Treasury & Risk.

Leveraging AI to Improve Fraud Detection and Prevention

By Steve Wiley
November 3, 2025

Bad actors have dramatically altered the landscape of corporate fraud in recent years, introducing increasingly complex schemes and using them more frequently. Deloitte's Center for Financial Services predicts that generative artificial intelligence (GenAI) could drive fraud losses to $40 billion in the United States by 2027. To put that projection into perspective, the number was just $12.3 billion in 2023.

Tactics are becoming ever more sophisticated. Traditional schemes have evolved to include AI-generated deepfakes, advanced business email compromise (BEC) attacks, and highly personalized phishing campaigns that can fool even experienced finance professionals.

The rapid growth in fraud risk has fundamentally altered the baseline risk profile for businesses. The question is not whether an organization will face these threats, but whether it will be ready when threats arrive. And this escalating threat environment is fundamentally changing the roles of corporate treasury and finance professionals, who have transitioned from a focus only on liquidity and traditional financial risks to become the first line of defense against financial crime.

Organizations today expect their treasurer to be well-versed in fraud mitigation strategies and to partner with technology teams to protect organizational assets. This is a significant shift from just five years ago, when fraud detection was primarily reactive and largely the domain of IT. Now finance leaders are expected to proactively mitigate fraud, in part by leveraging the latest AI-powered tools.

Foundation First: Organizational Structure and Workflow Controls

Before implementing AI-powered fraud detection tools, corporations must build the proper foundation. Technology alone won't stop fraud if the organization's payment environment is fragmented. Many companies still operate with decentralized global payment structures, multiple payment systems with different workflows, and fragmented technology architectures over which they have varying degrees of control. In these environments, the risk of fraud is inherently higher, regardless of the technology deployed.

The most effective fraud prevention requires centralizing treasury operations under unified oversight rather than allowing individual departments

to maintain separate processes. A centralized structure eliminates the gaps between decentralized systems that fraudsters often try to exploit, creates consistent control environments, and enables comprehensive monitoring of all payment activities. While some organizations resist centralization due to concerns about operational flexibility, the fraud-prevention benefits far outweigh the inconvenience of minor workflow adjustments.

Once a company has established a centralized organizational structure for treasury, the treasury team should design standardized workflows that govern how payments are initiated, approved, and recorded across the company. Many modern treasury systems are designed to detect fraud using anomaly-detection technologies, but those solutions are effective only when expectations around user and system behaviors are consistent companywide. If a significant proportion of payments are anomalous relative to expectations, the fraud-detection software will have a much more difficult time rooting out true threats.

Strong workflows incorporate well-defined checks and balances. Segregation of duties is one of the most important—no single individual should be able to create, approve, and release a payment. A common model includes three roles: One person initiates, another reviews and approves, and a third executes the payment. Approval hierarchies should scale with risk, requiring more senior signoff for larger or higher-risk transactions, such as international wires or payments to new vendors.

In building these workflows, consider key questions: Who should be able to initiate these payments, and what documentation should we require? What approval thresholds should trigger additional review? And how will the organization verify banking and other information for new vendors?

Well-crafted workflows act as speed bumps for fraud attempts. For example, when an individual receives a phishing email and attempts to initiate a payment without realizing the request is fraudulent, a standardized workflow with proper controls, including segregation of duties, significantly reduces the risk that the misled employee will release the payment to an unverified third party. The four-eyes principle, where a second individual must review and approve every payment, can be a critical control point in preventing fraud.

Another key component is staff training and awareness. This requires ongoing effort—it won't be once-and-done—but human intelligence remains crucial to payment decision-making. Treasury and finance team members need to understand the threats they are likely to encounter, the organization's fraud-prevention policies, and the capabilities and limitations of the technologies they will be using. Building out a robust, ongoing training regimen helps ensure staff remain prepared to follow best practices.

