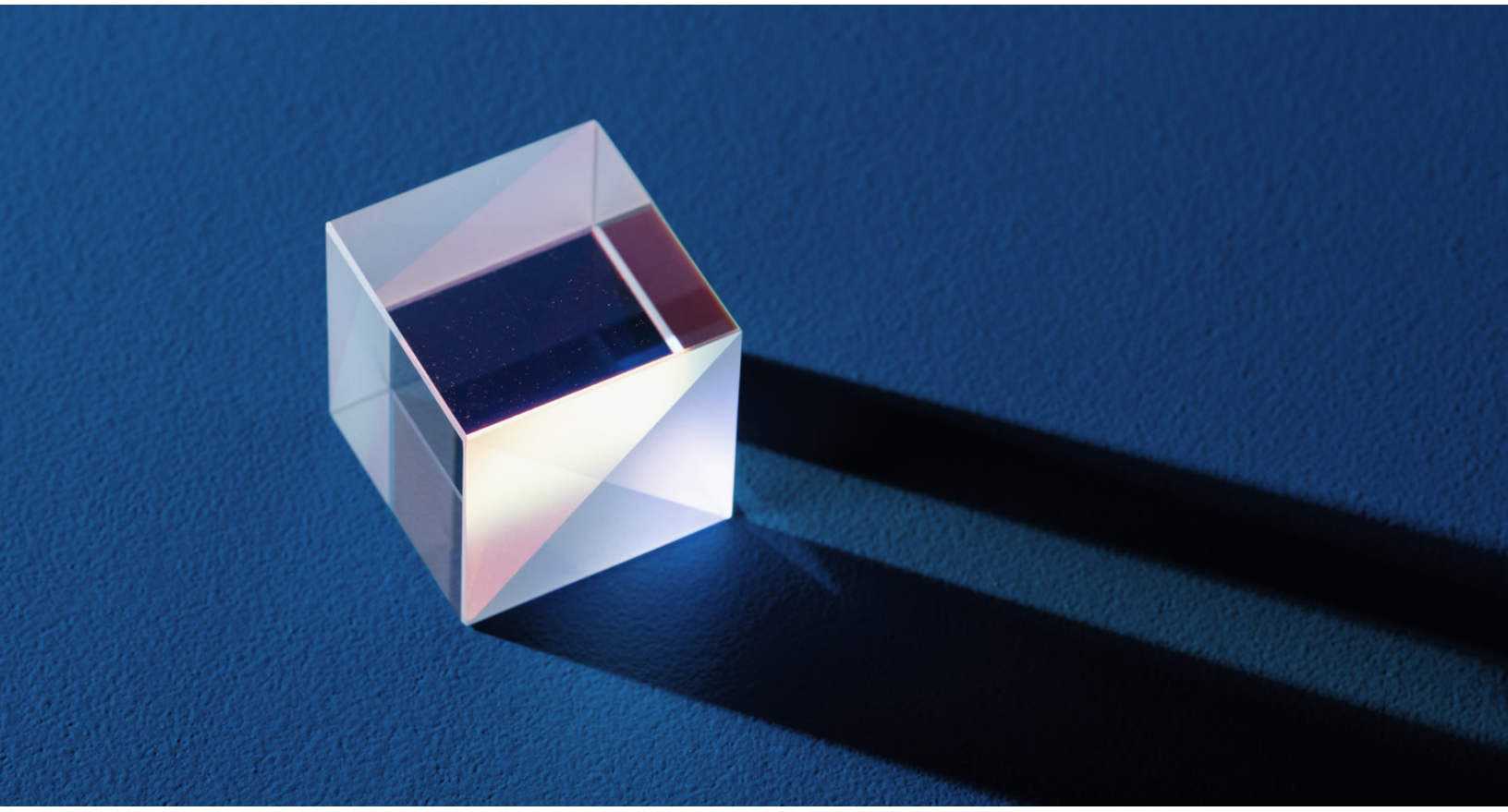
McKinsey & Company

Risk & Resilience Practice

# Managing financial-crime risks in digital payments

To face down the financial-crime threat, payments service providers can learn from banks while utilizing their own advanced technological skills.

