPI	Non-public Information
NPPS	New Payment Products and Services

NPRM	Notice of Proposed Rulemaking
NPWMD	Non-proliferation of Weapons of Mass Destruction
NRA	Non-resident Aliens
NS-ISA	Non-SDN Iranian Sanctions Act
NSL	National Security Letter
NS-PLC	Non-Specially Designated National Palestinian Legislative Council
NTFRA	National Terrorist Financing Risk Assessment
NVD	National Vulnerability Database
NYSE	New York Stock Exchange
NZP	New Zealand Police
OAS	Organisation of American States
OCC	Office of the Comptroller of the Currency
ODFI	Originating Depository Financial Institution
OEA	Office of Enforcement Analysis
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
OFC	Offshore Financial Center
OIA	Office of Intelligence and Analysis
OMG	Outlaw Motorcycle Gang
ONDCP	Office of National Drug Control Policy
ORS	Office of Refugee Settlement
OSFI	Office of the Superintendent of Financial Institutions
OTP	One Time Passwords
OTS	Office of Thrift Supervision
OVDP	Offshore Voluntary Disclosure Program
PEP	Politically Exposed Person
PFFI	Participating Foreign Financial Institution
PHI	Protected Health Information
PIC	Private Investment Company

PII	Personally Identifiable Information
PIN	Personal Identification Numbers
POB	Place of Birth
POC	Points of Contact
POS	Point of Sale
PROTECT Act	Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003
PTA	Payable-Through Account
PUPID	Payable Upon Proper Identification
QI	Qualified Intermediaries
RAS	Risk Appetite Statement
RBA	Reserve Bank of Australia
RBA	Risk-Based Approach
RCC	Remotely Created Check
RDC	Remote Deposit Capture
RDCFFI	Registered Deemed Compliant Foreign Financial Institution
RDFI	Receiving Depository Financial Institution
RICO	Racketeer Influenced and Corrupt Organisations Act of 1970
RMSB	Registration of Money Services Businesses
RMLO	Residential Mortgage Lender or Originator
RO	Responsible Officer
RPA	Robotic Process Automation
RTGC	Real Time Gross Settlement
SAR	Suspicious Activity Report
SDD	Special Due Diligence
SDGT	Specially Designated Global Terrorists
SDN	Specially Designated National
SDN List	Specially Designated Nationals and Blocked Persons List
SDNT	Specially Designated Narcotics Traffickers

SDNTK	Specially Designated Narcotics Traffickers – Kingpins
SDT	Specially Designated Terrorists
SEA	Securities Exchange Act of 1934
SEC	U.S. Securities and Exchange Commission
SIFMA	Securities Industry and Financial Markets Association
SLC	State Liaison Committee
SPE	Special Purpose Entity
SPV	Special Purpose Vehicle
SRO	Self-Regulatory Organisation
SSI	Sectoral Sanctions Identifications
SSN	Social Security Number
STR	Suspicious Transaction Report
SUA	Specified Unlawful Activities
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TAR	Terrorist Assets Report
TBML	Trade Based Money Laundering
TCO	Transnational Criminal Organisation
TCSP	Trust and Company Service Providers
TEA	Targeted Employment Area
TF	Terrorist Financing
TFFC	Office of Terrorist Financing and Financial Crimes
TFI	Office of Terrorism and Financial Intelligence
TFTP	Terrorist Finance Tracking Program
TI	Transparency International
TIC	Trade Information Center
TIN	Taxpayer Identification Number
TIP Report	Trafficking in Persons Report
TPPP	Third-Party Payment Processors
TPSP	Third-Party Service Provider

