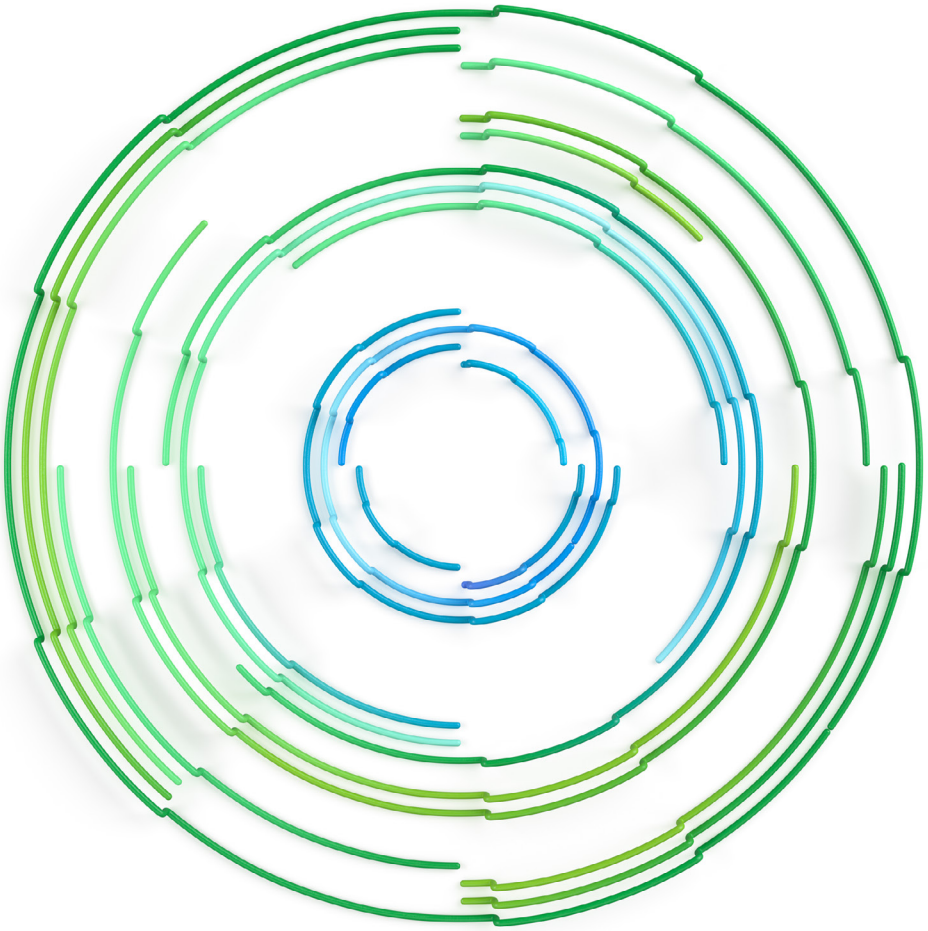
Deloitte.



Making sure that financial crime doesn't pay

Considerations for technology-driven payment services providers

November 2021

Contents

The promise of payments technologies is being realized. Consumers are executing frictionless payments in their everyday transactions. Organizations are enhancing customer experiences through faster payments and richer payment data that enables value-added services. Countries are updating their payments infrastructures, realizing that faster payments reduce costs and can even boost GDP growth by serving unbanked individuals and enabling digitalized capabilities in the economy. In some nations, taking cash out of the economy is a driver, with rapid or real-time mobile payments facilitating and accelerating transactions that traditionally may have occurred face-to-face.

Unfortunately, these advances have come with certain risks, particularly for technology-driven payments companies. As those payment services providers (PSPs[1]) have become key players in the payments landscape, highly skilled, tech-enabled financial criminals have increasingly targeted them. Their goal is to exploit any potential weaknesses in a company's controls, defenses, and responses related to fraud, money laundering, and other financial crimes.