*by Daniel Mikkelsen, Shreyash Rajdev, and Vasiliki Stergiou*





June 2022

**Payments services** were long offered to companies and individuals by banks, but in the past 20 years dedicated and specialized providers greatly expanded the market. In 2020, global payments revenues reached $1.9 trillion. During the past decade, individuals and e-commerce merchants have increasingly adopted payments services. About half the recent growth has been in consumer-to-business and business-to-consumer payments. In North America and Europe, electronic payments are expanding very fast, at twice the GDP growth rates in these regions; in Asia, the expansion is happening even faster. The explosion in the number of electronic transactions is part of the e-commerce and m-commerce booms and the shift away from cash payments. Digital-payments mechanisms include cards but also recent payments innovations, such as digital wallets. This shift to digital payments is expected to continue.

One unavoidable measure of the booming success of payments service providers (PSPs) is the increased risk of financial crime. Unmanaged, this risk can pose an existential threat for PSPs. Perceived weaknesses in the controls applied by electronic-payments platforms will consequently draw attention from regulators. Banks, furthermore, are increasingly expecting the PSPs that form part of their network to have strong anti–money laundering (AML) and fraud controls in place. Rather than wait for new regulation, PSPs can move proactively, incorporating lessons from banks' experience while utilizing their own advanced technological skills. This discussion lays out the key principles for designing a strategy that PSPs can use to their advantage in countering the threat of financial crime while preserving and enhancing the PSP customer experience.

## The rising regulatory focus

The rising threat of financial crime has drawn increased regulatory attention. The UN Office on Drugs and Crime reports that money-laundering values are extremely difficult to estimate but stresses that the amounts are enormous and rising, reaching 2 to 5 percent of global GDP, or $800 billion to $2 trillion annually.[1] Those engaged in prohibited and outlawed activities—such as the illicit drug trade, tax-avoidance schemes, money laundering, and consumer scams—are increasingly utilizing digital-payments channels, raising the risk that money is being laundered by these means.

Financial-crime incidents and failings have been on the rise throughout the pandemic, according to the Financial Action Task Force, a leading international standards-setting body for financial crime. Particularly in the consumer realm, the potential for fraud has also grown with the advent of the COVID-19 pandemic. To cope, many PSPs enhanced their controls, such as transaction monitoring, while regulators updated requirements relating to remote onboarding and ongoing customer due diligence. While most platforms have stringent know-your-customer (KYC) requirements (such as identity verification) and ongoing transaction monitoring, others require less detail to open and maintain an account. In any case, vulnerabilities in existing controls across the anti–financial crime value chain are targets for those engaged in financial crime. Crucially, digital and contactless payments as well as remote onboarding are capabilities now favored by many more customers. The increasing volumes stretch the capacity of companies and their ability to identify and manage the relevant operational risks without negatively affecting customer experience.

Financial crime can pose an existential threat for PSPs if left unmanaged. For example, PSPs offering acquiring services at scale can expose themselves to fraudulent organizations set up specifically to use these services to launder proceeds from illegitimate sources. A lack of robust, continuous KYC processes, for onboarding and thereafter, can attract money launderers and damage the provider's reputation and regulatory standing. Similarly, as PSPs facilitate the transfer of funds to and from different entities, they must ensure that none are sanctioned entities nor are owned by a sanctioned ultimate-beneficial owner. Scalable customer-monitoring, transaction-monitoring, and screening programs are key controls. In addition, PSPs' facilitating payment services to and from virtual-

[1] "Money laundering," UN Office on Drugs and Crime.

asset exchanges (VASPs) are exposed to reputational and financial-crime risk arising from certain activities and customers associated with these exchanges. To counter the threat, the PSPs need to understand these exchanges' anti–financial crime control frameworks.

Perceived weaknesses in the controls of digital-payment platforms may lead to increased regulation. This is a well-recognized pattern within the industry because financial institutions generally react to new regulation rather than anticipate it. The European Union, for example, adopted the Revised Payment Services Directive (PSD2) in 2015. The regulation was intended to harmonize and enhance consumer protections throughout the PSP landscape in the European Union and the European economic area. It introduced a new focus on antifraud controls. Firms are now expected to be more or less compliant with PSD2, which is likely to be comprehensively reviewed soon, with an increased focus on fraud and customer protection. Similarly, as PSPs form part of the payments value chain, regulators are already cautioning banks that facilitate payments on behalf of PSPs to validate the adequacy of PSPs' anti–financial crime controls across their network of customers and partners.

