protiviti®
Face the Future with Confidence

Managing Financial Crime Risk in a Rapidly Changing Environment

18 May 2020

Financial crime risk and vulnerability in the current economic climate

The current social and economic climate is a new frontier for financial institutions seeking to navigate challenges posed by deteriorating market conditions, consumer panic and the ever-watchful eye of industry regulators. Meanwhile bad actors who pose an ongoing threat are also discovering new channels of opportunity to disrupt the integrity of our financial system and abuse banks and other market participants through new COVID-19 fraud scams and laundering the proceeds of crime. Accordingly, institutions need to be aware of the evolving typologies and vigilant in taking proactive measures to prevent this abuse from occurring in order to maintain robust regulatory and reputational posture.

The new scarcity of certain products, such as protective clothing in hospitals, facemasks, hand sanitiser and similar goods, has brought a lot of illegitimate providers on the market seeking to exploit the situation. Already authorities have uncovered sophisticated scams with organised criminals attempting to pose as Government bodies, financial institutions, not-for-profit organisations and manufacturers of personal protective equipment (PPE), to deceive individuals and businesses into divulging personal details and authorise misdirected payments. We are entering uncharted territory and the crisis will be seen as an avenue by some for opportunistic fraud and increased laundering attempts or activity. At the same time, we don't know exactly what to expect from customers.

Examples of emerging COVID-19 related financial crime risks and vulnerabilities:

- Superannuation emergency drawdown of up to AUD$10,000 without satisfying customer verification for anti-money laundering and counter-terrorism financing (AML/CTF) purposes.
- Future superannuation voluntary contributions where cash repayments are made, or source of funds are difficult to verify.
- Reliance on online delivery channels and absence or reduction of face-to-face verification with simplified customer due diligence measures.
- Control deficiencies due to weak or immature processes and remote handovers.
- Delayed sign-offs due to technology constraints or unavailability of authorisers.
- Fast tracking of approvals due to hardship and increased pressure on call centres.
- Risk of transaction-service gatekeepers for struggling companies 'looking the other way'.
- People withdrawing hard currency in a state of panic about market volatility.
- Wire transfers declining in volume, balancing out the surge in cash withdrawals, online banking and cryptocurrency-related activity.
- Influx of people using virtual currency in a volume greater than ever encountered.

- Inexperienced customers turning to mobile apps for banking in hope that it is safer.
- Change in consumer behaviour resulting in AML officers finding it difficult to discriminate between legitimate activity and illegal transactions.
- Increase in use of 'money mules' (individuals being used by organised syndicates to launder money, who may be either complicit, or unaware of the underlying criminal activity).

Desperate times call for decisive measures

Financial institutions should closely scrutinise transfers linked to the procurement of medical products, government subsidies and charitable donations, and conduct deeper checks on large cash transactions as criminals seek to exploit the coronavirus pandemic. While scams are being exposed every day involving cybercrime, procurement fraud, investment fraud and government subsidy fraud, amongst others, much remains unknown about the emerging fraud and money laundering risk landscape. Therefore it is especially important that financial institutions evolve their ongoing customer due diligence programs, and report suspicious activity in a timely manner.

Australian regulators expect banks to employ dynamic risk assessment policies that respond to changes in a financial institution's risk environment, while maintaining robust business continuity protocols. Now is the time to take steps that will demonstrate to regulators that your institution recognises and has responded to the likelihood that it will increasingly encounter both internal and external fraud indicators in transactions and be the target of exploitation by criminals seeking to launder the proceeds of crime.

Identifying, managing and mitigating financial crime during a time of crisis

Detecting and mitigating external financial crime risk

Financial institutions need to remain vigilant of red flags related to potential impostor, investment and product scams, including government funding schemes, charities and cyber fraud related to the outbreak, while also operating with reduced resources. The red flags below identified by global financial intelligence units and regulators relate to COVID-19 vulnerabilities that institutions should consider, inclusive of a customer's overall financial activity and the institution's risk profile, to determine whether a transaction may be suspicious.

Identity scams

- Impersonation of government agencies such as the Australian National Centre for Disease Control, international organisations such as the World Health Organisation, or other healthcare organisations.
- Transactions where the payee name has a resemblance to, but not the same as, those of reputable charities.
- Payments to websites that are seemingly identical to legitimate charities and humanitarian relief organisations, often using URLs that end with a ".com" or a ".net", while most legitimate charities' websites end in ".org".