TRA	Iran Threat Reduction and Syria Human Rights Act of 2012 (aka ITRSHRA)
TSRA	Trade Sanctions Reform and Export Enhancement Act of 2000
TTU	Trade Transparency Units
TVPA	Trafficking Victims Protection Reauthorisation Act (aka Trafficking Victims Protection Act)
TWEA	Trading with the Enemy Act of 1917
UAV	Unmanned Aerial Vehicles
UIGEA	Unlawful Internet Gambling Enforcement Act Of 2006
UN	United Nations
UNODC	United Nations Office on Drugs and Crime
UNPA	United Nations Participation Act
UNSCR	United Nations Security Council Resolution
USAD	U.S. Attorney's Offices
USAID	U.S. Agency for International Development
USA PATRIOT Act	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act
USC	United States Code
USCIS	U.S. Customs and Immigration Services
USDA	U.S. Department of Agriculture
USML	U.S. Munitions List
USSS	United States Secret Service
VCPPS	Virtual Currency Payments Products and Services
VDP	Voluntary Disclosure Program
VTC	Voluntary Tax Compliance
WB	World Bank
WCO	World Customs Organisation
WMD	Weapons of Mass Destruction
WTO	World Trade Organisation

Useful Websites

Protiviti	www.protiviti.com
Protiviti's AML site	www.protiviti.com/AML
KnowledgeLeader	www.knowledgeleader.com
Pillsbury Winthrop Shaw Pittman LLP	www.pillsburylaw.com
American Bankers Association (ABA)	www.aba.com
American Gaming Association (AGA)	www.americangaming.org
American Stock Exchange (AMEX/ASE)	www.amex.com
Bank for International Settlements/Basel Committee on Banking Supervision (BIS)/(BCBS)	www.bis.org
Bureau of Industry and Security (BIS)	www.bis.doc.gov
Central Intelligence Agency (CIA)	www.cia.gov
Code of Federal Regulations (CFR)	https://www.ecfr.gov
Commodity Futures Trading Commission (CFTC)	www.cftc.gov
Consumer Financial Protection Bureau (CFPB)	www.consumerfinance.gov
Customs and Border Protection (CBP)	www.cbp.gov
Department of Defense (DoD)	www.defense.gov
Department of Health and Human Services (HHS)	www.hhs.gov
Department of Homeland Security (DHS)	www.dhs.gov
Department of Justice (DOJ)	www.usdoj.gov
Department of State (DOS)	www.state.gov
Department of the Treasury (DOT)	www.treas.gov
Egmont Group of Financial Intelligence Units	www.egmontgroup.org
Drug Enforcement Administration	www.dea.gov/index.shtml

Electronic Payments Association (NACHA)	www.nacha.org
European Union	www.eurunion.org/eu
Federal Bureau of Investigation (FBI)	www.fbi.gov
Federal Deposit Insurance Corporation (FDIC)	www.fdic.gov
Federal Financial Institutions Examination Council (FFIEC)	www.ffiec.gov
Federal Reserve Bank of Boston Consumer Payments Research Center (CPRC)	www.bos.frb.org/economic/cprc
Federal Reserve Board (FRB)	www.federalreserve.gov
Financial Action Task Force (FATF)	www.fatf-gafi.org
Financial Crimes Enforcement Network (FinCEN)	www.fincen.gov
Financial Industry Regulatory Authority (FINRA)	www.finra.org
Financial Stability Board (FSB)	www.fsb.org
Government Accountability Office (GAO)	www.gao.gov
Homeland Security & Governmental Affairs: Permanent Subcommittee on Investigations	www.hsgac.senate.gov/subcommittees/investigations
Immigration and Customs Enforcement (ICE)	www.ice.gov
Internal Revenue Service (IRS)	www.irs.gov
Internal Revenue Service – Criminal Investigations (IRS-CI)	www.irs.gov/uac/Criminal-Investigation-(CI)-At-a-Glance
International Association of Insurance Supervisors (IAIS)	www.iaisweb.org
International Chamber of Commerce	www.iccwbo.org
International Criminal Police Organisation (INTERPOL)	www.interpol.int
International Finance Corporation	www.ifc.org/
International Labour Organisation	www.ilo.org
International Monetary Fund (IMF)	www.imf.org