Meanwhile, technology-driven PSPs inhabit a vulnerable position in the payments space:

- Various drivers are heightening the risk of financial crime at PSPs, opening pathways for bad actors to capitalize on those companies' relative lack of financial crime experience. The coronavirus pandemic and its economic impact is one such driver (see sidebar). Indeed, the US Treasury's Financial Crimes Enforcement Network (FinCEN) has asked financial services organizations how they have been addressing potentially heightened financial crime risks during this period[2].
- While they are not regulated as banks, technology-driven PSPs are subject to anti-money laundering (AML) and counter terrorist financing (CTF) regulations, and to laws related to bribery, corruption, and other illegal payments; in many jurisdictions, they are facing increasingly intense law enforcement scrutiny.
- While PSPs possess deep technological and analytical resources and often excel at targeted marketing, credit analysis, and managing cyber risks, financial crimes can present new and unfamiliar risks and significant exposures. Technology-driven PSPs also often grow exponentially, which can exceed their ability to scale their control environments and risk management processes at the same rate.

For these reasons, many PSPs need to upgrade their fraud and financial crime programs to adequately address the risks to their systems, customers, users, partners, and reputations. This paper illuminates some of the major financial crime risks posed to PSPs and considerations to address those risks more effectively and efficiently. It also presents regional perspectives on those global risks.

COVID-19 & Financial Crime Risk

The coronavirus pandemic and its economic impact has heightened financial crime risks in several ways:

COVID-19 related fraud schemes: Bad actors have set up bogus online storefronts purporting to sell personal protective equipment (PPE), test kits, and other COVID-related products that turn out to be counterfeit or nonexistent after they've been purchased. In addition, PSPs should exercise heightened vigilance around AML, CTF, sanctions, and other illegal payments schemes, given that times of extraordinary disruption typically present new opportunities for crime.

Increased financial pressure and motivation: Unemployment, reduced cash flow, and business failures have—in some cases—heightened the motivation of usually ethical individuals, including internal parties, to engage in unethical conduct.

Abuse and fraud around government assistance: Bad actors invariably target government programs set up to rapidly disburse funds to distressed parties. These programs may lack adequate fraud deterrence and detection mechanisms to control and monitor the money being distributed due to modifications or waivers of controls or other governance protocols in order to quickly provide relief. Organizations that have not been vigilant in monitoring for fraud risks are often caught up in efforts by governments to recoup fraudulently paid benefits.

Dislocation within organizations: To the extent that an organization has reduced or reallocated staff, experienced internal distractions, or failed to keep pace with heightened threats, it may become more vulnerable to financial crime. For example, rapid transition to remote work and the resulting strain on cyber defenses, as well as laid-off and/or potentially disgruntled staff who have continuing system access, may generate exposures.

Risks associated with volume: Companies and consumers are both rapidly increasing their use of online ordering and payments. Some companies are not accustomed to high volume and many have reduced their information standards or risk-related hurdles for new customers. Others may lack the security or support needed to handle this kind of change.

This period calls for **heightened vigilance** at a time when resources may be stretched thin.

1. In this paper, payment service providers include mobile money transmitters, money service businesses, and other transmitters of funds and payments who employ digital technologies to execute or support mobile payments
2. Notice Related to the Coronavirus Disease 2019 (COVID-19), FinCEN NOTICE, May 18, 2020 https://www.fincen.gov/sites/default/files/shared/May_18_Notice_Related_to_COVID-19.pdf

The payments landscape and financial crime

The payments landscape covers a lot of ground. It is a global business with players ranging from major banks and tech giants to small start-ups, from facilitators of e-commerce to providers of mobile wallets. It includes any company that facilitates payments on behalf of others, from the latest peer-to-peer payments app to traditional money services businesses (MSBs). Customers range from government agencies and multinational corporations through to online shoppers and day laborers paid in cash. Even gaming companies that enable conversion of cash to tokens and back to cash are, for purposes here, PSPs.

PSPs usually charge a fee per transaction. Yet this space also includes aggregators that organize customers' transactions—as well as bank accounts, credit cards, loans, and investments—to provide a single view of their finances. While payment aggregators do not initiate payments, instead charging subscription fees for their services, they are exposed to financial crime risks through the data they handle and their access to accounts.

