Trustpair | ActualizeConsulting

Beyond the AI Hype: Strengthening Treasury Against Fraud Risks

WHY REAL-TIME CONTROLS, CONTINUOUS MONITORING, AND VERIFIED DATA ARE THE FUTURE OF FRAUD PREVENTION

Table of Contents

Introduction

> The acceleration of fraud due to generative AI (GenAI) means businesses must invest in proactive defenses.

AI is a technology for which the sky is the limit. We have seen advanced Large Language Models (LLMs) pass university entrance exams and specifically train models to complete tasks, such as patient diagnosis, at super-human levels, showcasing how AI can be configured for and excel at specific tasks if given sufficient training data.

However, the same AI advancements that enable businesses to automate workflows and enhance security are also being leveraged by cybercriminals to launch sophisticated scams, making it imperative for organizations to stay ahead.

Trustpair and Actualize Consulting recognize that AI is not just an efficiency tool - it is a battleground. The acceleration of fraud due to generative AI (GenAI) means businesses must invest in proactive defenses. Deepfake fraud, AI-generated phishing attacks, and automated credential stuffing are becoming more refined, increasing the risks of financial loss. Companies can no longer afford a reactive approach; AI-powered fraud prevention is a necessity, not an option.

01
AI Is Not The Fraud Solution It's The Fraud Accelerator

While AI can be a helpful tool in some areas, it is not a simple solution for fraud prevention. In fact, AI is making fraud more effective, scalable, and harder to detect. Businesses that assume AI-powered defenses alone will protect them risk falling into a false sense of security.

Fraudsters are using AI to:

Bypass authentication systems with deepfake audio and video.	Mimic legitimate communication to execute business email compromise (BEC) scams.
Generate realistic fake invoices and bank details to fool accounts payable teams.	Automate credential stuffing attacks to break into financial systems.

The sheer speed and adaptability of AI-powered fraud make traditional reactive fraud detection strategies ineffective. Instead of relying on AI to detect fraud after it happens, companies need real-time, proactive fraud prevention tools that focus on validating vendor information, securing payment workflows, and ensuring human oversight at key decision points.

> Social engineering, like phishing, spear phishing, and deep fakes, is now the bigger threat compared to direct attacks like password cracking. Users are often tricked into revealing sensitive information. Implementing secondary checks and data-driven fraud analysis—similar to multi-approval processes in TMS systems—is essential to protect against fraud in today's global treasury environment

Rob Granger
Senior Manager,
Actualize Consulting

02
Why Businesses Need To Strengthen Reliable and Systemic Controls

To combat AI-driven fraud, organizations must prioritize **proven fraud prevention tactics** that do not rely on AI models prone to manipulation. Businesses should focus on:

1# Vendor Validation & Continuous Monitoring

Instead of AI-based fraud detection, organizations need real-time vendor validation that ensures payment details are accurate before a transaction is processed. Automated and reliable bank account ownership verification plays a critical part in this process, ensuring that payments are directed to legitimate vendors. Solutions like Trustpair provide ongoing monitoring to flag changes in vendor banking information, preventing fraud before it occurs.

2# Human Oversight & Multi-Layered Verification

AI should not replace human judgment when it comes to financial security. Over-automation increases risk, as employees may become disconnected from the fraud detection process. Businesses must reinforce case management, approval workflows, and multi-layered validation steps to prevent fraudulent payments.

3# Stronger Payment Controls & Approval Processes

Payment fraud thrives in environments with weak approval workflows.

Companies must implement multi-step authentication, dual approval systems, and strict access controls to reduce fraud risks. By reinforcing these human-led controls, businesses create strong barriers against AI-generated fraud attempts.

4# Employee Awareness Training

Fraudsters exploit human error, and AI-generated scams are designed to deceive employees. Yet, 90% of executives feel confident in spotting deepfake scams and BEC fraud, while 90% of companies have still been targeted by cyber fraud. Even with 43% investing in fraud awareness training, 39% of employees don't consistently follow fraud prevention policies. Stronger controls, automated and reliable bank account ownership verifications, and reinforced training are crucial to closing these security gaps.

