Bottomline

Transforming Fraud Defense for an AI-Driven World

bottomline.com

Securing Trust in a Dangerous Digital Landscape

Financial fraud is undergoing a radical transformation. Enabled by generative AI, fraud schemes are now faster, more personalized, and more difficult to detect than ever before. At the same time, the global regulatory climate is tightening, with proposed mandates placing increased emphasis on operational resilience and fraud prevention accountability.

Rethinking fraud detection and prevention is crucial to earn customer trust and gain market share in this environment. To combat aggressive, sophisticated fraud vectors, it is imperative that banks and financial institutions:

- **Shift to multi-layered, real-time fraud detection** with interconnected layers of authentication, behavioral analysis, and transaction monitoring. This provides broader coverage and earlier detection of complex fraud patterns.

- **Adopt identity-centric security models** where authentication moves from passwords and devices to continuous, behavioral, and biometric verification. By keeping user identity at the core, institutions can significantly reduce account takeovers and session hijacking.

- **Expose internal-external collusion** by closing internal visibility gaps and embedding proactive risk detection through advanced behavior monitoring, system integration, and internal oversight.

- **Engage in fraud intelligence sharing** with banks, fintechs, and regulatory bodies to enhance early detection. Technologies like tokenization and blockchain are enabling real-time, privacy-compliant intelligence exchanges that strengthen ecosystem-wide resilience.

Implemented together, these actions combine to form a comprehensive defense framework. They address not only the technical dimensions of fraud prevention but also the organizational, regulatory, and cooperative factors essential to navigating a volatile threat landscape.

Table of Contents

The Surge of AI-Enabled Fraud

Financial institutions are being confronted with an unprecedented escalation in cyber threats, propelled by the rapid advancement of generative AI and deepfake technologies. These tools have significantly enhanced the sophistication of phishing, business email compromise (BEC), and social engineering attacks, challenging traditional security measures and demanding a more intelligent, adaptive defense posture. Here are five current AI-enabled fraud trends to be aware of:

1. Deepfakes: The New Frontier of Social Engineering

Deepfake technology has emerged as a formidable weapon in the cybercriminal toolkit. A high-profile incident involved a finance worker at a multinational firm who was deceived into transferring $25 million after participating in a video call featuring a deepfake of the company's CFO.[1] Such incidents exemplify the power of synthetic media to manipulate trust in visual and auditory signals—long regarded as verification strongholds.

The prevalence of deepfake-enabled scams is expanding rapidly, and it is easy to see why: it takes just $5 and 10 minutes to create a creditable deepfake.[2] This underscores the urgent need for financial institutions to develop robust countermeasures capable of detecting and neutralizing manipulated media.

47% of organizations cite adversarial advances powered by generative AI as their primary cybersecurity concern.

Source: Global Cybersecurity Outlook 2025, The World Economic Forum

2. Synthetic Identity Fraud: The Fastest-Growing Financial Crime

Synthetic identity fraud—where fraudsters create fictitious identities using a combination of real and fabricated personal data—is the fastest-growing type of fraud, and accounts for 85% of financial fraud cases.[3] Criminals exploit manufactured identities to open bank accounts, build credit histories, and eventually extract substantial sums through loans, credit lines, and other financial services.

The rise of generative AI has significantly amplified this threat. Fraudsters are now using AI to automate the development of highly realistic identity profiles, complete with synthetic selfies, deepfaked identification documents, and fabricated employment histories. These identities can be customized to bypass common verification controls, making detection increasingly difficult.

In the first half of 2024, U.S.-based lenders faced an all-time high risk exposure of $3.2 billion due to synthetic identity fraud—a 7% increase over the same period in 2023.[4] As AI-driven identity creation becomes more accessible and scalable, the threat landscape will continue to evolve, placing additional pressure on know your customer (KYC) and onboarding processes.

3. Mule Accounts: Facilitators of Illicit Financial Flows

Mule accounts, which are used to move, launder, or obscure the origins of illicit funds, are a persistent and growing challenge for financial institutions worldwide. In 2024, nearly 2 million mule accounts were identified by 257 financial institutions across 21 countries,[5] reflecting the global scope and systemic nature of this threat.

AI is playing a dual role in the proliferation of mule accounts. On one front, it enables the creation of vast networks of mule accounts by automating account setup using synthetic identities and deepfaked documentation. On another, AI-driven social engineering tactics—often deployed via social media platforms and messaging apps—are used to recruit individuals, particularly younger users, into acting as unwitting money mules. A recent survey revealed that one in five UK adults have been approached to participate in money laundering activities, with many unaware of the criminal implications of their involvement.[6]

4. Insider Fraud: The Hidden Risk Within

While external threats garner the majority of attention, insider fraud remains one of the most damaging and difficult-to-detect forms of financial crime. Increasingly, artificial intelligence is being used by malicious insiders to obfuscate unauthorized activity, evade detection, and exploit system access.

