McKinsey & Company

Risk & Resilience Practice

The future of the payments industry: How managing risk can drive growth

In the coming year, the payments industry will be confronted with high levels of risk, intensifying regulatory scrutiny, and significant changes in global standards.

This commentary is a collaborative effort by Mariah Braxton, Ismael Hernandez, Tim Natriello, Ishanaa Rambachan, Julian Sevillano, and Vasiliki Stergiou, representing views from McKinsey's Risk & Resilience Practice.

February 2024

The fast-changing payments industry is on the cusp of a new "decoupled era,"[1] in which payments will be progressively disconnected from accounts and dominated by a few winning technologies. In this context, customer expectations will continue to heighten, and payments companies will differentiate themselves by offering their customers outstanding convenience, affordability, and security. For the risk function, this new dynamic offers an opportunity to play an expanded role, moving beyond threat management to serve also as an enabler of and engine for growth.

In this commentary, we consider the future role of the risk function, starting with four differentiating capabilities in risk management, followed by three ways the risk function can support companies in building the payments businesses of the future.

Risk as a mechanism for protection

In a highly competitive payments landscape, customers (and regulators) demand faster and more secure transactions. As a result, strong risk management is increasingly an imperative for payments institutions. Our analysis of the industry's shifting dynamics highlights four areas companies can focus on to gain a competitive edge.

1. Strengthening risk processes to maintain regulatory compliance

In addition to increasing the focus on fraud mitigation, payments service providers (PSPs) could be looking to modify their risk management programs to protect their revenue and improve regulatory compliance. This may include enhancements to issue management, due diligence processes, risk appetite setting, or risk identification processes.

Governments and regulators globally have noted the industry's shortcomings when it comes to risk management. In March 2023, the United Kingdom's Financial Conduct Authority (FCA) sent a letter to PSP CEOs detailing its concern over a perceived lack of sufficiently robust controls. Specifically, the regulators cited that the deficit might present a risk to their customers and to the integrity of the financial system.[2] Similarly, in the United States, the Department of Justice (DOJ) and the Federal Trade Commission (FTC) have taken enforcement actions against more than ten payments firms in the past three years, resulting in over $200 million in fines. Insufficient merchant due diligence and poor adherence to industry standards were among the main drivers of the regulatory action.

Meanwhile, the US Consumer Financial Protection Bureau (CFPB) has focused enforcement actions on negative customer impacts, including deceptive enrollment programs, erroneous charges, expensive exit fees, and fees on inactive accounts.

When enforcement actions are issued in the form of consent orders, it typically takes institutions more than five years to close, and at an annual run rate of over $100 million for the largest players. Further, there are longer-lasting impacts: after remediation, risk and compliance programs typically cost 35 to 50 percent more than comparable peer programs. This is because enhancements are often made haphazardly to close gaps, rather than systematically in line with a broader risk management strategy. The intensity of remediation efforts can also negatively affect employees and morale, from distracting senior executives from other priorities to pushing employee turnover above 30 percent for some functions. Finally, consent orders can inflict significant reputational damage. Through more proactive risk management processes, many of these potential liabilities could be reduced or even avoided.

To strengthen risk management, payments services providers can take steps that include enhancing processes, focusing sharply on industry standards, addressing customer impacts, proactively managing risks, investing in remediation and compliance, and maintaining a strong corporate culture. By prioritizing these actions, firms can reduce potential liabilities, protect their customers, maintain

[1] "On the cusp of the next payments era: Future opportunities for banks," McKinsey, September 18, 2023.
[2] "Dear chief executive officer: FCA priorities for payments firms," Financial Conduct Authority, March 16, 2023.

regulatory compliance, and safeguard the integrity of the financial system.

2. Fighting fraud while enhancing the customer experience

The incidence of fraud and scams, such as account takeover (ATO) and authorized push payment, or APP (when someone is tricked into sending money to a fraudster), are growing at alarming rates. In 2022, the FTC reported that scams were up 49 percent from 2021, with consumers losing nearly $8.8 billion.[3] At the same time, consumers expect that payments providers will protect—and reimburse—them when fraud occurs. As a result, fraud protection has become critical to ensuring payment system integrity, managing the customer experience, and protecting companies against reputational risk.

