Bottomline

The Time Is Now: **A Dedicated Fraud Strategy Is Mission-Critical**

A Systemic Threat Demands a Systemic Response

The tactics used by today's fraudsters have progressed from opportunistic schemes to systemic assaults on commercial banking infrastructure. No longer the domain of isolated actors relying on crude tactics, fraud has become industrialized, scalable, and increasingly invisible. Fueled by artificial intelligence (AI) and insider collusion, today's fraud schemes operate at a velocity and complexity that outpace many banks' current defenses.

The consequences are immense. According to the 2025 AFP Payments Fraud and Control Survey, 79 percent of organizations experienced actual or attempted payment fraud in 2024—a near match to 2023's 80 percent. Check fraud alone targeted 63 percent of organizations in a troubling indicator that legacy channels remain highly vulnerable. Meanwhile, wire transfers have become the most common vehicle for business email compromise (BEC), cited by 63 percent of respondents. [1]

While these statistics speak to known threats, there is a deeper danger: new techniques are emerging that do not yet have names, patterns, or playbooks. From deepfake-enabled scams to synthetic identity fraud, commercial banks face a multi-front battle. What is needed is not more tools, but a unified fraud strategy—one that integrates technology, governance, and oversight into a holistic and adaptive framework.

79% of organizations experienced actual or attempted payment fraud in 2024

The Industrialization of External Fraud

The archetype of the lone fraudster has been replaced by coordinated threat actors equipped with sophisticated tools and real-time infrastructure. In 2024, the Federal Trade Commission reported consumer fraud losses of $12.5 billion, up $2.5 billion from the prior year. Bank transfers and payments accounted for more than $2 billion of these losses, highlighting the increasing effectiveness of social engineering and account takeover techniques. [2]

Commercial banks are particularly vulnerable to authorized push payment (APP) fraud, BEC, and phishing schemes. These attacks exploit human behavior rather than technological flaws. In a now-notorious case, a Hong Kong finance employee was duped into wiring $25 million after participating in a video call with deepfake images of the company's CFO and legal team. [3]

Even more concerning is the shift in attacker mindset. Rather than focusing on high-value targets alone, fraudsters increasingly favor high-volume, low-value attacks that evade traditional detection systems. In the United Kingdom, for example, remote purchase fraud surged by 22% in 2024 while APP fraud cases fell 20%, [4] as criminals capitalized on less-scrutinized payment channels to siphon funds at scale.

Another alarming trend is the rise of fraud-as-a-service (FaaS), where professional fraud developers sell prebuilt kits, including phishing websites, credential stuffing bots, and digital identity forgeries. This commoditization of fraud tools means a broader set of criminals can now perpetrate advanced attacks with minimal expertise.

To counter these developments, leading banks are exploring cloud-based fraud detection platforms that use federated learning; that is, allowing data models to be trained across multiple institutions without exposing underlying data. This collaborative approach helps detect emerging attack patterns earlier and improves the overall effectiveness of machine learning engines.

A dedicated fraud strategy must recognize this shift. Tactical fraud prevention—such as flagging unusual transactions—is absolutely necessary, but it is insufficient. Banks need to anticipate the industrial logic of modern fraud: it is agile, diversified, and relentlessly opportunistic. This calls for real-time detection, cross-channel monitoring, and ongoing threat modeling as core competencies.

$2B lost to consumer fraud in 2024 from bank transfers and payments

[1] "AFP Payments Fraud and Control Survey 2025." Association for Financial Professionals.

[2] Federal Trade Commission, 2024.

[3] "Finance worker pays out $25 million after video call with deepfake 'chief financial officer.'" CNN, 2024.

[4] "Annual Fraud Report 2025." UK Finance, 2025.

The AI Arms Race

Generative artificial intelligence (GenAI) is accelerating both the scope and sophistication of fraud. Fraudsters now use AI to generate synthetic identities, impersonate executives, and mimic communication styles. Deepfake audio, text, and video are no longer rare or difficult to produce. In fact, Deloitte estimates that AI-driven fraud losses could reach $40 billion annually by 2027, up from $12.3 billion in 2023. [5]

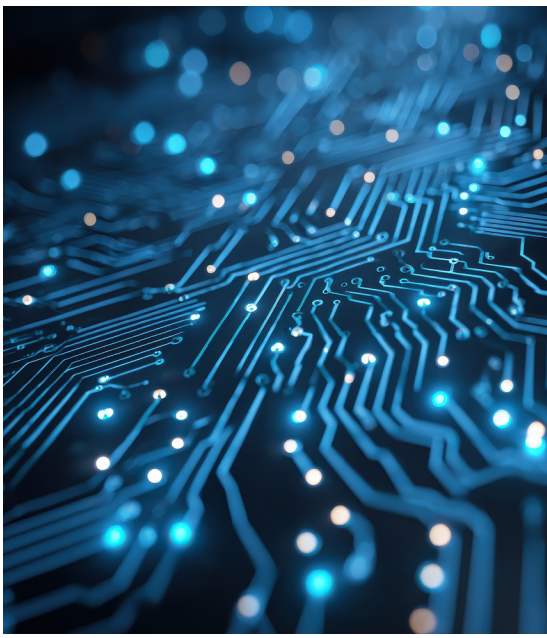
Synthetic identity fraud is particularly difficult to detect. These identities, which blend real and fictitious information, can pass verification checks and establish creditworthiness over time before executing fraudulent transactions. This type of fraud is now the fastest-growing financial crime in the U.S. [6]

