VIEWPOINT

FROM RISK TO RESILIENCE: TRANSFORMING PAYMENT FRAUD DETECTION WITH AI

As the speed and complexity of financial crime continue to grow, banks and payment providers face mounting challenges in detection, prevention, and response. Real-time payments, mobile banking, and new consumer expectations have created opportunities for fraudsters to exploit gaps in outdated infrastructure and siloed systems. At the same time, evolving regulations and rising demands for customer protection are shifting the burden of reimbursement to financial institutions.

Infosys®
Navigate your next

This paper explores the emerging dynamics of financial crime in the payments space, with a focus on how artificial intelligence (AI), machine learning (ML), and consolidated data infrastructures are transforming the fight against fraud and money laundering. It also examines the limitations of current systems, from disjointed customer journeys to legacy IT barriers, and presents strategic considerations for financial institutions seeking to modernize their defenses. From integrated fraud and anti-money laundering (AML) platforms to AI-driven behavioral analytics and real-time risk assessments, the paper identifies the tools and trends reshaping financial crime prevention. Finally, it offers forward-looking insights into institutional collaboration, regulatory adaptation, and the importance of explainable AI (XAI) as well as customer trust in building resilient systems for the future.

Introduction: Payment Fraud and the Role of Technology

The evolving landscape of payments and banking presents both opportunities and significant challenges, particularly in combating financial crime. As fraudsters and money launderers employ increasingly sophisticated tactics, financial institutions face growing pressure to bolster their defenses while maintaining a seamless and superior customer experience. The rise of real-time payments and digital wallets has inadvertently opened new avenues for fraudsters to exploit opportunities arising from faster transaction speeds. Instant payments, now a norm in many parts of the world, help accelerate fraud due to the irreversible nature of completed transactions. Banks can no longer rely on payment delays as a fraud mitigation tool. They must adopt automated solutions and data-driven responses to address threats as they emerge. This shift requires advanced technology and robust data capabilities to accurately detect and block fraudulent payments in real time without compromising customer experience.

Technology, particularly artificial intelligence (AI) and machine learning (ML), is crucial in this ongoing fight. The speed and sophistication of financial crime often outpace human defense capabilities. However, technology is advancing significantly in both detection and response, with key advancements in detection including:

External Document © 2025 Infosys Limited

- AI-powered monitoring systems that improve detection accuracy and reduce false positives
- Real-time transaction monitoring that enables instantaneous analysis of millions of transactions
- Large transaction models, capable of analyzing billions of global transactions to enhance detection rates
- Advanced network analytics that uncover complex criminal networks often missed by traditional systems
- Behavioral analytics, which create unique user profiles that are difficult for fraudsters to replicate, helping identify anomalous behavior in real-time payment environments

On the response side, autonomous AI agents and intelligent automation systems hold promise in streamlining investigations and helping banks adapt to regulatory changes. Automated suspicious activity report (SAR) filing is also becoming more prevalent due to technological advancements. Banks are actively working to close the technology gap with criminals, who often adopt new tools and methods much faster, sometimes several months ahead. They also need to improve data quality, enhance integration across the organization, and strengthen collaboration between anti-money laundering (AML) and fraud teams. Managing the end-to-end customer lifecycle and ensuring strong AI governance are also emerging as crucial areas of investment and focus.

Infosys' Role in Enabling AI-driven Fraud Prevention Solutions

Infosys plays a critical role as both a systems integrator (SI) and operations partner for global financial institutions. We help deploy AI-driven fraud prevention solutions tailored to client needs. Demonstrating our capabilities, we have reduced manual verification efforts by 40-50% in check fraud cases by integrating computer vision (CV), behavioral analytics, and ML. Our proprietary omnichannel fraud analytics platform correlates transaction patterns across channels to lower false positives and accelerate investigations.
In retail banking, Infosys' AI solutions helped recover over US $400,000 in point-of-sale (POS) fraud by integrating transaction monitoring with anomaly detection. In chargeback operations, AI-driven alert

External Document © 2025 Infosys Limited

prioritization and automated workflows significantly reduced manual review time, boosting operational efficiency and enhancing fraud mitigation. While AI and ML are essential tools, human oversight remains essential to ensure robust, context-aware decision making in a high-stakes environment where both regulatory compliance and loss prevention are critical.