International Organisation of Securities Commissions	www.iosco.org
International Trade Administration (ITA)	www.ita.doc.gov
Internet Crime Complaint Center (IC3)	www.ic3.gov/default.aspx
Joint Money Laundering Steering Group (JMSLG)	www.jmlsg.org.uk
Managed Funds Association (MFA)	www.mfainfo.org
Money Services Businesses (MSB)	www.fincen.gov/financial_institutions/msb
Money Transmitter Regulators Association (MTRA)	www.mtraweb.org
National Association of Insurance Commissioners (NAIC)	www.naic.org
National Bulk Cash Smuggling Center (BCSC)	www.ice.gov/bulk-cash-smuggling-center
National Credit Union Administration (NCUA)	www.ncua.gov
National Drug Threat Assessment (2016)	www.dea.gov/resource-center/2016 NDTA Summary.pdf
National Futures Association (NFA)	www.nfa.futures.org
National Geospatial-Intelligence Agency	www1.nga.mil
National Vulnerability Database	https://nvd.nist.gov
Network Branded Prepaid Card Association	www.nbpca.org
New York State Department of Financial Services (DFS)	www.dfs.ny.gov
New York Stock Exchange (NYSE)	www.nyse.com
Office of Foreign Assets Control (OFAC)	www.treas.gov/ofac
Office of National Drug Control Policy	www.whitehousedrugpolicy.gov
Office of Terrorism and Financial Intelligence (OTFI)	www.treasury.gov/about/organisational-structure/offices/Pages/Office-of-Terrorism-and-Financial-Intelligence.aspx
Office of the Comptroller of the Currency (OCC)	www.occ.treas.gov

Office of Trade Agreements Negotiations and Compliance (TANC)	tcc.export.gov
Organisation for Economic Co-operation and Development (OECD)	www.oecd.org
Polaris Project	www.polarisproject.org
Security Industry Association (SIA)	www.siaonline.org
Society for International Affairs	www.siaed.org
Society for Worldwide Interbank Financial Telecommunication (SWIFT)	www.swift.com
The Clearing House Association (TCH)	www.theclearinghouse.org
Trade Information Center	www.export.gov
Transparency International (TI)	www.transparency.org
Treasury Executive Office for Asset Forfeiture and Treasury Forfeiture Fund (TEOAF)	www.treasury.gov/about/organisational-structure/offices/Pages/The-Executive-Office-for-Asset-Forfeiture.aspx
United Nations (UN)	www.un.org
United Nations Office on Drugs and Crime	www.unodc.org
United States Citizenship and Immigration Services (USCIS)	www.uscis.gov
United States Code (USC)	www.gpo.gov/fdsys/search/submitcitation.action?publication=USCODE
U.S. Kimberley Process Authority (USKPA)	/www.uskpa.org
U.S. Securities and Exchange Commission (SEC)	www.sec.gov
Wolfsberg Group	www.wolfsberg-principles.com
World Bank (WB)	www.worldbank.org
World Trade Organisation	www.wto.org

ABOUT PROTIVITI

Protiviti is a global consulting firm that delivers deep expertise, objective insights, a tailored approach and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independently owned Member Firms provide consulting solutions in finance, technology, operations, data, analytics, governance, risk and internal audit to our clients through our network of more than 70 offices in over 20 countries.

We have served more than 60 percent of *Fortune* 1000® and 35 percent of *Fortune* Global 500® companies. We also work with smaller, growing companies, including those looking to go public, as well as with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Our Anti-Money Laundering Practice

Protiviti has a dedicated anti-money laundering (AML) team within its risk and compliance practice. The core members of this team are former regulators, former compliance officers, fraud and forensic specialists, and AML and sanctions technology experts who have hands-on experience working in and with financial institutions of all types. We draw on our experience to help compliance professionals, senior management and boards of directors, and internal audit departments address the challenges they face in meeting their AML responsibilities in a sustainable, efficient manner.

Protiviti provides a wide variety of consultative services designed to assist organisations in all aspects of AML/CFT (combatting financial terrorism) compliance, which includes the following areas.

Design and Implementation of AML/CFT Risk and Sanctions Risk Assessments

We assist clients with the design and implementation of AML/CFT and sanctions risk assessments that are foundational to effective compliance programs, including customer risk ratings, product/service risk ratings, geographic risk ratings, and line of business, enterprise and horizontal AML/CFT and sanctions risk assessments. We also work with our clients to ensure the proper alignment between their risk assessments and their overall AML/CFT and sanctions compliance programs and to introduce and leverage innovative technologies to improve efficiency.