Given growing concern about the effectiveness of the fight against financial crime, the European Union is also looking to set up a dedicated regulatory body, and PSPs are likely to see heightened scrutiny on these issues. In July 2021, the European Commission (EC) announced plans to create a new EU authority to counter money laundering and terrorism financing. The EU-level Anti–Money Laundering Authority (AMLA) will be supported by new legislative measures designed to strengthen the detection of suspicious activities and better insulate the financial system from criminal misuse. The EC announcement stated that AMLA will "greatly enhance" the existing EU framework on financial crime, by taking into account new and emerging challenges linked to technological innovation. These include virtual currencies, more integrated financial flows in the single market, and the global reach of some proscribed organizations. These proposals will help to create a much more consistent framework, making compliance with rules on anti–money laundering and countering the financing of terrorism (CFT) easier for the operators—especially those active across borders.[2]

In the United States, the current regulatory focus is on licensed money transmitters, but PSPs cannot assume that similar standards will not be applied to other providers in these areas. Nor can it be assumed that only banks will bear the burden of financial-crime compliance. The Financial Crime Enforcement Network (FinCEN) and the Federal Deposit Insurance Corporation (FDIC) have issued guidance to help financial institutions recognize the higher risks posed by PSPs. As a result, US financial institutions now expect the PSPs forming part of their network to have strong controls for AML, sanctions, and antifraud. These controls include merchant due diligence and suspicious-activity monitoring, as well as other processes (such as risk assessments), to ensure that PSPs do not inadvertently put financial institutions at further risk.

Since financial institutions in Europe and other jurisdictions do business in US dollars, all will be affected by some of these measures. As more incidents of fraud and money laundering surface, the United States and other jurisdictions will likely strengthen compliance expectations for payment providers. Within the European Union, proposed enhancements to PSD2 are expected to have a stronger focus on fraud, financial crime, and customer security. Technical requirements on customer identity and authentication are to be strengthened and payer protection through refined chargeback procedures are expected to be included.

Judging from banks' experience, the reputational damage from failure by PSPs to manage such risks appropriately can be considerable. In addition to regulatory attention, activities on payments platforms have attracted notice from watchdog organizations for reasons beyond financial crime, enhancing the importance of managing reputational risk effectively. The Institute for Strategic Dialogue and the Southern Poverty Law Center, for example, report that racist

[2] "Beating financial crime: Commission overhauls anti-money laundering and countering the financing of terrorism rules," European Commission press release, July 20, 2021.

groups continue to use mainstream payment platforms for fundraising. Press reports of such activities can prompt activist responses from the broader public—even boycotts of brands and companies that fail to meet social responsibilities.[3] Particular instances of misuse may be technically within the law but can cause serious damage to the brand and to the trust of clients nonetheless.

The control mechanisms for managing financial-crime risks thus have implications for the business model, customers, and internal operations of PSPs. The effects are determined by how the controls are set up. No miracle technological solution exists or will soon be developed to resolve these issues. For the most part, banks and PSPs continually evaluate their internal processes to make them more resilient, better structured, and more integrated. The tools, platforms, and systems they adopt in this process are simply the enablers. This article lays out the key principles for designing a strategy that PSPs can use to their advantage in managing financial-crime risks while preserving and enhancing the PSP customer experience.

## Mobilizing to manage financial-crime risks

As PSPs rethink their approach to managing financial crime, they can apply three core design principles.

1. *Build a proportionate framework.* The control framework should be proportionate to the overall business model. Organizations will have to decide which risks they are willing to accept versus those that will be outside their risk appetite. For example, some AML and KYC issues relate to an important advantage of the payment business model: the streamlined customer experience, including quick onboarding, verification, and transactions.

2. *Challenge the traditional control environment.* PSPs can challenge the efficacy of the control environments and frameworks of traditional banks. More controls do not necessarily mean better protection from financial crime for PSPs. By identifying this tension, PSPs will be able to think more creatively and actively develop solutions both to meet regulatory requirements and support their customer experience goals.

3. *Be continuously proactive toward exposures.* PSPs should do more than react to the regulatory requirements and attention from regulators. To respond effectively to their exposures, PSPs will have to anticipate risks and build protections into the design of core services and products. They must also continuously update their approach, swiftly adjusting their regular and ad hoc software releases, for example, to address the changing fraud threat landscape. Ultimately, this strategy will help PSPs design next-generation mechanisms to counter financial crime.