Traditional financial services companies such as banks and credit card issuers also provide mobile payments, often through mergers, acquisitions, or partnerships with PSPs. However, as we have noted elsewhere[3], some banks are refocusing on core financial services and moving away from payment services. Also, product commoditization and decreasing value derived from speed, access, and convenience are spurring PSPs to develop value streams from new offerings and strategies.

PSPs are exposed to financial crime in the form of fraud, money laundering, terrorist financing, and sanctions violations and other illegal payments, such as those related to drug and human trafficking and labor exploitation. Money laundering is among the most widespread financial crimes[4], one on which many governments have focused regulatory and law enforcement resources. Moreover, any profit-driven criminal activity, including fraud, is a predicate offence for money laundering. That means that a PSP's handling of those funds must be considered within the range of money laundering and terrorist financing risks.

"Criminals don't think in silos the way many PSPs and financial institutions may structure themselves. They don't separate fraud from money laundering or cyber crime. PSPs need to think the same way, and many are starting to. For example, some are developing cyber-fraud fusion centers to manage these risks more effectively or using managed services to tap expertise and efficiencies."

Michael Shepard
Principal, Global Financial Crime Leader
Deloitte US

Risks are rampant, but rarely apparent

The risks posed to PSPs by financial crime are significant and consistent with those posed to banks and other financial institutions. These risks primarily include:

- Financial losses to customers, to the PSP, and to related financial institutions in the payments system
- Regulatory censure and fines, which represent direct financial losses, as well as potentially increased regulatory scrutiny going forward
- Reputational risks, which can result from financial losses, regulatory censure, and negative media coverage, and which can undermine a prospective or existing partnership or merger

The exposures to these risks are rising for PSPs due to several factors:

- The sheer volume of transactions PSPs are handling as consumers move increasingly toward mobile payments has generated increased financial crime risk. That stands to reason, given that financial criminals go wherever large sums of money can be found.
- Financial and cyber criminals generally seek out relatively vulnerable parties, and relatively new PSPs tend to be less experienced in addressing financial crime (and more lightly regulated) than banks.
- Given that they are less heavily regulated, some PSPs may have less rigorous fraud and financial crime programs, and lack the more mature culture of compliance of most banks. This amounts

3. Payments trends 2020 – InFocus: Strategies to prepare for the future of payments, 2019 Deloitte Development LLC https://www2.deloitte.com/content/dam/Deloitte/us/Documents/financial-services/us-fsi-infocus-payments-2020.pdf
4. Money Laundering, United Nations Office on Drugs and Crime https://www.unodc.org/unodc/en/money-laundering/overview.html

to taking a "pay-and-chase" approach—accepting the loss and attempting to catch the criminals and recover the funds—rather than a risk-based approach to financial crime.

- Technology-driven PSPs tend to focus primarily on delivering a fast, frictionless, and enjoyable customer experience; as a result, they can sometimes view anti-crime considerations as an afterthought, rather than intrinsic to product and service design and delivery. Robust AML/CTF controls are genuinely risk-based and embedded in an organization's products and services, as well as in its systems and processes.
- PSPs facilitating a high volume of relatively low value payments may perceive themselves to be at lower risk than banks and other financial institutions; however, criminals are increasingly using low-value/high-volume platforms to launder criminal proceeds.
- While likely to possess the data management and analytical resources to address financial crime risks, some tech-based PSPs lack the risk management frameworks and infrastructure needed to address financial crime risks at a level commensurate with the risks they face. Some also lack the required expertise in financial crime and related regulatory expectations, or have dedicated people with that expertise to other matters.

In addition, financial criminals now use robotic process automation (RPA) and algorithmic models to discover how to bypass or exploit identification and authentication mechanisms and to monitor transaction thresholds and location detection. They also often try to obtain knowing assistance from internal accomplices or to compromise unwitting internal parties through phishing schemes and similar approaches. For its part, a PSP faces many competing priorities for resources, while a financial crime organization—and organized crime is exactly what it is—has one priority: profiting from crime.

