KPMG

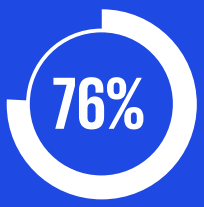
Fighting fraud in payments with AI

Leveraging AI solutions for next-generation fraud detection and prevention

kpmg.com

The Federal Trade Commission reports that US consumers lost more than $12.5 billion to fraud schemes in 2024—nearly quadruple the $3.5 billion lost just four years earlier.[1] Financial institutions (FIs), under pressure to strengthen their defenses against the growing threat, are increasingly turning to generative artificial intelligence (GenAI) to identify and mitigate fraud patterns: KPMG LLP found that 76 percent of FI survey respondents viewed fraud detection and prevention as their firm's top application for GenAI, with 83 percent expecting their firm to increase GenAI investments by at least 50 percent.[2]

These systems, which can analyze robust data sets in real time, have shown great promise in identifying and mitigating fraud patterns. Still, the journey to combat AI-driven fraud is fraught with challenges.



76 percent of FI survey respondents viewed fraud detection and prevention as their firm's top application for GenAI.

AI-powered fraud is growing in intensity

Schemes such as audio and video deepfakes, synthetic identities, fake ID documents, and tax-return scams are growing in number and sophistication. Studies suggest that the number of deepfake videos online is increasing by 900 percent annually,[3] underscoring the rapid advancement and accessibility of AI technology for creating realistic fake content.

Deepfakes are used in authorized and unauthorized transactions. In an authorized transaction, for instance, fraudsters could use a deepfake audio clip mimicking a familiar voice to persuade individuals to transfer their own funds. Liability for the transfer rests with the individual, even though it occurred because of fraudulent behavior.

Unauthorized transactions happen when fraudsters engage in transactions using the individual's personally identifiable information, but without the individual's consent. A fraudster, for example, could make unauthorized transactions after opening a credit card account in the individual's name. In this case, the credit card issuer is responsible for the individual's loss because the individual didn't authorize the transaction.

AI-powered fraud can overwhelm traditional detection methods

The financial losses and sophisticated nature of schemes such as synthetic identity fraud necessitate the adoption of advanced AI technologies, including machine learning. This approach is critical for FIs to effectively manage and mitigate risk because it allows for the real-time processing and analysis of large-scale data.

[1] "New FTC Data Show a Big Jump in Reported Losses to Fraud to $12.5 Billion in 2024," Federal Trade Commission, March 10, 2025, ftc.gov.

[2] The generative AI advantage in financial services, KPMG LLP, August 2023.

[3] Memon, Nasir, "Deepfakes, shallowfakes & cheapfakes – Seeing is believing," engineering.nyu.edu, March 28, 2021.

Siloed data hinders detection

A key challenge is the siloed nature of anti-money-laundering (AML) and know-your-customer (KYC) data, which hampers fraud detection efforts. FIs must integrate these data sources to combat AI-powered fraud. Doing so requires cross-departmental teamwork to provide a full picture of customer activity and improve regulatory compliance.

Using AI to stay ahead of bad actors

In the ongoing battle against AI-driven consumer fraud, the financial industry relies on advanced technologies and methods to enhance security and trust. A modern, robust fraud mitigation framework harnesses the power of AI to remain a step ahead of fraudsters.

Next-generation authentication

AI is transforming fraud authentication by leveraging biometrics for advanced protection against payment fraud. Applying sophisticated pattern recognition and anomaly detection, AI algorithms analyze user behavior and biometric data—e.g., facial recognition, fingerprint scanning, voice analysis—in real time to flag suspicious activities. This replaces traditional password vulnerabilities with a robust and adaptive system that evolves to counteract new fraud techniques.

However, a significant challenge lies in the integration of AI-driven authentication solutions offered by disparate vendors. Effectively leveraging data across these fragmented AI platforms is crucial for comprehensive, secure and streamlined authentication. Integrating the platforms enhances security and user experience, proactively blocking fraudulent attempts and ensuring the safety and trustworthiness of financial transactions.

Empowering a top-10 global fintech

In a detailed financial crimes vulnerability assessment for a pre-eminent global fintech, KPMG assessed the company's exposure to financial crimes, noting critical vulnerabilities. Our subsequent provision of actionable insights and strategic recommendations played a pivotal role in reinforcing the client's defenses against financial crimes, significantly improving its security posture.

Trust scoring

AI-driven risk profiling is an alternative to traditional screening methods. By profiling individuals based on their historical behavior, machine learning algorithms can assign a trust score to each. Trust scores are the result of analyzing various factors, including the duration of the customer's relationship with the FI and their transaction patterns. Popular payment platforms use trust scores to offer a more nuanced understanding of transaction risks, which enhances the platform's ability to detect and prevent fraudulent activities.

Feedback data

Incorporating feedback data into AI systems is a vital strategy for improving fraud detection and prevention. This involves analyzing customer complaints, chargebacks, and declined transactions to create a continuous feedback loop that refines algorithms and recalibrates detection rules.

Incorporating feedback data into AI systems is a vital strategy for improving fraud detection and prevention. This involves analyzing customer complaints, chargebacks, and declined transactions to create a continuous feedback loop that refines algorithms and recalibrates detection rules.