Operating Models: Integrating Fraud and AML Functions

Traditionally, many banks have managed fraud and AML as separate functions, each shaped by distinct historical drivers. AML has primarily been compliance-driven, focused on meeting regulatory requirements. Fraud prevention, while gaining prominence in recent years, has been more risk-based and driven by the need to prevent losses, provide secure services, and maintain customer trust. However, there is a growing recognition that fraud and AML are increasingly interconnected.
AML regulations emerged in response to primary crimes like fraud, as criminals must launder proceeds to legitimize illicit funds. Common datasets and transaction patterns are often observed across both domains. For instance, certain card usage behavior might simultaneously indicate both fraud and money laundering.

Therefore, having a common platform, shared datasets, unified transaction pattern analysis, and potentially integrated case management systems offer banks significant benefits. While specific skill sets are still necessary to address the distinct demands of AML (including regulatory compliance) and fraud (such as cyber prevention, event logging, and IP address analysis), effective financial crime prevention depends on close cooperation and a unified platform.

Systems integrators like Infosys play a key role in enabling this integration. We help banks deploy AI-powered data lakes to unify siloed transaction streams and customer profiles, thereby reducing duplicate alerts through shared analytics.
Key strategies include implementing middleware to bridge legacy batch-oriented AML systems with real-time fraud detection systems, and designing cross-functional dashboards that merge risk assessments from both compliance and fraud teams.

However, integration challenges remain. These include organizational silos between compliance-focused AML teams and loss-focused fraud teams, which require cultural realignment and organizational change. Furthermore, banks are often burdened by legacy IT systems that are difficult and costly to integrate. In fact, a significant portion of implementation costs are attributed to incompatible data formats and processing gaps.

Balancing Regulatory Compliance and Customer Experience

One of the most significant dilemmas for banks is balancing stringent fraud controls with customer expectations for seamless transactions. While friction is sometimes necessary to prevent fraud, banks aim to minimize its impact on the overall customer experience.
For DNB, Norway's largest bank, a key strategy is to automate and employ data-driven responses in the background. The goal is to avoid burdening customers with fraud prevention measures unless there is a high likelihood of its occurrence. For example, DNB's 2025 report on threats and trends reveals that the bank achieves a 96% prevention rate on phishing attempts by automatically blocking authentication devices upon suspicious login attempts, and then proactively contacting the customer to reset their method of access. Such behind-the-scenes prevention measures aim to turn a potential fraud attempt into a positive customer experience when the bank successfully intervenes on their behalf.

Interestingly, surveys carried out in Norway suggest that customers are often willing to accept some friction if it enhances their sense of security. This indicates that the pursuit of entirely frictionless experiences might be overemphasized. A balanced

External Document © 2025 Infosys Limited

approach, potentially allowing customers to choose their desired security level within banking applications, could be beneficial.

Despite heavy investments in fraud prevention and regulatory compliance, banks continue to face significant compliance gaps, evidenced by persistent billion-dollar fines. Three systemic issues contribute to this paradox:

1. **Limitations of legacy systems:** A significant portion of compliance spending goes towards maintaining outdated systems that cannot support modern AI/ML detection or event-driven architectures for operational efficiency.
2. **Delays in remediation:** The average time to resolve supervisory findings is increasing, particularly for smaller banks, leading to a large backlog of unresolved issues. Staffing shortages in compliance functions further compound this problem.
3. **Regulatory complexity and data fragmentation:** The ever-evolving and fragmented regulatory landscape, coupled with siloed data across bank functions, makes unified fraud and AML efforts challenging. Banks often find themselves perpetually playing catch-up with the rapid evolution of both regulatory requirements and fraudster tactics.

Despite advanced fraud prevention techniques, there is growing pressure on banks to take greater responsibility for reimbursing customers who fall victim to scams. For example, in the UK, some banks are now required to refund victims of authorized push payment (APP) fraud. While empathy for victims is high, some argue that banks should not be held accountable to customers for all fraud-related losses. Fraud prevention is viewed as a value chain where the 'aware customer' is the first link. If customers feel no responsibility, the quality of this first line of defense diminishes, potentially leading to false claims and rushed investigations due to short reimbursement deadlines. This debate risks shifting focus from cooperative fraud prevention efforts to arguments over who bears the loss, ultimately benefiting organized criminals.

