protiviti®
Face the Future with Confidence

Managing Financial Crime Risks in a Changing Economic Environment

U.S. Edition | June 2020

Financial Crime Risks in the Current Climate

The current economic and business climate is a new frontier for financial institutions seeking to navigate challenges posed by deteriorating market conditions, customer anxiety and the ever-watchful eyes of industry regulators. Concurrently, bad actors that pose an ongoing threat are also discovering new channels of opportunity to threaten the integrity of the financial system with new COVID-19 fraud scams and other illicit activities. Accordingly, financial institutions need to be aware of the evolving typologies and be vigilant in taking proactive measures to prevent this abuse from occurring and protect their organizations.

We have entered uncharted territory. The scarcity of certain products, such as personal protective equipment (PPE), disinfectants, hand sanitizers and similar goods, along with the understandable desire for medicines that will prevent or cure COVID-19, has attracted illegitimate providers seeking to exploit the situation. Already authorities have uncovered sophisticated scams by organized criminals attempting to pose as government bodies, financial institutions, nonprofit organizations and manufacturers of PPE and drugs to deceive individuals and businesses into divulging personal details and authorize misdirected payments. Huge sums of monies earmarked for businesses and individuals most impacted by the crisis, often dispersed quickly without optimal controls, also create massive opportunities for fraudsters. These threats come at the same time that financial institutions are attempting to address changing patterns in customer financial activity in response to the current environment, and personal circumstances.

Emerging Financial Crime Risks and Vulnerabilities

The following are examples of emerging financial crime risks and vulnerabilities triggered by the COVID-19 pandemic:

- Fraudulent applications for the Paycheck Protection Program (PPP) and other government-sponsored loan and assistance programs.
- Risk of gatekeepers "looking the other way" as they struggle to meet job demands in their work from home (WFH) environment
- An increase in cybercrime, made possible by weakened security defenses of WFH arrangements.
- Customers withdrawing hard currency in reaction to market volatility.
- Out-of-character purchases of precious metals, gold bullion or cryptocurrency.

- Inexperienced customers turning to mobile banking applications for convenience and personal safety reasons, but without adequate information security protections.
- Movements of large amounts of cash for the purchase or sale of illegal goods.
- Increase in use of "money mules" (individuals used by organized syndicates to launder money, who may be either complicit or unaware of the underlying criminal activity).
- Stepped up terrorist financing activity in the hope that it will go undetected because of other priorities.
- Changes in the supply chain and payment models for illicit drugs.

Critical Times Call for Decisive Measures

While U.S. regulators have acknowledged the challenges faced by financial crime compliance personnel forced to work from home, their empathy should not be interpreted as justification for laxity in the face of a dramatically changed landscape. The reality is that risks have changed, and these changes will require modifications to financial crime compliance programs, including modifying and reinforcing controls. These changes may include, but are not limited to:

- Updating financial crime risk assessments.
- Changes to customer onboarding requirements to compensate for the lack of face-to-face contact.
- Enhancements to transaction monitoring scenarios to capture new typologies.
- Revising scenario thresholds to reflect changes in customer activity.
- Employee training on newly identified risks.
- Greater use of data analytics and tools, such as contextual monitoring, to identify hidden underlying relationships.
- Enhanced quality assurance capabilities, such as natural language processing (NLP), to strengthen oversight of the work performed by remote teams.

Identifying, Detecting and Mitigating External Financial Crime Risks

Financial institutions need to remain vigilant in their efforts to identify and detect red flags related to potential imposter, investment and product scams, as well as schemes to defraud government funding and assistance programs, charities and other organizations serving as fronts for illicit activities and cyber fraud. They need to do this while also operating with reduced resources.

