Financial Crime Risks Post-Covid-19

By Eduardo Ferrari and Matthew Clark

What's Happening Right Now?

Financial services leaders are facing a series of challenges to make quick and effective business decisions during this rapidly evolving time of uncertainty. The proactive decisions these leaders make today will set the path for years to come.

Initially during the pandemic, most organizations were focused on protecting and preserving their employees. However, this focus has broadened to encompass compliance, profitability and new products in response to COVID-19. Thus, it is important to have open and honest dialogue on how these products affect the existing portfolio.

> "What your organization does today will prepare you for the "new normal." It will also get you ready for what lies ahead."

New challenges are emerging every week, causing financial investigation units (FIUs) to adapt to the transformations in transaction monitoring, risk scoring and case investigations. These can include:

- The release of new products in response to stimulus and relief packages and economic conditions.
- A shift in product utilization by customers (cash to credit transactions).
- The inability to perform in-person due diligence and new client onboarding.

Financial Crime Risks Amid COVID-19

Money Laundering and Transaction Monitoring

With the influx of stimulus money and government aid, it is important for financial institutions to foresee and plan for the following scenarios:

- Businesses that may take advantage of the economic shutdown to find an opportunity to launder money through capital improvements and work with vendors that are willing to "cook their books," leveraging government programs to clean money when there is no specific need for assistance.
- Transaction monitoring systems are configured for outdated product utilization thresholds. The systems are not ready to detect the sudden shift in utilizations, such as a decline in cash transactions and an increase in debit/credit card transactions, automated clearing house (ACH), wires, etc.

- Some businesses will have a short decline in deposits, while others will remain the same or even grow. Segmentation must be re-balanced and become more granular based on the types of businesses affected.
- As financial markets fluctuate massively during the pandemic, institutions and the Securities and Exchange Commission (SEC) must closely monitor the actions of traders and brokers to identify unlawful activity.

Fraud

Massive increases in fraud and scams have been reported by financial institutions. This includes fraudulent products sold by vendors, insider trading and natural disaster fraud. Additionally, since the federal and local governments have declared a state of emergency, fraud cases are also coming in the form of fraudulent benefits applications and fake charities.

When it comes to benefits fraud, one typology involves fictitious employee schemes. This happens when a number of fake companies are created and are filing unemployment claims.

There has also been an increase of money mule scams through the usage of the "good Samaritan" or "social networking romance" scams.

Corruption

Corruption has been and will continue to be on the rise. Governments are allowing states, provinces and even countries to overspend at an unprecedented measure to combat the pandemic.

Due to these rising risks, there are substantive areas of U.S. trade regulation that financial institutions must pay close attention to, including U.S. anti-corruption, export controls, sanctions laws (which permit most exports of medicines, medical devices and food to sanctioned locations), and U.S. customs rules on personal protective equipment and medical devices.

Remote Work

With financial investigations units' shift to working from home, the following business operations may be affected: operational synchronicity, coordinating communication and due diligence investigations with law enforcement, and on-site interviews.

As more non-work distractions occur from working at home, risk assessment may leave the forefront of their minds. This could lead to exceeding attacks and scams that come online or through the mail. Phishing attacks claiming to be from banks can easily catch people who are distracted and lead to frauds and exposure of personally identifiable information (PII). According to a study by the cybersecurity firm Lookout, mobile phishing attacks increased 37% globally in the first quarter of this year.

Some companies were not prepared for this shift and may not have had protected technology resources, such as a virtual private network (VPN), that can encrypt the information going through the internet. Taking such precautions is a good first step in combating these criminals.

CARES Act Risks

With far-reaching government funding made available through the stimulus program, criminals and fraudsters may see this as an opportunity to exploit the situation and pose risk to the financial institutions that are trying to help restart a suspended economy. Some of these risks may include misrepresentation or falsified documents, applicant impersonation, and cross-border theft.

Compliance teams at Paycheck Protection Program (PPP) lenders are in a challenging position. They must balance the work of their own internal procedures, complying with the Bank Secrecy Act (BSA) and anti-money laundering (AML) best practices, yet rapidly work and make decisions to support struggling small businesses. To minimize risks and detect fraud associated with the Payment Protection Program loans, lenders must continue to prioritize BSA/AML compliance through multiple mechanisms:

1. Perform know-your-customer (KYC) screenings on all applicants.
2. Conduct effective screening for third-party risk.
3. Utilize location-based politically exposed person (PEP) screening.
4. Enhance high-risk geography AML monitoring.
5. Retain relevant and quality data.

When market disruptions arise, there are actions that organizations can take today to position their business for success no matter what news tomorrow brings. Organizations must prepare to confidently respond to critical questions:

- Do you have the correct risk model to address the new products released by the financial institution?
- Are your transaction monitoring system and customer risk models prepared for the shift in product utilization?
- Are you prepared to remotely perform an enhanced due diligence of the clients?
- Do you have effective dashboards to monitor the productivity of your financial investigation unit?
- How are you onboarding your customers when there is no access to local branches or offices?
- How is the communication with law enforcement and other banks?
- How does the CARES Act impact your financial institution? What are the risks to look for?

A Path Forward

Now more than ever it is important for financial institutions to develop plans in support of the following activities and scenarios:

- Performing virtual onboarding of a customer and enhanced due diligence of your customers who are most affected by the COVID-19 situation is key. This includes understanding ultimate beneficial owners with a complete risk assessment and customers who have new suppliers that warrant an enhanced due diligence (EDD) investigation into all related parties.
- Focus on international cooperation for customer due diligence (CDD) and information sharing with the regulators. Ensure clear communication and prioritization with regulators.
- Improve enterprisewide information sharing, including bank-to-bank and bank-to-government.
- Increased demand placed on financial institutions' KYC/AML teams due to product utilization shifts, such as:
  - Guarantees and other mechanisms
  - Increases in online payments
  - Money transfers
  - Small increases in remittances to regions impacted by COVID-19
  - Deposits rising from government support programs
  - Corruption
- The closing of existing businesses and opening of net-new businesses will also add strain to these teams. Firms must assess how these new businesses operate and perform CDD along with sanctions and PEP screening.

Key Takeaways

Tweak your operations

COVID-19 may be new, but financial crime is not. With the right awareness and programs in place, your organization will be ready to fight it and shield itself from regulatory scrutiny. Proper risk assessments, model calibrations and technology implementations will prepare your organization for today's volatile market and the uncertainty that lies ahead. COVID-19 will impact people's lives forever. Businesses will continuously change the way they operate and perform activities and will never look back. What your organization does today will prepare you for the "new normal." It will also get you ready for what lies ahead.

What Can Huron Do?

Huron can help your firm with consulting services that include:

- Transaction monitoring tuning, alert/case backlog management, enhanced due diligence reviews, fraud and financial crimes advisory matters.
- Cloud adoption, even if you are not ready for a full transformation.
- Using analytics and artificial intelligence (AI) application programming interfaces (APIs) to quickly deploy your compliance requirements.
- Creating effective dashboards leveraging the top tools in the market: Tableau, Qlik, Oracle OBIEE and Oracle Analytics Cloud, among others.
- Applying the use of machine learning and analytical tools.
- Increasing the efficiency of screening programs by creating integration points and consolidating information in one place on your system of choice.
- Providing training for the FIU front-line workers to raise awareness.
- Facial recognition software to address KYC/ fraud needs.
- AML, KYC and Office of Foreign Assets Control (OFAC) consulting services.

Visit huronconsultinggroup.com/expertise/enterprise-solutions to contact Huron's financial risk and compliance experts.

huronconsultinggroup.com