What makes GenAI especially dangerous is its ability to weaponize trust. For example, a UK-based energy firm lost approximately $243,000 when fraudsters used AI-generated voice emulation to mimic the CEO. During a phone call, the scammers demanded an urgent wire transfer to a supposed Hungarian supplier, using cloned speech that convincingly replicated the executive's accent and tone. The call's authenticity was not doubted and the payment was authorized … and then, of course, the money disappeared. [7] These tactics erode traditional markers of authenticity—such as voice, language, and timing—and make it more difficult for employees and systems to distinguish real from fake.

Compounding these threats, commercial banks are under intense pressure to deliver faster, more seamless digital experiences while also supporting real-time payment rails. These innovations, while beneficial to customers, increase the complexity of fraud detection. Decisions must be made in milliseconds, leaving narrow windows to flag or intercept suspicious activity.

This swiftly-morphing environment has created an AI arms race with AI's massive capabilities equally essential on both sides of the battlefield. Criminals use it to scale and tailor attacks with unprecedented precision, while banks must deploy it not only to detect fraud, but also to anticipate, disrupt, and adapt in real time. Success now hinges on integrating AI into a proactive fraud strategy—one capable of defending against today's threats and adapting to tomorrow's.

$40B could be lost annually from AI-driven fraud by 2027



The AI arms race is not theoretical. It is active and ongoing. Commercial banks that fail to invest in AI-based fraud defenses are unlikely to keep pace with the adversaries that do.

[5] "Generative AI is expected to magnify the risk of deepfakes and other fraud in banking." Deloitte, 2024.

[6] Simons, Ted. "Trends in synthetic identity fraud." April 21, 2023.

[7] "Unusual CEO Fraud via Deepfake Audio Steals US$243,000 From UK Company." Cyber Attacks, 2019.

Layered AI Strategies for Fraud Prevention and Compliance

To meet the scale and complexity of modern fraud threats, commercial banks must adopt a layered defense strategy that integrates AI at its core. Within this framework, machine learning —a subset of AI—plays a vital role in driving real-time detection and response capabilities.

One of the most powerful applications is behavioral biometrics: the analysis of how users interact with systems through patterns such as typing cadence, mouse dynamics, touchscreen pressure, and device orientation. These subtle behavioral signals are highly individualized and difficult to replicate, making them a robust defense against account takeovers and credential compromise. AI models continuously learn from these inputs to build dynamic user profiles and flag anomalies that may indicate fraud or insider misuse—even after login credentials have been verified.

When paired with advanced transaction analytics, these models become even more effective. AI-driven systems can analyze vast volumes of transaction data, cross-referencing real-time activity against historical behavior to detect suspicious deviations. For example, a payment initiated outside of a user's normal geographic region, time window, or dollar range might trigger enhanced verification or immediate intervention. These systems do not rely on static rules but evolve with the data, allowing them to identify fraud tactics as they emerge—without needing to be explicitly programmed in advance.

This multi-dimensional approach, combining behavioral biometrics with transaction-level AI, offers a significant advantage: it enables both user-level precision and system-wide awareness. As fraud tactics grow more sophisticated, this fusion of granular insight and broad detection logic is essential to reducing false positives while improving accuracy.

However, AI systems are not foolproof—and their performance is only as good as their inputs and governance. High-quality, representative data is critical to training models that can recognize nuanced patterns without becoming biased or brittle. Poorly trained or under-tested models risk overfitting to known behaviors or failing to generalize across customer types, use cases, or regions.

Just as important is oversight. As regulators increasingly scrutinize algorithmic decision-making, banks must ensure that their AI systems are explainable and auditable. This is especially true for fraud tools that may impact customers' access to services or trigger compliance reviews. Transparent governance and strong documentation not only mitigate regulatory risk, but also support internal accountability and cross-functional collaboration.

Banks should also take a page from cybersecurity best practices by "red teaming" their AI models. In this exercise, adversarial simulations are used to probe system vulnerabilities, e.g., intentionally inputting edge cases or crafted anomalies to test whether fraud detection logic can be bypassed. These controlled attacks reveal blind spots, validate system resilience, and help teams iteratively improve model performance.

Ultimately, the power of AI in fraud prevention lies not in any one technique, but in the ability to integrate and adapt across detection layers. As fraudsters evolve their tactics, so too must banks evolve their defenses—ensuring that AI remains a dynamic shield rather than a static tool.

Checklist

Making AI Auditable and Accountable

- ✓ Ensure explainable model logic
- ✓ Maintain complete training data documentation
- ✓ Monitor for model drift
- ✓ Enable cross-functional review (compliance, IT, fraud ops)
- ✓ Retain logs for regulator audits

Use this checklist to ensure your AI tools meet both performance and regulatory standards.