Simon Elcham
CTO, Trustpair

AI excels at detecting anomalies and streamlining decisions, though human oversight remains crucial. Rather than aiming for complete payment automation, the goal is to intelligently flag transactions for focused human review, which greatly reduces workload. However, too much automation carries risks—when teams become disconnected from the underlying data, resolving issues becomes challenging. The ideal approach balances AI's efficiency with maintaining human transparency and control in decision-making.

03
A Treasury-Focused Approach to Combating AI-Driven Fraud

AI will continue to advance, and so will the tactics of fraudsters. Treasurers cannot afford to be reactive in this fight—they must adopt a proactive strategy built on trust, security, and verification.

Secure Treasury & ERP Integrations

A well-structured treasury system with controlled access and strict authentication policies remains the best defense against unauthorized modifications to payment instructions.

Strict Access & Authorization Controls

Ensuring only authorized personnel can modify payment details or approve transactions is critical in mitigating the risk of AI-driven fraud attempts.

Resilient Treasury Governance

Treasury policies must be continuously updated to account for emerging AI-related threats. Regular security audits and compliance checks should be part of every organization's fraud mitigation strategy.

04 How Can My Organization Prepare For The AI Revolution?

Instead of rushing to integrate AI into security processes, businesses need to reinforce fundamental safeguards - structured processes, reliable tools, and human oversight.
One of the biggest risks comes from disorganized financial data. Fraudsters exploit gaps in messy payment records and weak verification procedures. Treasury teams must ensure their data is structured, secure, and centralized in an ERP or TMS system. A strong financial foundation reduces vulnerabilities, making it harder for fraudsters to manipulate payment workflows.

At the same time, over-reliance on AI can create a false sense of security. AI-driven fraud tactics, like deepfake impersonations and AI-generated phishing emails, are designed to bypass automated detection. Businesses must take a security-first approach, ensuring that sensitive financial data is never fed into AI tools without proper oversight. Establishing an AI charter - a set of internal guidelines on how AI is used within the organization - may help align teams and set clear boundaries on AI's role in financial operations.

While AI may assist in certain areas, human oversight, automated and reliable bank account ownership verifications, and strict approval processes remain the foundation of fraud prevention.

To future-proof your business, centralizing systems with advanced tools is essential, ensuring your teams have clarity on authorized signers and eliminating confusion caused by multiple bank portals. Integrating this centralized system with a solution like Trustpair provides robust protection, proactively verifying payments—even against sophisticated social engineering attacks.

Simon Elcham
CTO, Trustpair

Looking Ahead

> AI is reshaping the fraud landscape, and finance leaders must take decisive action to stay ahead of these risks. Rather than viewing AI as a solution to fraud, businesses must recognize it as a growing enabler of fraud itself.

Investing in the right treasury tools, reinforcing human oversight, and maintaining strict validation processes will be the key to safeguarding corporate payments in an era of AI-powered fraud.

The question is no longer whether your organization will be targeted, but whether it has the right protections in place to withstand AI-driven fraud attacks. Trustpair and Actualize Consulting are here to help treasury leaders build fraud-resistant payment systems that don't rely on AI, but rather on verified, structured security measures.

For more insights on securing your treasury operations, contact Trustpair and Actualize Consulting today.

Trustpair

Take Action Against Vendor Fraud

www.trustpair.com

Trustpair empowers large global companies to eliminate vendor payment fraud with a market leading account validation automation platform. Trustpair serves over 400 enterprise customers, helping finance teams protect against 100% of fraud attacks.

The company's global presence includes **offices in New York City, Paris, London and Milan.** Our team is composed of **100+ employees** with 15 different nationalities who are dedicated to payment security. Trustpair raised 20 million euros to accelerate international growth, and equip finance leaders with the tools needed to tackle sophisticated fraud tactics such as AI, deepfakes, cyber attacks, and more.

Talk to an expert

contact@trustpair.com