Vaccine and medical supply scams

- Fraudulent marketing of COVID-19-related supplies, such as PPE or potential vaccines.
- Offers to participate in unverified COVID-19 vaccine research and development crowd-funding schemes.
- Selling unapproved or misbranded supplies that make false COVID-19 related health claims. A scam website was recently identified fraudulently claiming to offer "World Health Organisation vaccine kits".
- Promotions making false claims that products or services of publicly traded companies can prevent, detect, or cure coronavirus, especially where the claims involve microcap stocks.
- Investments or trades that suggest urgency, obscurity, unverifiable credentials, testimonials, free gifts, or assert special insider knowledge, unusually large returns, guarantees or low-cost account opening.

Government support schemes

- Multiple emergency assistance payments to the same individual.
- Multiple emergency assistance payments or electronic funds transfers into the same bank account, particularly when the amounts of the payments are the same or very similar.
- Emergency assistance payments, when the accountholder is a retail business and the payee is an individual other than the accountholder.
- Opening of a new account with an emergency assistance payment, where the name of recipient is different from that of the potential accountholder.

- JobKeeper allowance subsidy fraud (e.g. 'pay out first, validate later').
  - Company receiving wage compensation but has no employees.
  - Company receiving wage compensation but does not pay the wages.
  - Company withdraws a large sum of cash immediately after a support payment is received.
  - 'Pop up' companies being set up quickly, possibly in order to fraudulently apply for government support (e.g. companies wanting to setup new bank accounts).

Other red flags and suspicious transactions

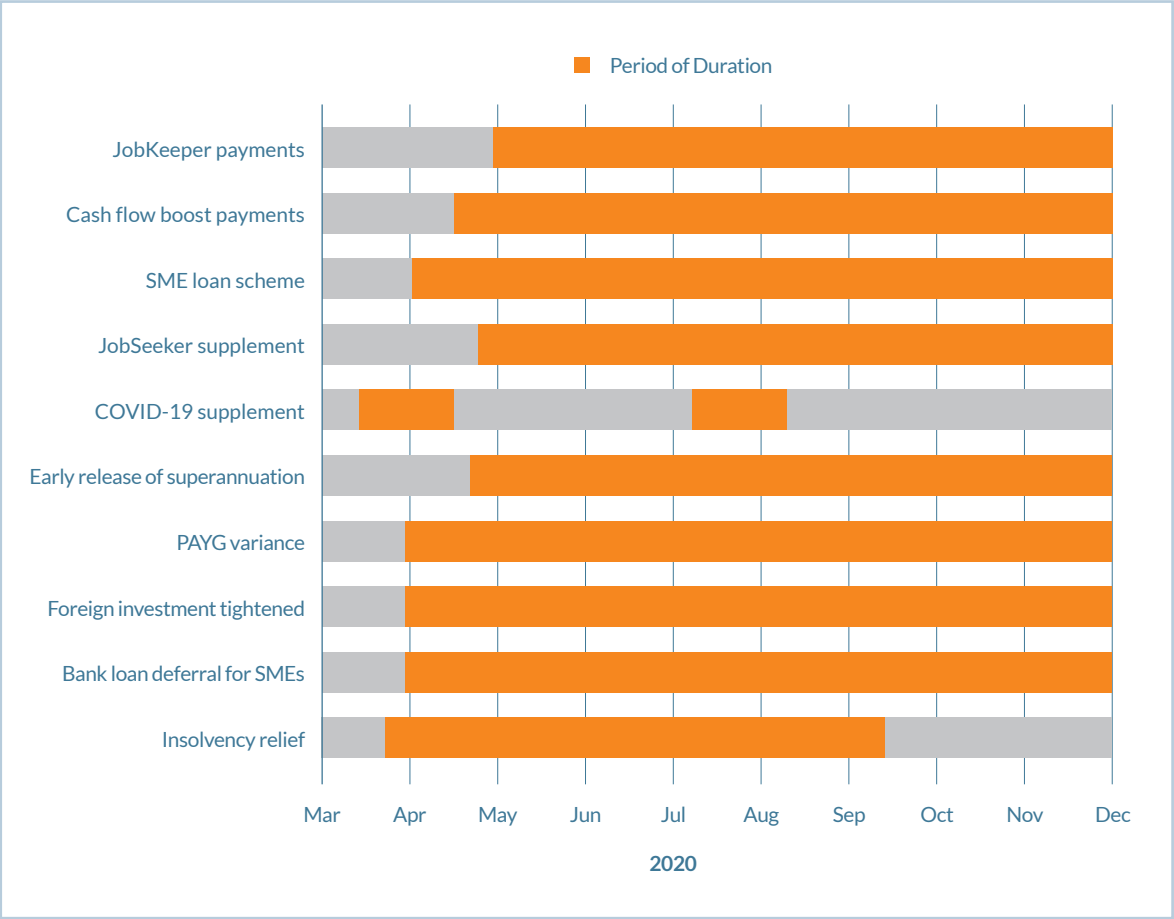
- The use of money transfer services for charitable donations.
- Price gauging of medical supplies and high-demand goods leading to potential offboarding or restriction of accounts.
- Crowdfunding platforms that have limited policies and procedures to protect customer funds and identification.
- 'Pop up' companies being set up quickly, possibly in order to launder and mix funds that are normally laundered by other entities, such as cash intensive businesses.
- Companies that are or should be struggling suddenly start receiving unexplained payments.
- Informal value transfer (e.g. manipulation of invoices, exploitation of correspondent accounts, trade diversion schemes, use of credit/debit cards by multiple individuals).