The solution to this challenge is conceptually simple: organizations need to do better at detecting and preventing fraud and minimizing customer inconvenience and disruption. Yet many organizations are challenged with putting these imperatives into practice. The most successful firms are deploying multiple authentication methods. For example, they might combine biometric identification, real-time monitoring using AI/machine learning (ML), and out-of-pattern analysis to detect suspicious activities. To minimize impacts on customers, the best companies embed these solutions seamlessly into their workflows and processes.

Advanced tools work best when paired with open communication and transparency with customers. This includes taking proactive steps to raise awareness about fraud, which fosters confidence and improves the overall customer experience.

3. Building operational resilience to prevent failures

In 2024, new rules and regulations could accelerate PSP action on operational resilience. In the United Kingdom and the European Union, regulators have provided more prescriptive guidance, including FCA Policy Statement PS21/3[4] and the European Union's Digital Operational Resilience Act (DORA).[5] These new requirements compel payments firms not only to address their own operational resilience but also to manage interdependencies in the service delivery chain. As a result, we expect many PSPs to widen the scope of their risk management program beyond internal processes to the entire transaction flow.

Notwithstanding regulatory attention, PSPs themselves are increasingly focused on operational resilience throughout the value chain because of the potential impact on their business. Disruptions from externalities, such as cyberattacks, to internal failures, such as outages, often result in heavy financial and reputational costs. For example, more than 60 percent of operational failures result in at least $1 million in total losses.[6]

To avoid these kinds of liabilities, payments companies need to take concerted action to bolster their operational resilience. A good place to start would be to conduct a top-down review of operations, including those provided by third-party service providers, to define the critical business services (CBS) and processes. After this identification, firms can evaluate and rank risks associated with continuity and redesign risk management practices to enhance resilience—for example, creating centralized units for monitoring and testing.

[3] *Federal Trade Commission business blog*, "FTC crunches the 2022 numbers. See where scammers continue to crunch consumers," blog entry by Lesley Fair, February 23, 2023.
[4] "FCA policy statement: Building operational resilience," Federal Conduct Authority, March 31, 2022.
[5] "Digital finance: Council adopts Digital Operational Resilience Act," European Council press release, November 28, 2022.
[6] "Uptime Institute's 2022 Outage Analysis finds downtime costs and consequences worsening as industry efforts to curb outage frequency fall short," Business Wire, June 8, 2022.

4. Improving credit and collections processes to address a new normality

During COVID-19, issuers and wallets reported low delinquencies, partly because of excess cash in cardholders' accounts that was associated with delayed spending, relief funds, and low interest rates. Further, many credit models were built and trained using data that assumed low inflation and a different macroeconomic environment than is prevalent today.

As delinquencies increase to almost pre-COVID-19 levels and as out-of-date credit models prove unreliable, many issuers and wallet providers are exploring new credit and collection practices. Leading players in the ecosystem are implementing more comprehensive credit risk management processes and establishing dedicated collections teams, trained to assess clients' situations and offer appropriate settlement options. These strategies, when effectively implemented, can improve credit and collection practices, reduce credit risk with improved underwriting, and bolster customer satisfaction.

Some players are experimenting with alternative data sources, combined with AI/ML, to supplement credit scoring models. One of these alternative data sources could be other players in the payments value chain. This data can be fed into risk analytics to enhance decision making. For example, an issuer can use a PSP's data on the average monthly ticket size of a specific business to make a dynamic assessment of commercial credit lines. Companies can also use alternative data sources to enhance credit models and unlock new approaches to managing credit risk exposure.

As the risk function continues to increase its relevance among payments companies, players that make proactive efforts to improve their fraud prevention approaches, comply with regulators' expectations, enhance their operational resilience, and adjust their credit and collections management to a new standard are likely to boost their prospects for outperformance.