AI-powered tools can automate the manipulation of transaction records, generate false documentation, and identify blind spots in internal monitoring systems. Additionally, insider recruitment by external threat actors is being facilitated through AI-enhanced reconnaissance. By analyzing internal organizational charts, social media profiles, and leaked data, bad actors can identify vulnerable employees and target them with personalized bribes or coercion schemes.

5. Instant Payments: A Prime Target for AI-Driven Exploitation

Instant payments, prized for their speed and convenience, have also become fertile ground for AI-enhanced fraud schemes. The immediacy of these transactions leaves little room for manual review or customer intervention once a payment is initiated, making them an ideal target for sophisticated, high-speed attacks powered by artificial intelligence.

Fraudsters are increasingly using AI to identify behavioral patterns, spoof legitimate payment requests, and auto-generate personalized phishing messages that can bypass basic authentication checks. In particular, AI-driven BEC attacks are being tailored to the context and urgency of real-time payments, convincing employees to initiate transfers that are almost impossible to recall. Moreover, AI bots can now launch coordinated fraud campaigns across hundreds or thousands of accounts simultaneously, exploiting weak points in fraud detection systems not yet calibrated for the dynamics of instant payments.

A Call for Intelligence-Driven Defense

The use of artificial intelligence in fraud is pervasive, adaptive, and accelerating. From deepfake-powered social engineering to AI-generated identities and insider threats, financial institutions must shift from reactive defenses to proactive, intelligence-driven strategies. Only through the integration of advanced technology with strategic foresight can institutions stay ahead of the evolving threat landscape and protect both their customers and their reputations.

---

[1] CNN, “Finance worker pays out $25 million after video call with deepfake ‘chief financial officer.’” February 4, 2024.

[2] McAfee, “The State of the Scamiverse.” January 2025.

[3] Veridas Identity Fraud Report 2024.

[4] TransUnion, “H2 2024 Update: State of Omnichannel Fraud.”

[5] BioCatch, “BioCatch Report: Global money mule networks.” 2025.

[6] The Sun, “One in five Brits claim they have been approached to help illegally launder money,” May 7, 2025.

The Regulatory Reckoning

Due to the continuing rise of fraud—aided and abetted by AI—financial institutions worldwide are being called on to enhance transparency, accountability, and preparedness in fraud response programs. Recent regulatory developments across the European Union, United Kingdom, and United States are central to this movement.

European Union: PSD3 and PSR Proposals

The European Commission's proposals for PSD3 and the Payment Services Regulation (PSR), introduced in June 2023, aim to modernize the EU's payment services framework. These proposals focus on enhancing consumer protection, promoting competition, and strengthening the security of electronic payments. Key aspects include:

- **Implementing stronger authentication controls to better protect customers and detect fraud in real time.**
- **Mandating clearer disclosure requirements to improve transparency around fees and terms.**
- **Requiring greater provider accountability for unauthorized transactions and fraud incidents.**

These proposals are currently under review by the European Parliament and the Council, with the aim of adoption in the near future.

United Kingdom: Failure to Prevent Fraud

In the UK, a major legislative milestone arrived with the enactment of the Failure to Prevent Fraud offence under the Economic Crime and Corporate Transparency Act 2023. This regulation introduced a new corporate offence that holds large organizations criminally liable if they fail to prevent fraud by employees, subsidiaries, or associates. Key implications include:

- **Establishing criminal liability for organizations when associated persons commit fraud on their behalf.**
- **Defining applicability thresholds based on size, turnover, and employee count to target large organizations.**
- **Reinforcing the need for preventative controls such as training, monitoring, and whistleblowing frameworks.**

This development signals a shift from reactive to preventative regulation in the UK, and positions fraud prevention as a board-level priority.

United States: FFIEC Guidance

In the United States, the FFIEC continues to update its guidance to address emerging fraud risks. Recent updates emphasize the importance of:

- **Adopting risk-based authentication methods that match the context and threat level of each transaction.**
- **Deploying continuous monitoring systems to track user behavior and detect suspicious activity in real time.**
- **Developing comprehensive response plans that cover detection, containment, investigation, and recovery.**

These expectations underscore the need for financial institutions to adopt a proactive and dynamic approach to fraud risk management.