Countering the Enemy Within

While much attention is paid to external threats, internal fraud remains a persistent—and arguably more insidious—risk to financial institutions. Insider fraud is particularly dangerous because it originates from individuals who already have legitimate access to systems and sensitive information. This access allows them to bypass traditional perimeter security measures.

In one recent example, a major bank in the U.S. identified multiple lower-level employees selling client data to organized online scammers, including full identity records and account credentials, in exchange for cash payments. [8] Such incidents not only result in financial losses but significantly erode customer trust and brand credibility.

According to the Association of Certified Fraud Examiners' 2024 Report to the Nations, internal fraud results in a median loss of $145,000 per case globally, with financial services organizations ranking among the industries with the highest number of reported cases. Detection often takes months, as insiders tend to conceal their activities well, and the red flags are subtle.

Banks should invest in continuous user behavior analytics (UBA) to monitor employee interactions with critical systems. UBA tools help detect unusual patterns—such as access to dormant accounts, abnormal login hours, or attempts to override controls—that could indicate insider risk. In addition, separation of duties, frequent access reviews, and a principle of least privilege in system access must be rigorously enforced. These operational controls limit the potential damage a single insider can inflict.

As fraud grows more complex, insider risk will continue to rise in parallel with technological threats. A robust fraud strategy must treat insider risk not as a compliance checkbox, but as a core component of organizational resilience.

[8] "Bank employees sell client data to online scammers." New York Post, December 30, 2024.

Red Flags That May Signal Insider Threats

- ⚠ Accessing systems outside of normal working hours
- ⚠ Downloading or printing large volumes of data
- ⚠ Repeatedly accessing dormant or restricted accounts
- ⚠ Attempting to disable security controls or logs
- ⚠ Refusing to take vacations (a known fraud concealment tactic)

Fraud Governance, Customer Education, and Metrics of Resilience

Effective fraud management begins at the top—with a robust governance framework that elevates fraud risk to a board-level priority. A centralized fraud risk governance structure brings together leaders across fraud operations, risk, compliance, IT, and legal to ensure alignment on risk appetite, policy, and resource allocation. This collective oversight embeds fraud prevention and detection into the institution's broader risk management strategy, moving it beyond isolated silos and fragmented responses.

Strong governance fosters clear ownership and accountability. Fraud leaders must be empowered to establish standards, enforce controls, and escalate issues with the authority and visibility necessary to drive timely action. To measure progress, key performance indicators—such as fraud loss rates relative to payment volumes, investigation turnaround times, and fraud capture effectiveness—should be consistently tracked and communicated to senior leadership and board members. These metrics transform governance from a compliance exercise into a dynamic tool for strategic decision-making and continuous improvement.

Equally important is customer education. Many fraud schemes, including APP fraud and BEC, exploit the customer as the weakest link. An informed customer base can significantly reduce fraud exposure. Leading banks have adopted proactive communication strategies that include:

- **Real-time transaction alerts that prompt customers to verify high-risk activity.**
- **Fraud awareness campaigns tailored to both consumers and business clients.**
- **Simulated phishing campaigns for commercial customers to strengthen internal controls.**

Small and mid-sized businesses (SMBs), in particular, often lack the resources for robust fraud defenses. A 2024 BAI Banking Strategies article urged banks to expand and strengthen the fraud protections they make available to SMB clients, noting that this segment faces growing threats but receives relatively little support[9].

Beyond education, commercial banks should build resilience into their fraud response. This includes:

- **Playbooks for coordinated incident response that span fraud, cybersecurity, communications, and customer service.**
- **Crisis simulation exercises to prepare teams for high-impact events, such as coordinated deepfake attacks.**
- **Post-mortem analysis after major fraud events, with structured lessons learned and control enhancements.**

Furthermore, fraud strategies must evolve with changing conditions. A 12-month static roadmap is no longer sufficient. Banks need agile governance mechanisms to adapt priorities, redeploy resources, and respond to real-time threat intelligence.

[9] "Banks must rethink the fraud protections they offer SMB clients." BAI, 2024.

Embrace transparency. Institutions that regularly publish fraud trends, incident statistics, and mitigation efforts demonstrate leadership and instill confidence in both customers and regulators.

Transforming Fraud Defense

Read the Report

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

Book a Meeting

Building Institutional Resilience in the Face of Modern Fraud

Fraud has become a persistent, shape-shifting adversary to the commercial banking industry. What was once considered an operational issue is now an enterprise risk with the power to compromise customer trust, regulatory standing, and long-term profitability.

As the financial crime landscape grows more sophisticated—from AI-driven scams to insider exploitation—commercial banks must respond with equal sophistication. This requires moving beyond reactive point solutions toward an integrated, institution-wide fraud strategy that encompasses governance, technology, education, and agility.

The time to act is now. Fraudsters are already operating at scale. Commercial banks that build strategic resilience today will not only reduce losses, but also reinforce trust and differentiate their brand … thereby positioning themselves for long-term success in a digital-first financial ecosystem.

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 UK112025LD

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