What AI Brings to the Fraud-Detection Table

Once a company has established proper workflows and payment controls, AI-based software can supplement the efforts of treasury, finance, and A/P staff by identifying anomalous activity, autonomously flagging unusual patterns that might indicate fraud. A basic example involves an organization preparing to send a payment to a particular country or region where it has never before done business—an AI-based system can automatically flag the transaction for additional human review. Similarly, payments exceeding a certain threshold and initiated by a specific user can be automatically flagged for additional scrutiny.

Sophisticated AI-driven platforms extend the hunt for anomalies beyond simple rule-based detection. Modern solutions can analyze vast amounts of transaction data and identify subtle patterns that might indicate fraud. AI systems can also learn from new threats as they emerge, a capability that is particularly valuable for identifying previously unknown fraud schemes that might bypass traditional rule-based systems.

All this functionality sits on top of the company's traditional controls like segregation of duties and approval hierarchies to create a multilayered mechanism for fraud detection and prevention. Each layer provides a different type of protection; together they build a holistic defense of the organization's payments.

Organizations that pull all these elements into their fraud-detection platforms are finding that their AI fraud-detection systems are becoming

increasingly effective against various schemes that have previously proven difficult to control. External fraud, such as sophisticated phishing attacks, can be mitigated through the combination of centralized workflows and automated anomaly detection. For instance, a midsize manufacturing company recently faced repeated phishing attacks where fraudsters impersonated vendors and requested urgent wire transfers to new accounts. Previously, these attempts slipped through because the payment requests appeared legitimate and came from seemingly trusted contacts. Once the company centralized its treasury operations and layered in AI-based anomaly detection, the system automatically flagged the unusual payment requests and routed them for human review. As a result, the fraudulent transfers were stopped before any funds were released.

There is only so much that organizations can do to prevent employees from receiving and responding to a phishing email, but companies can use workflows and AI-powered alerts to intercept fraudulent payments before money leaves the organization.

Internal fraud presents another significant risk area in which AI can prove valuable. With proper segregation of duties and anomalous payment destination detection, systems can flag payments to accounts that the company hasn't previously used or verified. This creates a new layer of protection against insider threats while maintaining comprehensive audit logs for investigation purposes.

The Next Generation of Corporate Treasurers

AI-powered fraud detection is critical for any serious fraud-prevention program. The next generation of finance professionals, many of whom have grown up using AI tools for research and problem-solving, expect to be able to ask AI-powered assistants questions about optimizing payment controls or implementing fraud-prevention measures. This evolution extends to large language models (LLMs) specifically designed for treasury. These are specialized AI tools that can provide immediate answers to complex questions about fraud prevention, system configuration, and best practices—capabilities that weren't available even two years ago.

The selection of technology partners is now a critical component of any corporation's fraud-prevention strategy. Finance professionals must conduct thorough assessments of technology vendors, scrutinizing their fraud-recognition capabilities as well as their overall cybersecurity posture, capabilities, and track record, and their investment in protecting client assets.

Then they should extend this scrutiny to other counterparties—including banks and payment processors—scoring them on their demonstrated ability to protect assets and their investment in cybersecurity infrastructure. Many financial institutions and technology providers are now embedding AI not just in their products and workflows, but also within their cybersecurity functions, creating multiple layers of protection that benefit their clients through reduced overall risk exposure.

In designing fraud-prevention technologies and processes, treasury teams need to keep in mind that although AI systems learn and improve over time, they require ongoing adjustments to remain effective against evolving fraud schemes. And continuous monitoring and adaptation will only get more important in years to come, as the trajectory of AI use in fraud prevention points toward increasingly sophisticated and autonomous systems. Future developments will likely include more advanced pattern-recognition capabilities, better integration with external threat intelligence sources, and an improved ability to uncover previously unknown fraud schemes.

Treasury departments that are early adopters of AI systems will help their businesses stay ahead of the curve on fraud prevention.