Norway's BankID Initiative: A Case Study

Norway's BankID system is a notable example of a secure digital authentication model. It functions as a single sign-on system across banking, government services, online retail, and e-commerce, reducing fraud risk while improving convenience. A unique aspect of BankID is its connection with national Social Security numbers, which helps prevent synthetic identity fraud. While effective in preventing phishing attempts, stolen BankID credentials can lead to serious identity theft.

Historically, banks issued BankIDs that provided them access to valuable user data. Although banks cannot see the usage of BankID in other user interfaces due to competitive confidentiality, the system remains a strong fraud prevention tool due to its unified approach to identity verification. Moving forward, BankID is evolving into a separate service entity, which will enable it to collect more user data points and build its own fraud risk engine. This will allow for better cross-platform login analysis and enhanced fraud prevention in the future. Similar common identification systems exist in Sweden and Denmark, facilitated by their smaller populations.

Collaboration and Information Sharing

Given the interconnected nature of the financial system, enhancing collaboration and information

External Document © 2025 Infosys Limited

sharing is crucial for combating fraud more effectively. Strategies include bilateral cooperation with law enforcement, which has shown significant success in Norway. There is also a growing momentum to automate and broaden information sharing with other financial institutions, telecommunication companies, and government bodies like the police and the Serious Fraud Office (SFO). European initiatives are also exploring what types of information should be shared within payment transactions.

However, a key challenge in broad information sharing is ensuring high data quality. Banks may have varying standards for data input, which can lead to false positives if not managed carefully. Strict adherence to data quality standards and a common understanding of what information to share are essential for successful automation and intelligence sharing. It is widely held that shared information, including intelligence-level data beyond confirmed cases, can empower banks to prevent frauds they might not otherwise detect with their isolated data foundations.

Advancements in Authentication Technologies

Authentication technologies are rapidly evolving, with a significant advancement being the layering of sophisticated customer behavior analytics into the mix. This approach is inherently challenging for fraudsters to replicate, as it identifies fraudulent behavior and suspicious activities by analyzing granular, dynamic customer patterns rather than relying on static credentials. Financial institutions are advised to follow key design principles:

- Proportionate frameworks: Build dynamic thresholds to assess acceptable risk levels and apply flexible, risk-based authentication. In Europe, the revised Payment Services Directive (PSD2) requires Strong Customer Authentication (SCA) for electronic payments but allows exemptions based on contextual risks, such as low-value transactions or low fraud rates. This supports a more intelligent and proportionate approach to security.
- Challenging traditional controls: Adopt a layered approach that focuses on intelligent, context-aware security measures rather than adding more controls.
- Continuous, proactive exposure management: Banks must move beyond merely reacting to regulatory requirements by anticipating threats to proactively embedding protection into the design of core services and products. Weaving security into the product design ensures ongoing adaptability and resilience against evolving threats.

External Document © 2025 Infosys Limited

Combating Social Engineering and AI-generated Fraud

Social engineering and AI-generated fraud, including deepfakes, are becoming increasingly sophisticated and difficult to detect. Financial institutions primarily focus on the security of authentication methods, apps, and internet banking as they monitor user behavior and anomalous transaction patterns within their services. However, the quality and volume of false information presented to customers are rising dramatically. AI plays a dual role in this landscape. While it enables fraudsters to create high-quality, automated attacks through AI-powered phishing emails and voice cloning, it also helps banks build robust defenses and improve predictive capabilities. Specialized preventative measures on the customer side, specifically for deepfakes, may not always be the primary focus for banks as this often falls to broader cybersecurity. Banks are primarily concerned with whether a customer is tricked into making a payment, regardless of how the manipulation occurs. Since they cannot control how customers use websites, social media, email, or messaging apps, they are unable to directly prevent such influence. Their responsibility lies in monitoring the use of banking services, staying aware of evolving threats, and being ready to investigate suspicious activity. The priority is not to block every possible manipulation but to remain alert and responsive when fraud occurs. At the same time, the rise in sophisticated deception demands robust AI governance and critical human oversight. As human judgment remains central to any complex detection or response strategy, there is a continuous need to assess and mitigate biases within AI models as well as ensure rigorous quality controls for all AI deployments.