Implementation and enhancement of controls to mitigate COVID-19 financial crime risk

Below are some considerations for financial institutions to demonstrate best practice when detecting and preventing misconduct based on lessons learned from the 2008 financial crisis and recent guidance from global financial intelligence units and regulatory authorities regarding COVID-19. Financial institutions should consider these scenarios to reduce the risk of financial crime, misconduct and potential regulatory violations by employees, vendors and independent contractors during and after the COVID-19 pandemic.

- **Continuity of critical functions**
  Financial institutions will need to review resource allocation to adapt to the changing social and economic environment. The continuance of critical risk and compliance functions such as AML/CTF monitoring and sanctions screening is crucial to maintain integrity of the financial system and protect institutions from potential regulatory breach.
- **Supervision of internal systems**
  Ensure internal systems are closely monitored for potential vulnerabilities to financial crime risk intensified by reduced workforce, operational restructuring, social distancing and remote working measures.
- **Good governance practice**
  Where robust compliance or risk management standards are interrupted, ensure that consistent and centralised governance decisioning is maintained (e.g. involving compliance supervisory board committees). Decisions should be rationalised and documented, along with clear action plans to address deviation from normal operating standards.
- **Insider trading**
  The noise of increased market volatility can provide camouflage for securities fraud and market manipulation. Ensure surveillance measures are heightened and adaptative to the current volatile environment.
- **Keep compliance records**
  Where technology solutions are unable to support compliance obligations, such as voice-recording of trader communications, consider temporary alternatives such as contemporaneous records that are consistent with regulatory guidelines.
- **Monitor government funding schemes**
  Ensure that deposits and transfers involving funds from superannuation emergency drawdowns and 'JobKeeper' payments are scrutinised in accordance with imposed conditions and irregularities suggesting potential abuse. Employees should be familiar with terms, conditions and restrictions associated with such schemes.
- **Monitoring transactions**
  Consider production of new transaction monitoring scenarios, or fine-tuning existing rules, as customer spending habits change, and emergency assistance payments start to flow into customer accounts.
- **Preserve privacy and data security**
  Ensure remote working systems and virtual private networks are updated with security patches, multi-factor authentication is enabled, user access rights are effectively maintained, and employees are adequately educated on the principles of customer privacy and information security.

Australian COVID-19 Economic Measures Impacting Change in Customer Behaviour



Regulatory outreach and response as the pandemic paradigm shifts

Both the Financial Action Task Force (FATF) and the Australian Transaction Reports and Analysis Centre (AUSTRAC) have provided guidance to the financial services sector. FATF released a paper in early May 2020: *'COVID-19-related Money Laundering and Terrorist Financing, Risks and Policy Responses'.* The paper identifies challenges, good practices and policy responses to emerging money laundering and terrorism financing threats and vulnerabilities arising from the COVID-19 crisis.

AUSTRAC have released a number of public updates since mid March 2020 which are summarised below.

AUSTRAC COVID-19 updates

- **18 March 2020 — Coronavirus (COVID-19) — Working with our reporting entities**
  AUSTRAC communicated its commitment to work with reporting entities during disruptions presented by the COVID-19 crisis and to consider the circumstances of those entities with regards to meeting AML/CTF risk management and compliance obligations.
- **27 March 2020 — AUSTRAC supports ATO early release of super initiative**
  AUSTRAC indicated its intention to introduce a new AML/CTF rule that was implemented on 9 April 2020. The rule would make an exemption for superannuation funds making early release payments to its members and where the payment is approved by the Australian Tax Office (ATO), to perform simplified customer due diligence (CDD) to streamline the process.
- **27 March 2020 — AUSTRAC to accept Compliance Report 2019 until 30 June 2020**
  AUSTRAC announced that due to the exceptional circumstances, it would be accepting 2019 Compliance Reports from reporting entities until 30 June 2020 — a three-month extension to the 31 March 2020 deadline.
- **1 April 2020 — Fighting financial crime together — SMRs during the COVID-19 pandemic**
  AUSTRAC provided examples of identified areas of the financial system more vulnerable to criminal

exploitation during the COVID-19 pandemic and encouraged reporting entities to submit suspicious matter reports (SMRs) accordingly. The examples provided were as follows:

- Targeting of government assistance programs through fraudulent applications and phishing scams.
- Movement of large amounts of cash following the purchase or sale of illegal or stockpiled goods.
- Out of character purchases of precious metals and gold bullion.
- Exploitation of workers or trafficking of vulnerable persons in the community.
- An increase in the risk of online child exploitation following restrictions on travel.
- A rise in extremist views either against members of the community or the government.

- **1 April 2020 — How to comply with KYC requirements during the COVID-19 pandemic**
  AUSTRAC acknowledged the increase of AML/CTF compliance challenges during this period of social distancing, self-isolation and other disruptions to everyday business. This includes the reliance on face-to-face or documentation for the purposes of 'know-your-customer' (KYC) where electronic verification is not in use. With this recognition, these alternative customer identification procedures were provided.
  - Using alternative proof of identity processes (Rule 4.15.1).
  - Using electronic copies (scans or photographs) of reliable and independent documentation, in accordance with your AML/CTF program, to verify the identity of individual customers (Rule 4.9.3(3)) or companies (Rule 4.9.5(3)).
  - Relying on disclosure certificates to verify certain types of information about customers who are not individuals, where measures put in place by industry as part of their response to the COVID-19 pandemic mean that such information is not otherwise reasonably available from other sources (Rules 4.3.12, 4.4.16, 4.5.8, 4.6.8 and 4.7.8).

To support the verification process, AUSTRAC provided the following practical alternative processes to consider.

- Using a video call, such as Skype, Zoom or FaceTime to compare the physical identity of a customer with scanned or photographed copies of identification documents.
- Requiring a customer to provide a clear, front-view 'selfie' of themselves that can be compared with the scanned or photographed copies of identification documents.
- Telephoning the customer to ask questions about their identification, their reason for requesting a designated service or other questions that would assist in ascertaining whether the customer is who they claim to be.

- **17 April 2020 – New customer verification AML/CTF Rule to support early release of superannuation initiative**
  AUSTRAC introduced a new AML/CTF rule: *'Chapter 77, Exemption from the applicable customer identification procedure for the purposes of Schedule 13 to the Coronavirus Economic Response Package Omnibus Act 2020'.* The Rule declares that where the ATO has approved the payment, a superannuation fund will not have to carry out customer identification procedures described in section 32 of the AML/CTF Act, before making these payments to its members. The exemption is a time-limited measure that will apply for the period 15 April 2020 to 24 September 2020. Reporting entities will still have suspicious matter reporting and ongoing customer due diligence obligations relating to the provision of the relevant designated service.

Other Obligations

Additionally, AUSTRAC provided guidance on a number of key areas that would be impacted during the disrupted period caused by the COVID-19 pandemic. These include:

- **Ongoing Customer Due Diligence (OCDD)**
  Advice on the continuation of OCDD systems and controls, including the transaction monitoring program. Also provided acknowledgement that with simplified CDD for early superannuation release temporarily acceptable, that OCDD will therefore be more likely to identify suspicious transactions and for higher risk transactions enhanced CDD should be performed in accordance with their AML/CTF program.

- **Enhanced Customer Due Diligence (ECDD)** Guidance that reporting entities should follow processes described in the ECDD program, either before or after making payments with a higher level of money laundering and terrorism financing (ML/TF) risk.
- **Suspicious Matter Reports (SMRs)** A reminder to submit SMRs were there are reasonable grounds to suspect a transaction is related to financial crime or the customer is not who they claim to be.

  Additionally, reporting entities are requested to include the term "FASUPER2020" in any SMRs submitted in relation to the early release of superannuation.

Where to next as the uncertain economic landscape evolves?

With the pandemic now becoming a way of life for most, and with some countries tentatively looking to resurrect local economies from hibernation, financial institutions equally need to consider pre-emptive actions in response to these restorative challenges. The implementation of practical measures to address new threats, fluctuations in operational capacity, increased charitable activity, fiscal stimulus and government relief packages will promote control and resilience as the world slowly returns to a sense of normality.