## Five pillars for managing financial-crime risks

The success of digital-payments channels has challenged the industry to manage the associated nonfinancial risks—in particular, financial-crime risk. PSPs are in a good position to manage these risks effectively, as they can build on the prior experience of banks, adopting the positive lessons and avoiding practices that have not worked.

In shaping their strategy to fight financial crime, PSPs can consider five core pillars (exhibit).

The five pillars for fighting financial crime are designed to capture the inherent strengths of PSPs and build on lessons from the experience of industry participants. Using mainstream and advanced technological capabilities, PSPs are well positioned to challenge the standard anti–financial crime approaches and reengineer ineffective industry practices. The staged rollout of this journey begins with a risk assessment and the definition of the risk appetite before it proceeds through the fuller set of actions:

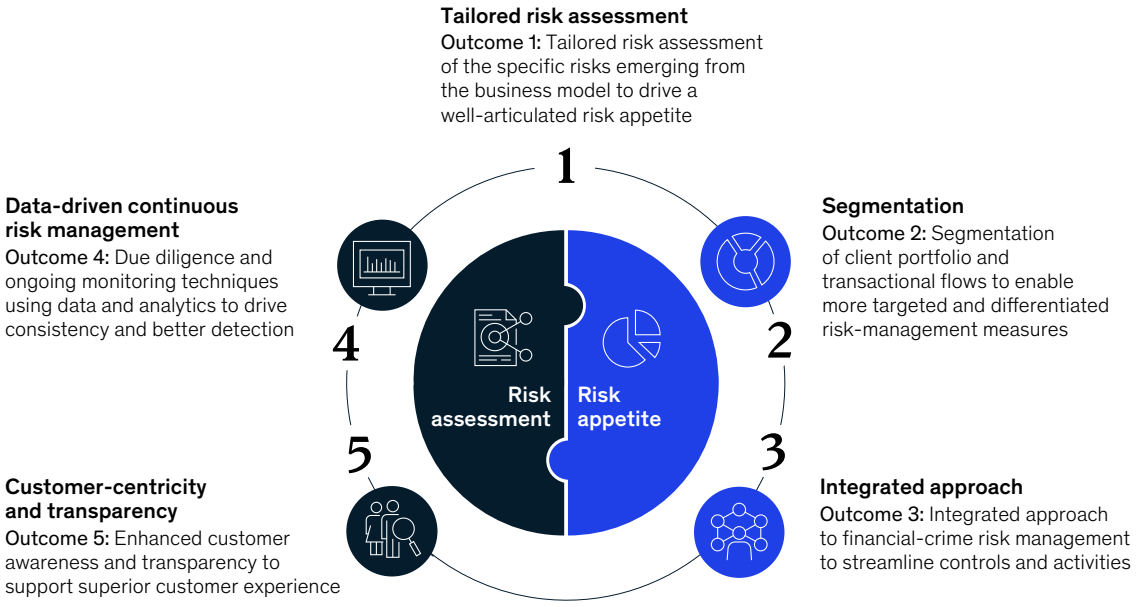
**1. A tailored risk assessment driving risk appetite**

A tailored risk assessment of the specific risks emerging from the business model is needed to drive a well-articulated risk appetite. PSPs and other service providers to consumers and merchants

[3] Olivia Solon, "Tech platforms continue to let US-based hate groups use them to make payments," NBC News, October 27, 2020.

Exhibit

## Five core pillars can shape the anti–financial crime strategy for payment service providers.




need to identify the specific potential risks they face and build the appropriate internal infrastructure to protect their business. Each PSP will have to consider the distinct typologies and scenarios of the financial-crime risks to which their business models are exposed. An e-commerce platform may, for example, attract fraudulent merchants that collude with customers to transfer illicit funds. Platforms providing cross-border payments may be used to bypass controls adopted by other institutions.

Effective risk identification entails much more than creating high-level definitions and theoretical assessments of risks. It should involve detailed, data-driven analyses of the merchants' role in the payment value chain, the types and segments of customers within their portfolios, their business models and product offerings, and their transaction flows in terms of volumes and types. The analysis can then be used to set the risk appetite and associated tolerance thresholds, to monitor on an ongoing basis. All of this data should be continuously captured and updated, with triggers embedded in the controls when divergence from the risk appetite is identified.