Global financial intelligence units (FIUs) and regulators have identified a number of COVID-19-related red flags that institutions should consider, inclusive of their customers' overall financial activity and the institutions own risk profile, to determine whether a transaction may be suspicious. Some red flags are discussed in detail below:

Identity scams

- Impersonation of government agencies such as the Centers for Disease Control and Prevention, international organizations like the World Health Organization (WHO) or other healthcare organizations.
- Transactions where the payee name has a resemblance to, but not the same as, that of a reputable charity.
- Payments to websites that are seemingly identical to legitimate charities and humanitarian relief organizations, often using URLs that end with .com or .net. (Most legitimate charities use website addresses that end with .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, and crowdfunding schemes.
- Selling unapproved or misbranded supplies that make false COVID-19-related health claims (e.g., a recently uncovered scam website was fraudulently claiming to offer WHO vaccine kits).
- Promotions of false claims that products or services of publicly traded companies can prevent, detect or cure coronavirus, especially where the claims involve microcap stocks.

- Goods offered by merchants that do not have an established corporate history and/or where the true business of the company is unclear.

Government support schemes

- Applications for government loans where supporting documentation is limited, cannot be reasonably validated using public databases and/or appears fraudulent.
- Requests for loan proceeds to be sent to a seemingly unconnected third party and/or to high-risk jurisdictions outside of the United States.
- Applications for assistance by multiple customers sharing an address or phone number.
- Applications for government-sponsored loans from out-of-area companies.
- An inordinate volume of government-sponsored loans made by a single or small group of loan officers within a financial institution.
- Multiple emergency assistance payments received by the same business or individual.
- Emergency assistance payments, where the accountholder is a retail business and the payee is an individual other than an authorized account party.

While U.S. regulators have acknowledged the challenges faced by financial crime compliance personnel forced to work from home, their empathy should not be interpreted as justification for laxity in the face of a dramatically changed landscape.

- Opening of a new account with an emergency assistance payment, and where the name of the recipient differs from the potential accountholder.

Other red flags and suspicious transactions

- The use of money transfer services for charitable donations.
- Crowdfunding platforms that have limited policies and procedures to protect customer funds and identification.
- Pop-up companies set up 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).
- Use of a customer's personal account for activity related to the sale of medical supplies, potentially indicating that the selling merchant is unregistered/unlicensed or conducting fraudulent medical transactions.

Implementation and Enhancement of Controls to Mitigate COVID-19 Financial Crime Risks

Below are some considerations for financial institutions to demonstrate best practices when detecting and preventing misconduct. These suggestions are based on lessons learned from the 2008 financial crisis and recent guidance from global FIUs 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.

- **Ensure 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 the integrity of the financial system and protect institutions from potential regulatory breach.
- **Foster good governance practice:** Where robust compliance or risk management standards are interrupted, it is important to ensure that consistent and centralized governance decisioning is maintained (e.g., involving compliance supervisory board committees). Decisions should be rationalized and documented, along with clear action plans to address any deviation from normal operating standards.

- **Enhance financial intelligence capabilities:** Engage with regulators and representatives of law enforcement, as well as other industry participants who are continuously monitoring the changing risk landscape and can offer insights on new and emerging threats, impacts observed locally or globally, and prioritization of risk-based AML/CTF countermeasures.
- **Create employee awareness of new and emerging risks:** Use internal communications (written or video training) to educate staff on risks and typologies.
- **Implement agile risk assessment:** Ensure financial crime risk assessments reflect the volatility of current conditions, adequately measure the potential impact of known vulnerabilities and articulate the level of control your organization can reasonably expect to exert over those risks. This will likely require more frequent risk assessments.

To the extent that the pandemic and the need to WFH accelerated digital initiatives or otherwise resulted in the adoption of practices that enhanced compliance activities and outcomes, develop a plan for making these changes permanent and sustainable.