Program Development and Remediation

We help clients with the development and/or enhancement of all aspects of their AML/CFT and sanctions compliance programs including, but not limited to, risk strategy and risk appetite statements, policies and procedures, job descriptions, staffing analyses, and board and management reporting.

AML/CFT and Sanctions System Selection, Implementation and Utilisation

We assist in the selection of appropriate technology tools to support ongoing AML/CFT and the Office of Foreign Assets Control (OFAC) monitoring. This includes vendor review and comparison, assessment and/or determination of current and future business and functional requirements, data lineage and validation, system optimisation, implementation support, pre- and post-implementation reviews, system validation and overall system project planning and management.

Money Laundering Reviews and Investigations

Using our proprietary work flow and data analytics tools, we assist clients in performing regulator-mandated look back reviews and other large-scale or focused-transaction reviews. As required, we identify applicable rules and scenarios for the customers and transactions in-scope, code the desired rules and scenarios, determine through quantitative and qualitative analysis the appropriate thresholds, and generate alerts, which our investigation specialists review to determine whether potentially suspicious activity is present. The documented reviews developed by our investigators leverage the financial institution's customer due diligence/enhanced due diligence, and open source and subscription data sources, as well as the investigators' knowledge of AML/CFT typologies. Our client and, as applicable, the regulators are provided complete documentation of the work performed.

DFS Part 504 Compliance

We can assist covered New York State-regulated financial institutions with all aspects of their Part 504 compliance efforts, from internal training and awareness, program development, program management, program documentation, model validation, data lineage and validation, control testing, and design of certification and sub-certification processes.

Independent Testing of AML Programs

We assist internal audit departments in developing comprehensive AML/CFT and sanctions audit programs, including risk assessments, risk and control matrices, audit work programs and training for audit teams. We also perform independent testing of existing AML programs on an outsourced or co-sourced basis and work with or on behalf of internal audit departments to validate actions taken by companies to address regulatory exceptions.

Focused Training

Customised and relevant AML/CFT training provides the basis for a successful AML/CFT and sanctions compliance program. We assist organisations with the development, implementation and delivery of AML/CFT and sanctions training that is customised to reflect a company's primary business activities, customer profile, current AML/CFT and sanctions knowledge base and internal procedures.

For additional information about Protiviti's AML services, please contact:

Carol M. Beaumier
Managing Director/Global AML Practice Leader
+1.212.603.8337
carol.beaumier@protiviti.com

THE AMERICAS

UNITED STATES

Alexandria
Atlanta
Baltimore
Boston
Charlotte
Chicago
Cincinnati
Cleveland
Dallas
Fort Lauderdale
Houston
Indianapolis
Kansas City
Los Angeles
Milwaukee
Minneapolis
New York
Orlando
Philadelphia
Phoenix
Pittsburgh
Portland
Richmond
Sacramento
Salt Lake City
San Francisco
San Jose
Seattle
Stamford
St. Louis
Tampa
Washington, D.C.
Winchester
Woodbridge

ARGENTINA*

Buenos Aires

BRAZIL*

Rio de Janeiro
Sao Paulo

CANADA

Kitchener-Waterloo
Toronto

CHILE*

Santiago

MEXICO*

Mexico City

PERU*

Lima

VENEZUELA*

Caracas

EUROPE MIDDLE EAST AFRICA

FRANCE

Paris

GERMANY

Frankfurt
Munich

ITALY

Milan
Rome
Turin

NETHERLANDS

Amsterdam

UNITED KINGDOM

London

BAHRAIN*

Manama

KUWAIT*

Kuwait City

OMAN*

Muscat

QATAR*

Doha

SAUDI ARABIA*

Riyadh

SOUTH AFRICA*

Johannesburg

UNITED ARAB EMIRATES*

Abu Dhabi
Dubai

ASIA-PACIFIC

CHINA

Beijing
Hong Kong
Shanghai
Shenzhen

JAPAN

Osaka
Tokyo

SINGAPORE

Singapore

INDIA*

Bangalore
Hyderabad
Kolkata
Mumbai
New Delhi

AUSTRALIA

Brisbane
Canberra
Melbourne
Sydney

*MEMBER FIRM

© 2017 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans. PRO-0817-101094
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®