"Some PSPs seek a single technology solution to try and manage their financial crime risk, but that doesn't really exist. They usually need an ecosystem of solutions to help manage their data to ensure completeness and accuracy and then identify the right solutions that work together to help detect and predict financial crimes. Even more advanced data-driven PSPs often find it challenging getting the ecosystem right and fail to implement the correct technologies required to adequately manage their fincrime risk."

Andrew Oates
Partner, Financial Advisory, Forensic Analytics Leader,
Deloitte UK

Risks can vary by region

Certain financial crime risks apply to PSPs regardless of location, and the coronavirus has become a catalyst for similar schemes worldwide. However, regional and local financial crime trends can vary. Also, for a company operating in a global marketplace, a significant financial crime can quickly spiral out of control, spreading financial market disturbance and triggering regulatory inquiries and negative media coverage in multiple locations.

Therefore, it's essential that PSPs conduct and document a detailed assessment of financial crime risks, and actively monitor new and emerging threats. To assist these efforts, we offer the following observations from just a few of Deloitte's regional forensic and financial crime specialists.

Africa

With more than 50 countries—marked by various cultures, languages, and levels of literacy and economic development—Africa represents a highly diverse payments market. South Africa has the most highly developed payments system, but it too contains variations.

In addition, in Africa:

- Many PSPs see mobile payments as relatively low risk, which is often not the case; in fact, that perception can itself create risks because criminals target entities with lax defenses.
- The mobile payments market here typically has strict regulations regarding payments. Ironically, those regulations contribute to the perception that this is a low risk activity, for example with low transaction limits equating to low risk.
- The foregoing two factors can lead some PSPs to reduce spending on controls and monitoring and lead regulators to devote less attention to PSPs than to banks.
- However, we've seen terrorist activity being funded through multiple, relatively small payments via mobile wallets, as well as cases of fraud and money laundering. Also, due to the pandemic, fraud schemes and new financial crime typologies are flourishing.

"The African market has in a way leapfrogged other locations in terms of payments solutions, sometimes adopting new technologies without having a long history of regulatory processes, manual controls, and strict compliance. That situation can heighten financial crime risks while limiting visibility into those risks."

Muzzi Ebrahim
Financial Crime & Data Analytics Leader and Partner, Financial Advisory
Deloitte United Arab Emirates

Asia Pacific

The APAC region possesses a rich mix of highly mature companies on the one hand and smaller emerging ones on the other. Some of the newer companies are working to secure an early mover advantage by handling a high volume of low value transactions, similar to the Africa model.

In addition, in the APAC region:

- The speed of adoption of digital technologies in finance is quite rapid. For example, in Australia consumers quickly adopt new technology, including in the payments arena. Financial criminals are attracted to areas that are scaling rapidly, as payments technologies have been in this region.
- PSPs are often not subject to licensing requirements and regulatory oversight at the levels that banks experience. This can leave them relatively more exposed to risks, particularly in locations where bribery, corruption, and labor exploitation are more common.
- Regulators often find themselves playing catch-up with PSPs, to the point where, for example, in Australia, the speed of evolution in payments products often exposes gaps in the regulatory framework; however, regulators are actively working to cover these offerings.
- Some US or EU companies with APAC operations may dedicate less funding and management attention to those operations, which can be problematic from both the financial crime and the regulatory standpoints. Also regulatory regimes in this region vary, with many of them quite stringent, as they are in Hong Kong, Singapore, Australia, New Zealand, Japan, and China. Companies based outside the region often underestimate the resulting complexity.

5. Anti-money laundering and counter-terrorist financing measures – United Kingdom – Mutual Evaluation Report – December 2018, Financial Action Task Force https://www.fatf-gafi.org/media/fatf/documents/reports/mer4/MER-United-Kingdom-2018.pdf

"Certain areas within APAC grapple with relatively low transparency and high corruption that can heighten risks. Also, the APAC region includes a wide range of regulatory regimes, many of them quite stringent. We are seeing some significant regulatory enforcement actions in this region, relating to significant underlying criminal activity, so PSPs should not underestimate the regulatory complexity or scale of financial crime activity in this region."