- **Know your customer:** Consider whether different information or verification techniques is necessary to compensate for lack of face-to-face contact.
- **Review adequacy of transaction monitoring programs:** Ensure transaction monitoring systems include appropriate scenarios to identify red flags applicable to the institution's customers and activities, and all thresholds (existing and new) have been retuned or validated appropriately. Consider use of data analysis and data analytic tools to enhance monitoring capabilities and quality assurance of monitoring output.
- **Focus on insider trading or market manipulation risks:** Ensure surveillance measures are heightened and adaptative to the current volatile environment. The noise of increased market volatility can provide camouflage for securities fraud and market manipulation.
- **Keep compliance records:** Where technology solutions are unable to support compliance obligations, such as voice recordings of trader communications, consider temporary alternatives like contemporaneous records that are consistent with regulatory guidelines.
- **Monitor government funding schemes:** Ensure that deposits and transfers involving funds from government-supported programs are scrutinized to identify any potential irregularities suggesting potential abuse. Employees should be familiar with terms, conditions and restrictions associated with such schemes.
- **Preserve privacy and data security:** Ensure remote working systems and virtual private networks (VPNs) 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.
- **Reinforce importance of management reporting:** Identify, report and track trends in financial crimes compliance to surface and respond in a timely manner to escalating risks.
- **Plan for sustainable transformation:** To the extent that the pandemic and the need to WFH accelerated digital initiatives or otherwise resulted in the adoption of practices that enhanced compliance activities and outcomes, develop a plan for making these changes permanent and sustainable.
- **Communicate with regulators on program challenges:** Keep regulatory supervisors informed of any challenges with meeting regulatory requirements to ensure the necessary guidance, support or exemptions can be provided individually or multilaterally.
- **Continue monitoring and testing:** Notwithstanding the added challenges resulting from working remotely, now is not the time to ease up on monitoring and testing financial crimes compliance programs. It is imperative that program gaps be identified and addressed to protect the institution from undue compliance and reputation risk.

How Protiviti Can Help

Protiviti's Financial Crime Risk and Compliance practice specializes 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 frameworks. Our team of specialists assist organizations 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 in the following areas:

- Operating model optimization to support the shift toward remote workforce while maintaining defined risk management and compliance strategy, business continuity, performance metrics, regulatory reporting and horizon planning for a return to work.
- Revision of financial crime compliance governance models to reflect changes to authorization, sign-off and reporting procedures.
- Incorporating COVID-19 vulnerabilities into the money laundering/terrorist financing (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 know your customer/customer due diligence (KYC/CDD) procedures to reflect shift from face-to-face, to online identification and verification procedures during social distancing measures.
- Development 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.

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

Contacts

Carol Beaumier
Senior Managing Director
+1.212.603.8337
carol.beaumier@protiviti.com

Shaun Creegan
Managing Director
+1.212.708.6336
shaun.creegan@protiviti.com

Matthew Moore
Managing Director
+1.704.972.9615
matthew.moore@protiviti.com

Erick Christensen
Managing Director
+1.704.972.9604
erick.christensen@protiviti.com

Resources

The following is a limited list of relevant releases from regulators, governmental agencies, multinational organizations and law enforcement agencies. This list will continue to expand and the content updated as more information about the types of illicit activity being identified becomes available.

- U.S. Department of Health and Human Services, COVID-19 Fraud Alert, May 2020.
- U.S. Department of Homeland Security, COVID-19 Exploited by Malicious Cyber Actors (AA20-099A), April 2020.
- Europol, Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis, March 2020.
- Federal Bureau of Investigation, FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic, April 2020.
- Financial Action Task Force (FATF), COVID-19-related Money Laundering and Terrorist Financing Risks and Policy Responses, May 2020.
- Financial Crimes Enforcement Network, Advisory on Medical Scams Related to the Coronavirus Disease 2019 (COVID-19), April 2020.
- Financial Industry Regulatory Authority (FINRA), COVID Fraud Task Force, March 2020.
- International Federation of Accountants, Reporting and Fraud Risk Arising from COVID-19 Pose Significant Challenges for Professional Accountants, May 2020.
- Transparency International, Corruption and the Coronavirus, March 2020.
- (UK) National Crime Agency, COVID-19, Suspicious Activity Reporting, April 2020.
- (UK) National Cyber Security Centre, UK and US Security Agencies Issue COVID-19 Cyber Threat Update, April 2020.
- Nasdaq, Fraud and Coronavirus (COVID-19), March 2020.
- United Nations Office on Drugs and Crime, Money Laundering and COVID19: Profit and Loss, April 2020.
- U.S. Securities and Exchange Commission (SEC), Look Out for Coronavirus-Related Investment Scams - Investor Alert, June 2020.