### 2. Segmented client portfolio and transactional flows

Segmentation enables more targeted and differentiated risk management measures. Pursuing the objective of detecting and stopping prohibited transactions and bad actors often comes at high operational cost. Enterprises do not have enough resources to monitor all transactions and customers equally. The idea behind an appropriate risk-based approach is that PSPs should focus more comprehensively on the small percentage of potentially risky transactions and customers. To do this, institutions will need to develop more nuanced segmentation models, based on real-time, up-to-date data to enable targeted detection and a clear ranking of customers and transactions, from lowest

to highest risk. Such a model would consider not only historical transactional data and static customer records in KYC files but also forward-looking datapoints and external data on bad actors.

**3. Integrated, streamlined controls and activities**

PSPs are highly skilled in developing unified infrastructure and integrated teams across risk types—such as fraud, AML, sanctions, and cyberrisk. Their experience has led to quicker decision making while increasing the effectiveness of the respective controls. PSPs have a less siloed structure in this respect than banks. They can use data from each of these related risk disciplines to inform decision making across processes. They should invest in building solutions that can bring together several controls, ideally ensuring that journeys are "compliant by design."

This may involve the use of data and controls for fraud detection and AML transaction monitoring to identify trends that suggest correlations with money laundering and other prohibited activities. It may also involve integrating the various anti–financial crime controls that apply to certain products or services, in order to avoid customer friction and enhance overall effectiveness. This approach could result in better outcomes, as these risks are inherently linked.

**4. Data-driven, continuous risk management**

The use of innovative and existing technologies and data will enable PSPs to roll out continuous and targeted monitoring solutions, the design of which is informed by tailored data analysis rather than expert judgment only. PSPs should aim to design intelligent automated processes, applying machine learning and analytical approaches where they make the most sense. These tools can dramatically improve effectiveness, reducing false-positive rates and reliance on labor-intensive processes.

Leading firms, for example, are adopting a live, always-on model to assess the risk of customers throughout their life cycle. The analytics-driven approach draws on both dynamic data, such as transaction flows, and static data, such as customer segments and geographical risk rankings, to better risk-rate customers. Some firms are developing AI models that learn from the experience of historical investigations to segment and prioritize alerts. Many are also deploying machine learning to drive dynamic optimization of transaction-monitoring scenarios. Utilizing analytics is not only about deploying machine learning and artificial intelligence; often, basic descriptive analyses using customer and transactional data (to understand expected customer behavior, for example) can help experts save time, make better decisions, and deploy more targeted controls overall.

**5. Customer-centricity and transparency**

Stronger anti–financial crime controls need not have a negative impact on customer experience. Instead, the controls embedded in the customer journeys can enhance customer experience and trust in the PSP. Critical journeys such as onboarding can be redesigned to improve the customer experience. Features could include faster transaction speeds and enhanced ease of interactions via digital channels, using external data and user-friendly interfaces. Even simple ideas can improve the customer experience, such as making requirements clear, communicating about onboarding progress, or informing them of outstanding documents, for example.

The approach closely ties together the business and risk objectives of the organization. Many institutions have moved to a model where controls relating to financial crime are developed hand in hand with new products or customer journeys and are duplicated across risk types. When designing a new product focused on financing, for example, some institutions ensure that documents requested from clients are shared in advance. These can be reused to assess or mitigate risks or use cases and are differentiated based on their risk profile. Documents required for certain processes (such as ownership structures or income and bank statements for underwriting) can also be used to address financial-crime risks by providing a clear view of ownership structures and

sources of funds. Enabling a holistic view of controls and creating transparency for customers on the requirements and their purpose are paramount to ensuring a smooth customer experience.

## Considerations for a sustainable operating model

The control mechanisms for countering financial crime will likely have implications for the business model, customers, and the internal operations of PSPs. These effects will be determined by how the controls are set up. Policy decisions will balance the dual purpose of higher speed and lower risk—to calibrate, for example, the level and timing of due diligence conducted on new merchants on an e-commerce platform.