Lisa Dobbin
Partner, Deloitte Forensic and Financial Crime Leader,
Deloitte Australia

Europe

Some of the greatest risks in Europe relate to data privacy, which European users tend to be more guarded about than in many other areas, particularly the United States.

In addition, in Europe:

- The EU, despite its efforts at harmonization, still poses a patchwork of regulations. This occurs as member nations translate a European Commission directive, which automatically becomes law in each member nation, into workable regulations. That is where efforts to harmonize regulations can break down.
- Identity theft and the fraud that stems from it continue apace in the EU. There has also been an increase in bogus messages purportedly from the user's contacts requesting funds to assist the contact in a nonexistent emergency.
- In the EU, financial criminals aggressively apply RPA and machine learning technologies to test thresholds and location limits on payments and to find ways of establishing fake accounts.
- As in the United States, EU governments aggressively enforce AML regulations and law enforcement agencies monitor for payments related to terrorism, trafficking, and other illegal activities.

"Regulatory attention to financial crime in the EU payments space has grown significantly over the past two to three years. Therefore, more companies have made financial crime defenses a priority, to the point where it has become a key topic in M&A deals – something PSPs should be aware of."

Baldwin Kramer
Partner, Financial Advisory, Forensic & Financial Crime
Deloitte Netherlands

United Kingdom

The UK regulator is, in their use of data and analytics, among the most advanced in Europe. The Financial Conduct Authority (FCA) has emphasized education as a strong defense and has issued principles around ways to enhance monitoring.

In addition, in the UK:

- The Financial Action Task Force (FATF) found that the UK has one of the better systems for combating money laundering and terrorist financing in the more than 60 countries they assessed[5]. However, there is no UK regulation around PSPs' ability to detect fraud, as there is around AML. So, in general, the resources that go into AML efforts far exceed those going to fraud detection and reporting.
- The most recent AML directive extends coverage to prepaid cards and custodian wallet providers. It also lowers the limits for when an organization must conduct customer due diligence transaction monitoring for detecting money laundering.
- As banks have cracked down, launderers are turning more to PSPs. Financial criminals realize that if, in laundering funds, they were to put £10,000 in a PSP account, it would almost certainly set off an alert, but even a long series of £100 deposits probably would not.

North America

The United States has long been an attractive location for money laundering due to the size of its banking system the stability and widespread use of its currency, and the ease of investing funds and purchasing real estate. The sheer number of financial institutions and financial technology companies in the country, the number of consumers, and the volume of transactions also make it attractive.

In addition, in North America:

- While attractive for financial criminals, the United States has robust legislative and regulatory regimes and vigorous enforcement of AML, Know Your Customer under Bank Secrecy Act (BSA), Foreign Corrupt Practices Act (FCPA), and similar regulations. When regulators and law enforcement succeed in controlling certain crimes, financial criminals tend to move on to less well-regulated and thus more attractive activities.
- Canada may be attractive to financial criminals in that the process of bringing charges and prosecuting cases can be long and costly, except in cases related to terrorist activity. However, in the past three to five years, regulators are focusing more intensely on PSPs than in the past.
- In the United States and Canada, as in other jurisdictions with numerous financial crime laws and strong regulatory regimes, PSPs need risk-based approaches and practical frameworks for organizing their technological and human resources efficiently. It's not something you can just put more people on or throw more money at to obtain the desired result.
- PSPs must be on guard in North America because digital channels and financial criminals' increasing sophistication and use of RPA and AI enable more efficient methods of executing fraud.