Emerging Future Trends

Financial crime prevention is evolving rapidly, with several key trends poised to materialize the future of the industry:

- AI-driven proactive defense: Almost all banks will deploy AI/ML for AML and fraud, utilizing large transaction models for real-time analysis and significantly reducing false positives. AI agents are expected to autonomously investigate and resolve cases, allowing human teams to focus on strategic oversight.
- Unified fraud and AML systems: The integration of fraud and AML into unified platforms with data lakes will become more common, eliminating duplicate alerts. Forward-looking financial institutions have already begun this transition.
- Crypto and regulations: Stricter rules for decentralized finance (DeFi) platforms and cross-chain crypto transactions will emerge, necessitating blockchain analytics to trace crypto flows.

External Document © 2025 Infosys Limited

- Infrastructure modernization: Banks must modernize their infrastructure, replacing legacy systems with cloud-native, event-driven architectures that can support the real-time nature of payments and fraud.
- Explainable AI and governance: There will be an increasing need to build robust, explainable AI (XAI) and governance frameworks to manage the deployment of AI, measure biases, and ensure quality controls.
- Upskilling teams: Staff involved in operations will need to be upskilled to align with advancements in architecture, evolving fraudster tactics, and integrated systems.
- Increased institutional collaboration: Similar to initiatives in the Nordic region, institutional efforts to share data and collectively fight financial crime across global financial organizations will become more prevalent.

Beyond these technological and operational shifts, the very nature of societal trust will be challenged by the volume and quality of fraud attempts. Digital information will appear more convincing, driving individuals to critically assess the content and the context of how they receive information. Furthermore, customer protection regulations, while sympathetic to victims, might inadvertently reduce individual responsibility, potentially leading to more false claims and shifting the focus away from preventative cooperation.

There is also a worrying trend of increased violence and organized crime involvement in fraud cases, with instances of coercion, assault, and kidnappings related to financial deception being observed. This emphasizes that while technology is a critical part of the solution, effective data sharing, cooperation between institutions, and a heightened societal awareness are equally vital to combat this evolving and escalating threat to financial security and public trust.

Conclusion: The Road Ahead

The fight against financial crime in the payments industry demands a multi-faceted approach. As digital payments accelerate, so does the scale and sophistication of fraud and money laundering. Technology, particularly AI and advanced analytics, is no longer an option but a necessity for robust detection and response mechanisms. Significant challenges persist in integrating historically siloed fraud and AML functions, stemming from organizational complexities and entrenched legacy systems. However, the compelling benefits of a unified approach are clear, especially when leveraging common data platforms, shared analytics, and collaborative efforts.
Banks must strategically balance stringent controls with customer experience, potentially by automating responses in the background and offering customers more choices in their security settings. The Norwegian BankID initiative exemplifies how a shared, secure authentication system can significantly enhance fraud prevention across an ecosystem. Ultimately, success in this ongoing battle will depend on continuous technological innovation, strategic organizational alignment, and a proactive stance against evolving threats.

External Document © 2025 Infosys Limited

About the Authors

Terje Aleksander Fjeldvær
SVP - Head of Financial Crime & Sanctions, DNB

Terje Aleksander Fjeldvær is a former Police Superintendent from the Norwegian police where he was a specialist within investigation of economic crime. He started working in the largest financial institution in Scandinavia, DNB, in August 2015 as a fraud investigator. Since September 2016 he has had the global professional responsibility for handling of fraud cases against DNB Group and the groups customers, including digital fraud. From January 2022 he in addition to fraud has the first line responsibility for sanctions transactions- and customer screening. He is one of DNBs spokesperson on fraud and digital safety and international sanctions.

Vivek Dwivedi
Regional Head, Infosys

Vivek Dwivedi leads a $450M P&L portfolio encompassing Payments, Exchanges, Market Infrastructure, and Banking for the North America region. He has close to 30 years of expertise in driving business outcomes for Fortune 500 companies through digital transformation initiatives. An expert in cards and payments, banking, investment management, and retirement services, Vivek operates at the intersection of business and technology

---

Amit Khullar
AVP, Industry Consulting Leader, Infosys

Amit Khullar leads the Industry Consulting team for the Financial Services segment at Infosys, specializing in Banking, Compliance, and Risk Management. With over 25 years of experience in business consulting and large-scale technology transformation initiatives, Amit has played a key role in advising financial institutions on financial crime prevention, regulatory compliance, and AI-driven risk management solutions.

External Document © 2025 Infosys Limited

For more information, contact askus@infosys.com

Infosys®
Navigate your next

© 2025 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.