Challenges and Opportunities

The regulatory environment presents both challenges and opportunities for financial institutions. By intentionally adapting to new requirements and investing in robust fraud prevention measures, institutions can not only achieve compliance but also enhance their resilience against fraud. This strategic alignment with regulatory expectations is essential for maintaining customer trust and ensuring long-term success in the financial sector.

The Shift to Multi-Layered, Real-Time Fraud Detection

Given the expansion and sophistication of fraud threats and the increasingly rigorous regulatory environment, financial institutions are transitioning toward integrated, multi-layered fraud detection systems that leverage real-time analytics and cross-channel data correlation to enhance security and resilience. This shift reflects the growing need for dynamic, proactive fraud defense mechanisms capable of identifying threats as they unfold, rather than relying on traditional, reactive approaches.

Layered Security for Layered Threats

Today's fraud schemes span a variety of channels—online banking, mobile apps, call centers, and payment systems—often exploiting gaps between them. A single-layer defense is no longer sufficient. Multi-layered fraud detection weaves together various protective elements, including device fingerprinting, behavioral analytics, machine learning, and threat intelligence feeds. By correlating signals across these layers, institutions can identify coordinated attacks and stop them in their tracks. This approach also enables fraud teams to detect previously hidden patterns, such as low-value test transactions across multiple accounts or anomalous behavior following credential compromise.

Real-Time Analytics for Immediate Response

Timely action is critical. Real-time analytics allow institutions to evaluate transactions as they occur, rather than hours—or days—later. According to a 2025 report by CoinLaw, 99.9% of fraud attempts are detected in real time by AI-powered systems,[7] enabling institutions to respond more swiftly to potential threats. Real-time capabilities are especially vital in mitigating instant payment fraud, where funds can be irrevocably moved in seconds.

Cross-Channel Correlation for Greater Visibility

Fraudsters often exploit siloed systems, launching coordinated attacks across multiple channels to mask their activity. By correlating data across all customer touchpoints—web, mobile, branch, and support—financial institutions can piece together a unified risk profile. For example, a login attempt from an unfamiliar device followed by a high-value transaction request via the call center may not appear suspicious in isolation, but becomes high risk when evaluated together. Cross-channel correlation enables smarter, more informed decision-making without adding unnecessary friction for legitimate users.

A Strategic Imperative for 2025 and Beyond

The implementation of multi-layered, real-time fraud detection is becoming a strategic imperative for financial institutions. This integrated approach empowers organizations to move beyond static rule sets and siloed monitoring, delivering smarter, faster, and more adaptive threat responses. It not only strengthens defenses against increasingly complex fraud schemes but also helps meet growing regulatory expectations around timely incident detection and reporting. As the speed and scale of digital finance grow, so too must the agility and depth of fraud detection strategies.

[7] "Big Data in Fintech Statistics 2025: How Big Data is Driving the Future of Finance." CoinLaw, 2025.

The Adoption of Identity-Centric Security Models

Complementing the shift to multi-layered, real-time fraud detection, financial institutions are increasingly adopting identity-centric security models. Here are three ways that institutions are placing user identity at the core of their security frameworks to combat sophisticated cyber threats effectively:

1. Biometric Authentication: Enhancing Security and User Experience

Biometric authentication methods, such as fingerprint scanning, facial recognition, and voice recognition, have gained significant traction in the financial sector. As of March 2025, 87% of global banks have implemented biometric authentication,[8] reflecting a commitment to enhancing security while providing a seamless user experience. The adoption of biometric technologies has led to a substantial reduction in fraud incidents. A comprehensive analysis by KPMG revealed that banks experienced an average 66% reduction in account takeover fraud within 12 months of implementing multi-modal biometric authentication systems.[9]

2. Adaptive Access Controls: Contextualizing Security Measures

Adaptive authentication systems adjust security measures based on contextual factors such as user behavior, device type, and location. This dynamic approach ensures that security protocols are proportionate to the assessed risk level of each access attempt. The adaptive authentication market is projected to reach $31.85 billion in 2025, driven by the rising need for intelligent, risk-based authentication solutions in response to escalating cyber threats.[10]

3. Continuous Verification: Sustaining Trust Throughout Sessions

Continuous verification involves the ongoing assessment of user identity throughout a session, rather than relying solely on initial login credentials. This approach is crucial in detecting and mitigating threats that may arise during active sessions. For instance, behavioral biometrics monitor user interactions, such as typing patterns and mouse movements, to establish a behavioral profile. Any deviations from this profile can trigger security responses, thereby preventing unauthorized activities even after initial authentication.