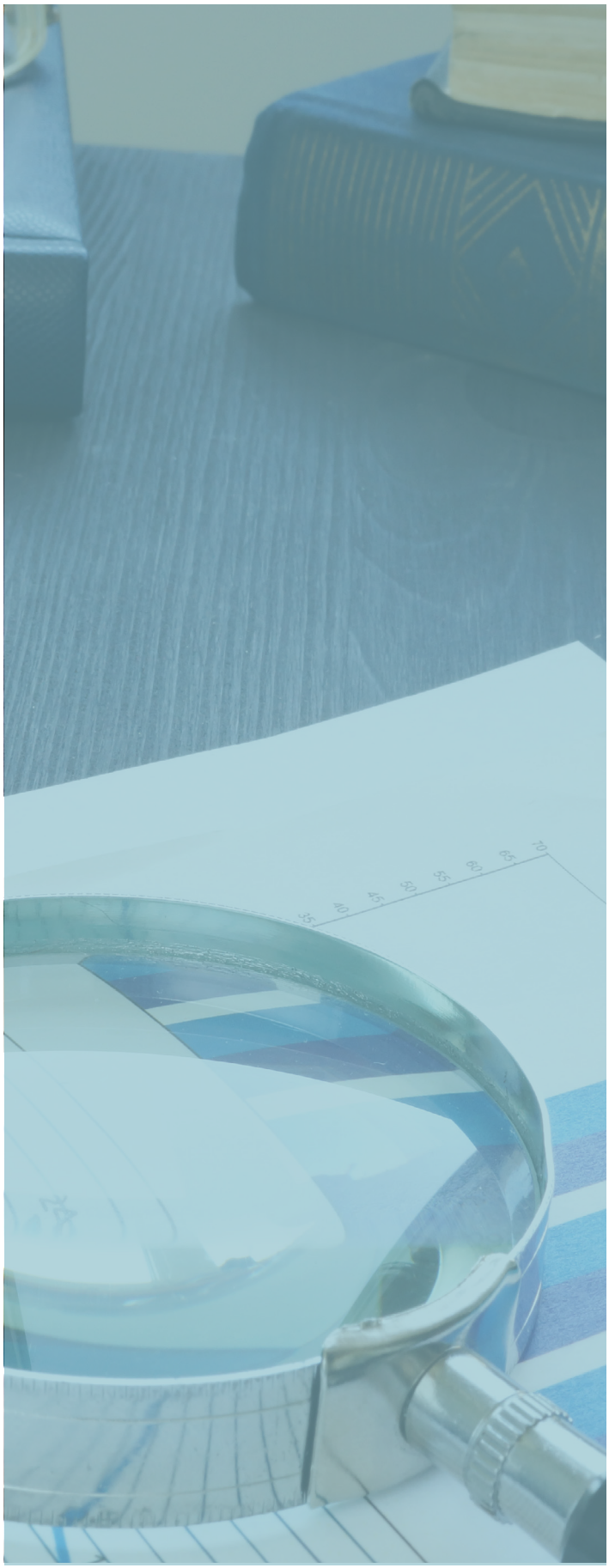
"Organized crime is sophisticated and lucrative business for threat actors, who are efficient in exploiting the design of payment systems. They camouflage their schemes, by peppering their transactions among millions of others, often going undetected. PSPs who constantly modify their fraud defenses, by harnessing collective fraud intelligence signals and refine detection activities—will increase the costs and time for those threat actors that continue to target the PSP."

David Stewart
Partner, Forensics and Financial Crime
Deloitte Canada

"PSPs are entrepreneurial, innovative, and agile and have strong data aggregation and analytical capabilities. Their challenges typically involve wedding those advantages and capabilities to an investigative mindset and a strategic understanding of the risks and costs of financial crime."

Jon Haywood
Partner, Forensics and Financial Crime
Deloitte Canada

All regions need greater cooperation among PSPs and financial institutions, and among companies and regulators, in sharing data related to financial crime. Public-private partnerships can facilitate data sharing while protecting individual privacy and business practices. Financial crime is a global enterprise and it will take considerable coordination and cooperation to address it as criminals increasingly realize that huge sums of money have migrated to digital payments platforms.



Potential flaws in current approaches

PSPs that face heightened risk, in our experience, tend to be those that view losses associated with financial crime as "a cost of doing business." They also tend to view a certain (usually too generous) level of financial losses as acceptable and may fail to recognize that fraud is a predicate for money laundering, which triggers regulatory obligations in most jurisdictions. As a result, they may dedicate fewer resources to financial crime until its costs reach an unacceptable level or they face regulatory censure.