Although it can be implemented only manually at present, the feedback approach enables companies to adapt to evolving fraud patterns by leveraging data from multiple sources. While just a few businesses have effectively adopted this method, its long-term application can help to make AI systems more sophisticated and accurate in combatting fraud.

Strategizing for a top-five global bank

KPMG developed a thorough strategy aimed at enhancing the security of payment transactions for a leading global bank. By identifying critical weaknesses in existing processes and controls, we met—and surpassed—industry security standards. Our efforts enabled the bank to better protect itself against the threats pervading the digital payments landscape.

Real-time entity resolution

AI-powered, real-time entity resolution is crucial for effective detection of consumer fraud. AI algorithms match incoming payments against blocklists and watchlists using datapoints such as phone numbers, addresses, emails, and transaction history. This sophisticated matching process allows FIs to identify and flag suspicious activities in real time.

Additionally, AI enhances identity management by analyzing large data sets across various payment channels to understand an individual's digital persona. By building these personas, AI can detect anomalies and label unusual activities as potential fraud, significantly boosting the payment system's security and trustworthiness.

How KPMG can help

KPMG stands at the forefront of the battle against AI-powered fraud. We harness our experience and leading technological solutions to empower FIs in their quest for security. By strategically deploying AI and analytics through the KPMG Modern Data Platform, we magnify the effectiveness of fraud detection and prevention capabilities, transforming challenges into opportunities for security enhancement. Our holistic methodology takes a longer-term view, gearing FIs toward enduring resilience and fortified defenses in the face of the digital era's evolving threats.

Our mission is to navigate clients through the complexities of AI-powered fraud with a suite of tailored services, including:

- AI-enhanced fraud detection and prevention. We've designed our advanced AI and machine learning algorithms to identify and mitigate sophisticated fraud attempts in real time.
- Data integration and analytics. KPMG professionals leverage our experience in integrating diverse data sources—including AML and KYC systems—to enhance the accuracy and efficiency of fraud detection mechanisms.
- Fraud risk assessment and strategy development. We enhance the accuracy and efficiency of fraud detection mechanisms by conducting thorough vulnerability assessments, which help us identify potential fraud risks and develop strategic action plans for mitigation.
- Intelligence sharing. We facilitate the creation and management of platforms for FIs to share insights, data, and leading practices on fighting AI-powered fraud.

Our dedicated approach to bolstering financial security showcases our commitment to addressing the challenges that FIs face. We equip them for the future, helping ensure they remain guardians of their customers' trust and assets.

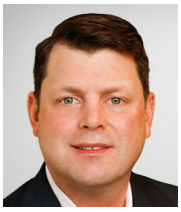
Authors

Dallas Bray
Director

Dallas has more than13 years of experience in data management, data risk, analytics, process governance, operations process improvement and consumer/commercial lending. He has worked with financial institutions in improving data governance and controls, for fraud management, regulatory reporting requirements, and operational efficiency.

Prince Harfouche
Partner

Prince is partner at KPMG who has experience working with financial services clients not only as a former regulator, but also as a market participant and consultant. His diverse background includes working with the SEC and law enforcement agencies to develop fraud detection systems and risk-based surveillance programs, developing leading analytics assets to track risk and controls to address risk management needs for financial services clients.



Matt Miller
Principal

Matt is a principal in the New York office of the KPMG LLP Advisory Services practice and is the U.S. Cyber Security Services Banking industry lead. With 20+ years of experience Matt's focus areas include insider threat and internal fraud, 3rd party risk, quantitative and qualitative risk assessment, and incident management.

We would like to thank: John Berry, Lisa Bigelow, Cynthia Bridges, Christine Chan, Whitney LaBounty, Jim Leach, Megan Marco, and Courtney Trimble for their contributions to this paper.

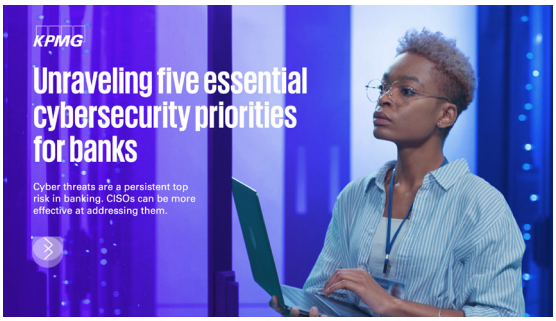
For more information, contact us:

Dallas Bray
Director, Advisory
Financial Services Operations
dbray@kpmg.com

Prince Harfouche
Partner, Advisory
Financial Services
pharfouche@kpmg.com

Matt Miller
Principal, Advisory
Financial Services
matthewpmiller@kpmg.com

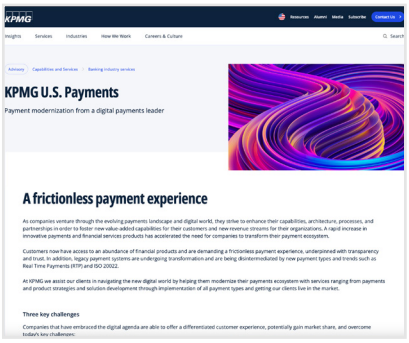
Related thought leadership:



Unraveling five essential cybersecurity priorities for banks

How banks can simplify digital payments

2024 KPMG US technology survey report: The digital dividend



KPMG U.S. Payments

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Please visit us: **kpmg.com** **Subscribe**

DASD-2025-17703