Similarly, operational choices will balance customer experience, cost, and responsiveness. An investment in superior technology with a low false-positive rate, for example, should reduce the number of human reviewers and the amount of time needed to review and adjudicate potentially suspicious transactions. Companies will also need to evaluate financial-crime risks as part of key business decision making about products and services and market entry. Compliance should likewise be an integral part of the processes for designing and approving products. E-commerce platforms face risks posed by potentially fraudulent merchants. In this area, PSPs and banks might want to work with these platforms and the customers the platforms serve, to help them fight financial crime in their own offerings. Such collaboration can involve increased data sharing among PSPs, banks, and clients, or it could simply mean better client education about common risks and approaches to mitigate them.

PSPs can expect increasing regulatory scrutiny as incidents of fraud and money laundering surface in connection with their business models. They now have an opportunity to set regulatory agendas before these are set for them, by engaging early on with regulators. Another opportune step would be to engage with market participants to advance collective thinking on these topics. Such an approach will build credibility with both regulators and investors and could give organizations a market advantage.

As PSPs develop their approaches to counter financial crime, they can learn from banks' past reactive approaches. Banks invested millions in detection infrastructure, but many projects proved to be only marginally effective. Banks implemented heavy transaction monitoring to detect money-laundering activity, for example. Often, these produced outcomes with very high false-positive rates—*even as high as 99 percent*. The experience of banks demonstrates that establishing a robust and effective infrastructure for fighting financial crime is a complex undertaking (for more, see sidebar, "A few lessons for banks").

## A few lessons for banks

**The enhanced customer experience** that payments service providers (PSPs) offer holds important lessons for banks as well. Not only do PSPs onboard customers with a minimum of bother but they also offer faster service, along with an extra level of security for purchases. Now that PSPs are turning their attention to financial-crime risks, the solutions they develop based on superior technical skills will no doubt be designed to protect that customer experience advantage.

Banks can use PSP-style solutions to improve their own customer experience and to counter financial crime more effectively. They can consider, for example, deduplicating and streamlining controls across different areas, leveraging data to improve analytical and digital approaches, and keeping customer profiles up to date proactively through transparent customer journeys.

In launching their own efforts, PSPs can utilize lessons from this experience to avoid wasting resources on ineffective approaches:

— *Embed controls within processes and decisions*. Many PSPs start with a clean slate and possess significant relevant advanced technological expertise. They are therefore in a good position to create compliant-by-design processes with few data or system constraints.

— *Design controls in proportion to the business model*. Often, the increased cost of and focus on controls is a direct function of the business model selected by PSPs—for example, to serve high-risk sectors such as crypto or digital-asset platforms. In such cases, investing in more effective and efficient controls and frameworks is a prerequisite for serving higher-risk parts of the market.

— *Think ahead and focus on data*. Define data requirements early and standardize and start capturing these data. PSPs can make their products and services better and improve the customer experience by drawing lessons from data gathered from control activities such as onboarding and ongoing due diligence (for example, on geographies and sectors served by merchants) and incorporating these into business decision making and product offerings.

— *Always build a business case*. Infrastructure investments should be supported by a clear business case to avoid expensive solutions that are only marginally effective.

— *Plan for complexity*. Establishing a robust and effective infrastructure for managing financial-crime risks is a complex undertaking that should be planned and tracked by dedicated experts.

— *Extract better value from existing controls*. Many anti–financial crime controls can be better utilized. For example, information on business activities and counterparties gathered as part of the onboarding and ongoing due-diligence process can yield insights into company activities that can be used to qualitatively assess their environmental, social, and governance (ESG) profiles and impact. Adverse media screening used to determine the financial-crime risk can similarly be tuned to focus on ESG-related topics.

— *Consider the unintended benefits of a strong financial-crime risk management program*. Strong anti–financial crime capabilities will help enhance the ESG profiles of PSPs.

---

The tremendous and continuing success of digital-payment channels and the business models of payment service providers coincided with the rise of financial crime and is therefore drawing regulatory attention. When PSPs build a response to counter financial crime, they can anticipate rather than react to the changing regulatory environment, taking advantage of their advanced technical knowledge and the prior experience of banks.

**Daniel Mikkelsen** is a senior partner in McKinsey's London office, where **Shreyash Rajdev** is an expert associate partner and **Vasiliki Stergiou** is a partner.

A shorter version of this article appeared in June 2022 in *ACAMS Today*.