Risk as a lever for growth

The risk function has historically focused on downside risks, and rarely has it been seen as a potential lever for growth. As we move into an era of heightened customer expectations, pressures on fees, and intense competition, companies should consider a reset, with risk capabilities seen as a potential driver of value creation and differentiation. Our assessment of the industry's focus suggests three areas where companies could leverage risk as a partner to further generate a competitive advantage.

1. Growing profitably into new markets or segments

Given intense competition on merchant networks and fees, some players are reconsidering markets where profitable growth may be possible but has previously exceeded most institutions' risk appetite. Industries that have been historically underserved, such as gaming, could represent a significant opportunity if risks are properly balanced.

To serve these markets, some leading payments companies are investing in specialized underwriting and fraud prevention tools, as well as creating products tailored to these unique segments. Such actions can help PSPs more accurately assess the risk exposure and needed mitigating actions presented by the specific type of high-risk customer. Ultimately, this enables PSPs to provide higher-risk customers with more compelling offers because they are relying on a more precise view of the customer's specific risks, rather than broad generalizations.

While the risk function might historically have steered PSPs away from riskier segments, institutions with a strong risk management approach could reevaluate their risk appetite, mature their risk rating and scoring capabilities, and reassess the risk of new products. Under this approach, the risk function would act as a partner to the business, thinking strategically about the trade-offs required to serve riskier segments and potentially enabling the business to gain a first-mover.

2. Seeing risk as a product to better serve merchants

With the FTC estimating that US fraud losses have grown by more than 60 percent year over year since 2019, the impact of fraud can be felt beyond the financial-services sector, as businesses in all industries suffer when there is fraud. Not all merchants, however, may be prepared to deal with the increased pressure fraud places on their business.

PSPs can act to prevent fraudulent losses and losses from legitimate transactions that are inaccurately flagged by productizing and commercializing their risk management capabilities as a service. Risk as a service (RaaS), the largest segment in fraud solutions, is now a $10 billion market and is growing at a rate of 12 to 14 percent a year. While third parties have been dominant up to now in the RaaS market, more PSPs are entering the space, offering merchants fraud protection, charge-back protection, dispute management, and data enrichment.

PSPs are uniquely placed to commercialize their risk management capabilities and offer them as a service, enabling them to partner more closely with their merchants.

3. Embracing servicing ops to improve

As digital payments continue to replace cash, PSPs have expanded their servicing operations teams, including fraud operations. But while many teams have grown and evolved, some practices have remained unchanged. Today, many servicing processes are highly manual, often involving multiple data handovers across different platforms and teams. This can result in a poor customer experience, errors, delays, and inconsistencies.

Additionally, PSP internal platforms are often stand-alone technologies. This lack of interoperability means systems cannot work together and data does not automatically flow. As a result, it is common for the same bank to request the same information from customers multiple times.

Leading payment players see an opportunity to improve the productivity and effectiveness of their operations through technologies, including AI, intelligent workflow automation, and generative AI. Early adopters are leveraging these technologies to make online interactions more conversational or help phone agents create scripts for problem resolution. Leading institutions are also backing up these technologies with improved servicing operations teams and by reviewing policies and procedures on a regular basis. These servicing operations improvements not only have the potential to cut costs but also they are commonly associated with an increase in customer satisfaction, which ultimately could prevent attrition.

In the coming months, the payments industry will be confronted with high levels of risk, intensifying regulatory scrutiny, and significant changes in global standards, especially in key markets such as Europe, the United Kingdom, and the United States. In this context, players in the payments value chain should not just react but proactively spearhead new risk management strategies. This will mean both protecting the business and partnering with it to identify growth levers that can enhance performance and boost differentiation.

Mariah Braxton is a consultant in McKinsey's Washington, DC, office; **Ismael Hernandez** is a consultant in the New York office, where **Tim Natriello** is an associate partner; **Ishanaa Rambachan** and **Julian Sevillano** are partners in the Bay Area office; and **Vasiliki Stergiou** is a partner in the London office.

Designed by McKinsey Global Publishing