Keep User Identity at the Center

The adoption of identity-centric security models marks a pivotal shift in the financial sector's approach to cybersecurity. By focusing on user identity as the central element of security strategies, financial institutions can more effectively safeguard against evolving cyber threats. Implementing biometric authentication, adaptive access controls, and continuous verification not only enhances security but also improves user experience, fostering trust and resilience in the digital financial ecosystem.

[8] "Financial Data Consent Trends: Biometric Data and Dynamic Permissions in 2025." Secure Privacy, April 4, 2025.

[9] "Global Banking Fraud Survey: Biometric Impact Assessment." KPMG, 2023.

[10] "Adaptive Authentication Market Insights - Growth & Forecast 2025 to 2035." Future Market Insights, March 5, 2025.

The Exposure of Internal-External Collusion

While most fraud strategies focus on perimeter threats, one of the most complex and costly risks continues to originate from within. Internal-external collusion—when employees knowingly or inadvertently assist external fraud actors—represents a unique challenge for financial institutions. These schemes often bypass traditional controls, exploit organizational silos, and evade detection for extended periods.

The TD Bank Case: A Wake-Up Call

A striking example of internal-external collusion emerged in 2024 when TD Bank had to pay $3B to U.S. authorities after it was revealed that employees had knowingly allowed fraudulent transactions to pass through their systems. These transactions were part of a larger money laundering and fraud scheme tied to organized crime networks. In some cases, employees manipulated internal controls or failed to escalate suspicious activity reports, allowing bad actors to exploit gaps in oversight. This illustrates the real-world consequences of collusion and the urgent need for institutions to close internal visibility gaps and and embed proactive internal risk detection into their fraud and anti-money laundering (AML) programs.

Enhancing Internal Risk Detection with Behavioral Analytics

Employees who engage in collusion often exhibit subtle but detectable deviations from normal activity. Modern behavior analytics solutions can flag high-risk patterns such as repeated access to dormant accounts, abnormal login hours, or the suppression of alerts in specific transaction types. When evaluated in real time and in context, these behavioral shifts provide critical early signals of insider involvement.

Integrating Fraud and AML Programs for Collusion Detection

Collusion often sits at the intersection of fraud and money laundering. Employees may facilitate fraudulent account openings, override transaction alerts, or act as internal facilitators for laundering illicit funds. When fraud and AML systems operate in concert—sharing risk indicators, correlating suspicious behaviors, and cross-validating anomalies—institutions gain a more complete picture of collusion risk. For example, when an employee accesses multiple flagged accounts shortly before large outbound transfers, that context becomes a key differentiator in detecting coordinated activity.

Embedding Governance and Oversight into Daily Operations

Technology alone is not enough. Leading institutions are building stronger lines of defense by integrating governance into daily workflows. This includes enforcing segregation of duties, strengthening approval hierarchies, and implementing continuous monitoring of internal access and activity. Just as importantly, anonymous whistleblower channels and strong retaliation protections empower employees to report concerns before they escalate.

Building a Culture of Transparency and Collaboration

Collusion thrives in fragmented environments. Financial institutions that prioritize cross-functional collaboration—between fraud, compliance, risk, and HR teams—are better positioned to detect and disrupt insider-assisted schemes. By promoting a culture of transparency and aligning investigative workflows, these organizations ensure that no critical signals fall through the cracks.

Unmasking Collusion Is Crucial

As fraud schemes become more sophisticated and internal threat vectors more complex, unmasking collusion is more and more crucial. Institutions that invest in advanced behavior monitoring, system integration, and internal oversight are not only better equipped to detect and prevent insider threats—they are also safeguarding their reputations, regulatory standing, and customer trust in a digital-first world.

The Power of Fraud Intelligence Sharing

Not every fraud detection and prevention effort is a solo venture: collaboration has emerged as a critical strategy for enhancing security measures. Financial institutions, fintech companies, and industry consortiums are increasingly recognizing the value of shared intelligence in identifying and preventing fraudulent activities. This collective approach enables faster threat identification, broader pattern recognition, and a more unified defense across the financial ecosystem.

Industry-Wide Collaboration: A Force Multiplier

Information-sharing networks like the Financial Services Information Sharing and Analysis Center (FS-ISAC) give financial institutions a way to stay ahead of emerging threats. FS-ISAC's global membership includes thousands of firms across 75 countries, collectively securing more than $100 trillion in assets. Through secure portals and automated feeds, members can share indicators of compromise and receive real-time threat alerts—an approach that has been shown to reduce response times and prevent repeat attacks.