Such approaches have several major flaws:

- They don't work well. A lax approach to financial crime invariably leads to excessive losses. After a crime, resources must be devoted to analysis of the incident, detection of the perpetrators, restitution of losses, and, when possible, apprehension and prosecution of the perpetrators. Then, defenses must be developed and deployed anyway, often at greater expense.
- Losses typically rise over time. When financial criminals—particularly fraudsters—find an avenue to exploit, they tend to exploit it to their full advantage. Many fraud schemes occur over a period of months and sometimes years before they are detected. This enables criminals to extract large sums cumulatively over time below the radar of inadequate monitoring.
- Customers gain no comfort. Educating users and other parties in the payments process is a key element of a sound financial crime risk-management strategy. That education enables those parties to do their part in the PSP's crime prevention program. It also gives them a sense of comfort and control around the PSP's approach to financial crime.
- They do not completely deter internal bad actors. A robust fraud monitoring program sends a strong message to potential bad actors within the organization and its payments system: They will probably get caught. The presence of such a program—and notification that it exists—is itself a deterrent to employees tempted to exploit their position and to any external parties who approach them.
- They increase exposure to reputational risks. Even if a PSP believes that financial crime losses do not (to date) warrant a robust program, there are reputational risks to consider. Those risks, and the prospective losses they create, can far outweigh direct financial crime losses. A single well-publicized incident can damage a PSP's reputation for months, even years, discouraging customers and potential business partners and inviting greater regulatory scrutiny.

A "pay-and-chase" approach to financial crime "works" until it doesn't. In contrast, a rigorous, risk-based financial crime program—with a diligent upfront assessment of financial crime risk—works from the start. It deters bad actors and facilitates faster, deeper investigations of any incidents that do occur. It provides greater comfort to senior executives, the board, regulators, customers, partners, and investors. It also enables internal and external auditors to provide assurance over controls and enhances the allocation of risk management resources.

Elements of a risk-based approach

Technology-driven PSPs have substantial resources to apply to managing financial crime risks, including copious amounts of data and strong analytical capabilities. What's often missing are the frameworks and methodologies that underpin and enable a sustained anti-crime program.

A good number of PSPs hire individuals from banks to design, develop, and implement a financial crime risk management program. While this can be a useful step, it is only a step. It may be unrealistic to expect a bank compliance officer or similar expert to enter a non-bank environment and unilaterally establish such a program. While writing policies and recommending controls are key tasks, they usually cannot, on their own, bring about all the needed changes.

That said, financial crime knowledge resides in institutions that have historically been subject to financial crime laws. Therefore, it's natural and sensible for PSPs to tap those sources of talent, particularly at senior levels. This pattern occurs in virtually any newly regulated sector. In addition, although banking-level rigor would be useful in program development, it must be paired with deep understanding of the payments infrastructure to be effective. Those initiating and maintaining the program will also need senior executive and organizational support.

In light of prevailing financial crime risks, every PSP should seriously consider:

- **Establishing a risk-based approach and framework:** A risk-based approach considers all of the risks posed by financial crime and goes on to develop a framework for managing those risks on a proportionate and prioritized basis. It lays the foundation for activities such as authenticating identity, onboarding users, monitoring transactions, handling alerts, and designing, testing, and implementing controls.

  Particularly in rapidly growing markets, it is useful to take a risk-based approach and to align the risk management framework with actual risks and regulatory expectations. Doing so enables management to adapt proactively to vulnerabilities and better deploy resources and redeploy them when, for example, the organization changes its business model, offers new services, enters new partnerships, or responds to new regulatory expectations. Further, in taking a risk-based approach, management can be proactive in adapting to vulnerabilities, rather than being stuck in a reactive cycle of chasing historical issues

- **Developing a holistic view of financial crime risks:** Financial crime covers a range of activities often viewed by regulators and financial institutions in silos – a view that PSPs should avoid. It's preferable to perform a comprehensive risk assessment that encompasses fraud, identity theft, account takeover, money laundering, bribery, corruption, and payments related to sanctions, drug and human trafficking, and labor exploitation

  Work then turns to assessing specific risks and mitigating them, and designing, implementing and testing controls and monitoring. Note that technology should not be mistaken for risk management itself. To be of real use, a technology tool must operate in the context of a risk-management framework and program. Otherwise, it will likely add costs, confusion, and a false sense of security as well as increase risk.