- Coordinate available resources and engage key stakeholders to develop a response plan that communicates a clear pathway to emerge from COVID-19 conditions with a range of time-horizons and variable outcome scenarios (e.g. COVID-19 second wave or discovery of a vaccine).
- Ensure your risk assessment reflects the volatility of current conditions, adequately measures the potential impact of known vulnerabilities being exploited and articulates the level of control your organisation can reasonably expect to impose on those risks.
- Engage with regulatory supervisors, who are continuously monitoring the changing risk landscape and centrally positioned to provide appropriate guidance on new and emerging threats, impacts observed locally or globally, and prioritisation on risk-based AML/CTF countermeasures.
- Cooperation with regulatory supervisors and other industry participants to understand and monitor the evolving risk environment. As with the introduction of many new industry-wide changes or events, like the new payments platform (NPP), criminal behaviours and typologies soon begin to reveal themselves, providing valuable regulatory and risk management intelligence.
- Keep regulatory supervisors informed of any challenges faced with meeting regulatory requirements, to ensure the necessary guidance, support or exemptions can be provided individually or multilaterally.
- Adopt a risk-based approach where regulatory supervisors have communicated appropriate interim standards under current conditions. These may include simplified CDD for lower risk accounts on government relief payments, legitimate reasons for customers being unable to provide information for KYC refresh, acceptance of government-issued ID for customer verification or implementation of provisional interim measures (e.g. transaction limits) in lieu of typically acceptable documentation.
- Ensure your organisation explicitly understands requirements in the context of economic relief measures, such as those outlined above. Reporting entities still have obligations to report suspicious transactions and retain records regarding customers and transactions.
- Consider practical adjustments to electronic and digital payments to support customer activity while maintaining social distancing. Such measures might include increasing limits on point of sale purchasing, contactless payments or e-wallets and reducing domestic inter-bank transfer fees.

What should your organisation consider to minimise exposure?

Protiviti's Financial Crime Risk and Compliance solution specialise in helping financial institutions satisfy their regulatory obligations and reduce their financial crime exposure using a combination of AML/CTF and sanctions risk assessment, control enhancements and change capability to deliver effective operational risk and compliance frame-works. Our team of specialists assist organisations with protecting their brand and reputation by proactively advising on their vulnerability to financial crime, fraud and corruption, professional misconduct and other financial business risk issues.

Protiviti COVID-19 Financial Crime Health Check

The ongoing uncertainty of COVID-19 brings new challenges for financial institutions facing evolving threats posed by opportunistic perpetrators of financial crime. While the world adjusts to the changing economic landscape, your regulatory obligations remain unchanged. Don't let your guard down.

Protiviti can assist your organisation with assessing its exposure to COVID-19 related financial crime risk and provide pragmatic guidance to ensure you are not left with a post COVID-19 compliance hangover. Our team of Financial Crime Risk and Compliance experts can assist with identifying where potential weakness in your anti-money laundering framework exists and support you in designing and enhancing systems and controls that protect your organisation from unwanted criminal abuse, regulatory scrutiny or reputational damage.

We can offer a customised solution to provide a level of confidence that your organisation will not be an easy target. Protiviti can review your AML framework and provide actionable recommendations to establish robust measures that preserve your organisation's operational risk and compliance integrity.

To assist your institution respond to increased financial crime risk as a result of the COVID-19 crisis, we would seek to determine higher AML/CTF risk areas within the business, assess adequacy of the existing control environment and provide a robust roadmap for rapid enhancement, with focus on the following:

- Operating model optimisation to support shift towards remote workforce while maintaining defined risk management and compliance strategy, business continuity, performance metrics, regulatory reporting and horizon planning for return to work.
- Revision of financial crime compliance governance models to reflect changes to authorisation, sign-off and reporting procedures.
- Incorporating COVID-19 vulnerabilities into the ML/TF risk assessment to ensure your institution is considering the "unknown-unknown" threats, identifying higher risk elements (e.g. customer types, products offered, delivery channels) and to address change in your financial crime risk profile.
- Adaptation of KYC/CDD procedures to reflect shift from face-to-face, to online identification and verification procedures during social distancing measures.
- Production of new COVID-19 specific transaction monitoring scenarios, or fine-tuning existing rules, as customer spending habits change, and emergency assistance payments start to flow into customer accounts.
- Enhancements to alert investigation, case management procedures and reporting protocols for suspicious transactions in a remote working environment.
- Assessment of the AML/CTF and sanctions control framework and revisions to address new and emerging COVID-19 financial crime risk typologies.

Contacts

Mark Burgess
Managing Director, Risk & Compliance
+61.408.506.411
mark.burgess@protiviti.com.au

Kris Burrows
Head of Financial Crime, Risk & Compliance
+61.419.735.988
kris.burrows@protiviti.com.au