The impact of such collaboration is tangible. One major U.S. bank saw a 1,700% improvement in detecting high-risk fraud events after participating in a cross-industry data-sharing initiative. Another institution improved its ability to identify risky card transactions by over 20 times, simply by incorporating shared fraud intelligence into its models.[11]

Cross-Sector Integration: Bridging the Gaps

As financial services become more interconnected—encompassing traditional banks, fintechs, and payment platforms—sharing data across these boundaries becomes critical. In the United Kingdom, the National Economic Crime Centre (NECC) exemplifies effective cross-sector collaboration. Established in 2018, the NECC brings together law enforcement agencies, regulatory bodies, and private sector partners to coordinate the UK's response to economic crime. By facilitating intelligence sharing and joint operations, the NECC enhances the collective ability to detect, prevent, and disrupt complex financial crimes.

These types of partnerships demonstrate how broader visibility leads to better outcomes. When institutions combine insights across platforms, they can model risk more effectively and detect anomalies that would otherwise go unnoticed.

Technology-Enabled Sharing: Real-Time, Privacy-Conscious

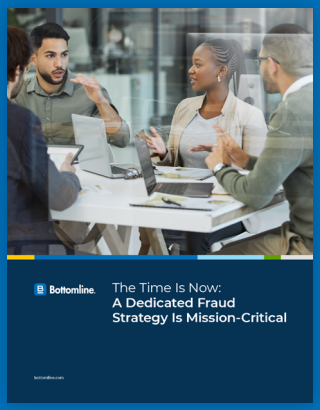
Emerging technologies are enabling financial institutions to share fraud intelligence in real time without compromising privacy or regulatory compliance. AI-driven platforms can analyze vast streams of transactional data, identify suspicious patterns, and flag threats across networks—instantaneously. Meanwhile, privacy-preserving techniques like data anonymization, tokenization, and differential privacy ensure that shared information cannot be traced back to individuals, protecting sensitive customer data.

Blockchain-based data exchanges add another layer of trust and transparency. These decentralized networks allow institutions to contribute and access verified fraud indicators—such as device fingerprints, IP addresses, or behavioral red flags—without revealing the underlying customer identities. These technologies enable secure, privacy-compliant collaboration while enhancing the ecosystem's collective defense.

Collaboration as a Competitive Advantage

Fraud intelligence sharing is quickly becoming a hallmark of mature fraud prevention programs. Financial institutions that engage in proactive, real-time collaboration gain a strategic edge—one that extends beyond compliance and cost savings. By pooling insights and resources, they are able to anticipate threats, act swiftly, and ultimately protect both their assets and their customers in a fast-evolving threat landscape.

[11] Woods, Rob. "Sharing fraud intelligence is a game changer for banks," Information Age, February 14, 2025.



The Time is Now

Read the Report

Contact us to learn more about Bottomline's payments fraud prevention solution.

Book a Meeting

Resilience Through Advanced Fraud Detection

The rapid evolution of financial fraud has outpaced the capabilities of legacy security frameworks. As attackers leverage generative AI, insider access, and real-time tactics to circumvent detection, institutions must adopt a fundamentally different approach to fraud prevention.

An effective response entails multi-layered, real-time fraud detection to address fast-moving and complex threats, and keeps user identity at the center through behavioral and biometric authentication. It addresses collusion through deeper internal oversight while simultaneously joining forces with external companies and institutions to share fraud intelligence.

Financial institutions that take this approach will not only improve fraud detection: they will safeguard operational resilience, regulatory standing, and long-term customer trust in an increasingly adversarial digital environment.

Bottomline

About Bottomline

Bottomline helps businesses transform the way they pay and get paid. A global leader in business payments and cash management, Bottomline's secure, comprehensive solutions modernize payments for businesses and financial institutions globally. With over 35 years of experience, moving more than $16 trillion in payments annually, Bottomline is committed to driving impactful results for customers by reimagining business payments and delivering solutions that add to the bottom line. Bottomline is a portfolio company of Thoma Bravo, one of the largest software private equity firms in the world, with more than $179 billion in assets under management.

For more information, visit www.bottomline.com

REV UK112125LD

Corporate Headquarters
100 International Drive, Suite 200
Portsmouth, NH 03801
United States of America

Phone: +1-603-436-0700
Toll-free: +1-800-243-2528
info@bottomline.com

Europe, Middle East, Africa Headquarters
1600 Arlington Business Park
Theale, Reading, Berkshire RG7 4SA
United Kingdom

Tel (Local): 0870-081-8250
Tel (Int): +44-118-925-8250
emea-info@bottomline.com