- **Implementing a program of financial crime monitoring:** When properly applied, intelligent technologies for monitoring transaction activity can now generate more targeted coverage along with far fewer false positives. These are not off-the-shelf, one-size-fits-all software products; rather, they are customized AI and machine learning tools based on the organization's business model, users, transaction type and volume, risks, and history.

  Similarly, predictive analytics can identify potential issues early in the process when a customer is applying for an account or being on-boarded. They can also flag emerging risks before they become incidents. For example, certain organizations, with proper notification to and respect for the privacy of the subjects, monitor internal emails for language that has been found to be related to potential criminal activity.

- **Building a culture equal to the risks:** A technology-driven PSP needs a culture of compliance commensurate with the risks it takes on when moving money on behalf of others. This kind of culture change begins with a senior executive commitment to proactive mitigation, detection, and prevention. It is the leaders who set the risk appetite of the organization and who decide which deterrents and controls will be designed and built into products and services.

  The organization's senior leaders also need to set the tone at the top and promulgate awareness of financial crime risks across the organizational ecosystem. Tone at the top together with regular training programs will create and reinforce the needed culture.

- **Establishing a whistleblower program:** To further reinforce that culture, the organization should consider establishing a whistleblower program. As with internal monitoring, the mere presence of such a program can reduce internal fraud risks while enabling early detection. It also signals that the organization takes financial crime seriously and does not intend to be an easy victim.

  Engaging with regulators. Regulators are increasingly recognizing the importance and scale of PSPs, particularly major ones, within the global financial system. Many are keen to actively engage with PSPs to learn of their benefits to that system and how to effectively approach the risks and regulatory challenges. Proactively engaging with regulators in the various markets in which the organization operates can improve both parties' understanding of the payments system and trends in products, services, technologies, and regulatory priorities, as well as the evolving financial crime landscape.

- **Accessing the needed assistance and resources:** Financial criminals possess technology and motivation equal to those of PSPs. Their methods change as fast as, and in many cases faster than, a PSP's ability to keep up. Therefore, it is wise for CCOs, CROs, and other executives to educate themselves about financial crime, methods of monitoring and prevention, and the business case for using those methods.

  Leaders should also consider an assessment of the organization's financial crime exposures and its ways of addressing them. This may require briefings from external specialists who monitor financial crime trends, understand regulatory expectations, and focus on financial crime full time.

Let's talk

As the payments landscape continues to evolve, PSPs will need to periodically reevaluate their financial crime programs and upgrade them as needed to address threats from increasingly sophisticated criminals. Those criminals are attuned to opportunities created by any business handling large amounts of funds amid potentially inadequate detection and deterrence mechanisms. Moreover, both financial crime and regulatory trends are likely to vary by region.

An effective program can not only deter financial crime; it can also assist in creating a more secure control environment and more timely and targeted risk monitoring. Deloitte stands ready to assist PSPs in their efforts to combat financial crime and navigate related regional regulatory complexities. To learn more, get in touch today.

Contacts

Michael Shepard
Global Financial Crime Leader and, Principal, Deloitte US

Samantha Parish
Partner, Global Financial Advisory Clients & Industries Leader, Deloitte US

Andrew Oates
Partner, Financial Advisory, Forensic Analytics Leader, Deloitte UK

Muzzi Ebrahim
Financial Crime & Data Analytics Leader and Partner, Financial Advisory, Deloitte United Arab Emirates

Lisa Dobbin
Partner, Deloitte Forensic and Financial Crime Leader, Deloitte Australia

Baldwin Kramer
Partner, Financial Advisory, Forensic & Financial Crime, Deloitte Netherlands

Nikil Mathur
Partner, Financial Advisory, Forensics, Deloitte UK

David Stewart
Partner, Forensics and Financial Crime, Deloitte Canada

Jon Haywood
Partner, Forensics and Financial Crime, Deloitte Canada

Brendan Maggiore
Senior Manager, Forensic and Financial Crime, Deloitte US

Deloitte.