2025
FRAUD REPORT
USA

Trustpair

Fraud in the Cyber Era: 2025 Fraud Trends & Insights

AN ANALYSIS OF HOW THE AI-DRIVEN FRAUD CRISIS IS RESHAPING PAYMENTS IN CORPORATE AMERICA

Table of Contents

Trustpair

Executive Summary

Cyber fraud is on the rise - and the financial and reputational impact of experiencing an incident is rapidly growing alongside.

Despite the rising prevalence and stakes of fraud attacks, executives in Corporate America have high confidence in their organizations' ability to spot and stop fraud. Yet a deeper dive into the inner workings of these organizations reveals that these executives could be overly confident and that investments in the fight against payment fraud aren't going far enough to stop today's savvy fraudsters.

Trustpair's research reveals a stark reality: 90% of companies were targeted by cyber fraud in 2024, with 47% suffering losses exceeding $10M. This surge in cyber fraud is primarily driven by fraudsters' rapid adoption of AI technologies, evidenced by a 118% increase in advanced Gen-AI tactics like deepfakes and deepaudio, as well as more convincing BEC, and other sophisticated social engineering attacks.

The rise can also be attributed to companies' fraud defenses being largely lagging and over-reliant on awareness training and manual processes. The urgency to strengthen fraud defenses will only grow in 2025 as macroeconomic factors drive up the risk of fraud.

This report dives deeper into the increasing risk of cyber fraud, where companies are most vulnerable, and strategies for keeping up with the rapidly evolving landscape.

Companies worldwide are facing budget constraints and cost-cutting. Yet, two-thirds of U.S. companies have kept or increased their fraud prevention budgets.

Our research shows that awareness needs to become action and that budgets need to be allocated more intentionally.

With the expertise of:
Baptiste Collot
CEO, Trustpair

Lee-Ann Perkins
Global Treasurer,
Ankura Consulting

Gloria Wan
Executive Director, Kinexys
by J.P. Morgan

Michael Van Keulen
CPO, Coupa

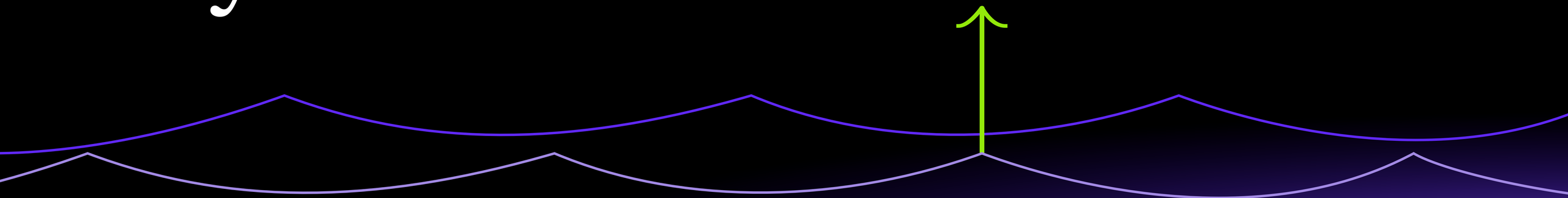
Methodology
Research group
Cint

Number of respondents
200

Field dates
11/27/24 - 12/05/24

Geography
U.S.

01
The Rising Tide of Cyber Fraud

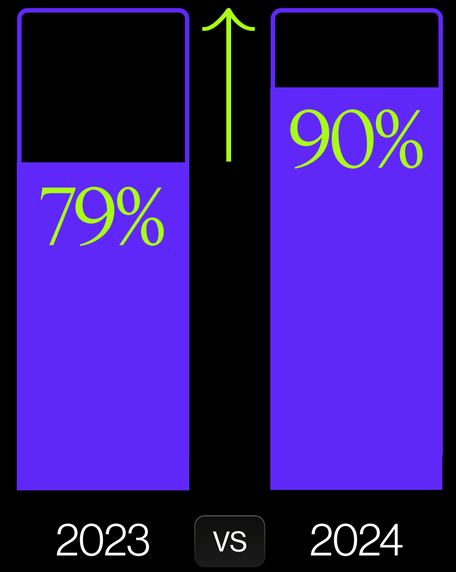


Cyber Fraud is Surging

of U.S. Companies Targeted by Cyber-Fraud in 2024

A Significant Increase in Cyber Fraud

(r=190)



Cyber fraud: any type of criminal activity that involves the use of technology or the internet to deceive or defraud, including hacking, deepfakes, highly sophisticated phishing schemes, voice cloning, etc.

Cyber Threats At a Glance

Cyber Vulnerabilities Increase Payment Risks

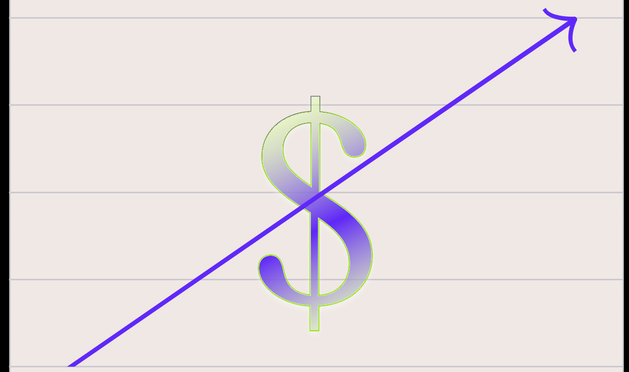
(r=200)

67%

of U.S. companies see cybersecurity vulnerabilities as the most likely to lead to a higher risk of payment fraud in 2025.

Budgets Increased

(r=200)



⅔ of companies have increased their budgets in fraud prevention over the past 12 months.

What started as a trend is now an inescapable reality: cyber fraud has taken over and is here to stay. Most companies (95%) that experienced a successful payment fraud attack in 2024 said it was driven by cyber fraud - a 14% increase from 2023.

This shift to cyber fraud reflects a fundamental change in how fraudsters operate: they now use AI and other advanced technologies to conduct fraud attempts. The widespread availability of AI tools has made it easier for fraudsters to generate highly convincing impersonations and social engineering attacks that make fraud attempts nearly impossible to detect through traditional prevention measures. **AI also enables fraudsters to send emails and execute schemes in much higher numbers, increasing the chances of a company being attacked. It's now almost guaranteed that all companies will be targeted.**

Companies seem to have grasped the risks, with cybersecurity vulnerabilities seen as the most worrying business risk and the biggest factor that will drive up fraud in 2025. As a result, fraud prevention budgets increased for 67% of companies, despite cost constraints in an uncertain economic context. These investments are encouraging but aren't enough - especially as payment fraud is expected to rise further in 2025.

> The rise of cyber fraud is happening at a much faster and concerning rate than anticipated. In just a few years, AI and ChatGPT have become common tools everyone uses, anywhere, making it easier than ever to create convincing fraud schemes. They're being adopted at a fast pace by fraudsters and leave no room for errors or loopholes within organizations.

Lee-Ann Perkins
Global Treasurer

02 Macroeconomic Pressures: A Gateway to Payment Fraud

The Toll of Economic Instability

(r=200)

Outside of cybersecurity vulnerabilities...

47%

of executives said that economic volatility and...

31%

...geopolitical uncertainty are most likely to lead to a **higher risk of payment fraud** at their organizations next year.

Payment fraud risk is increasingly tied to broader macroeconomic and business risks, with economic volatility, and geopolitical uncertainty emerging as key risk factors that will increase the risk of fraud in 2025.

These pressures create conditions that make organizations more vulnerable to fraud attempts.

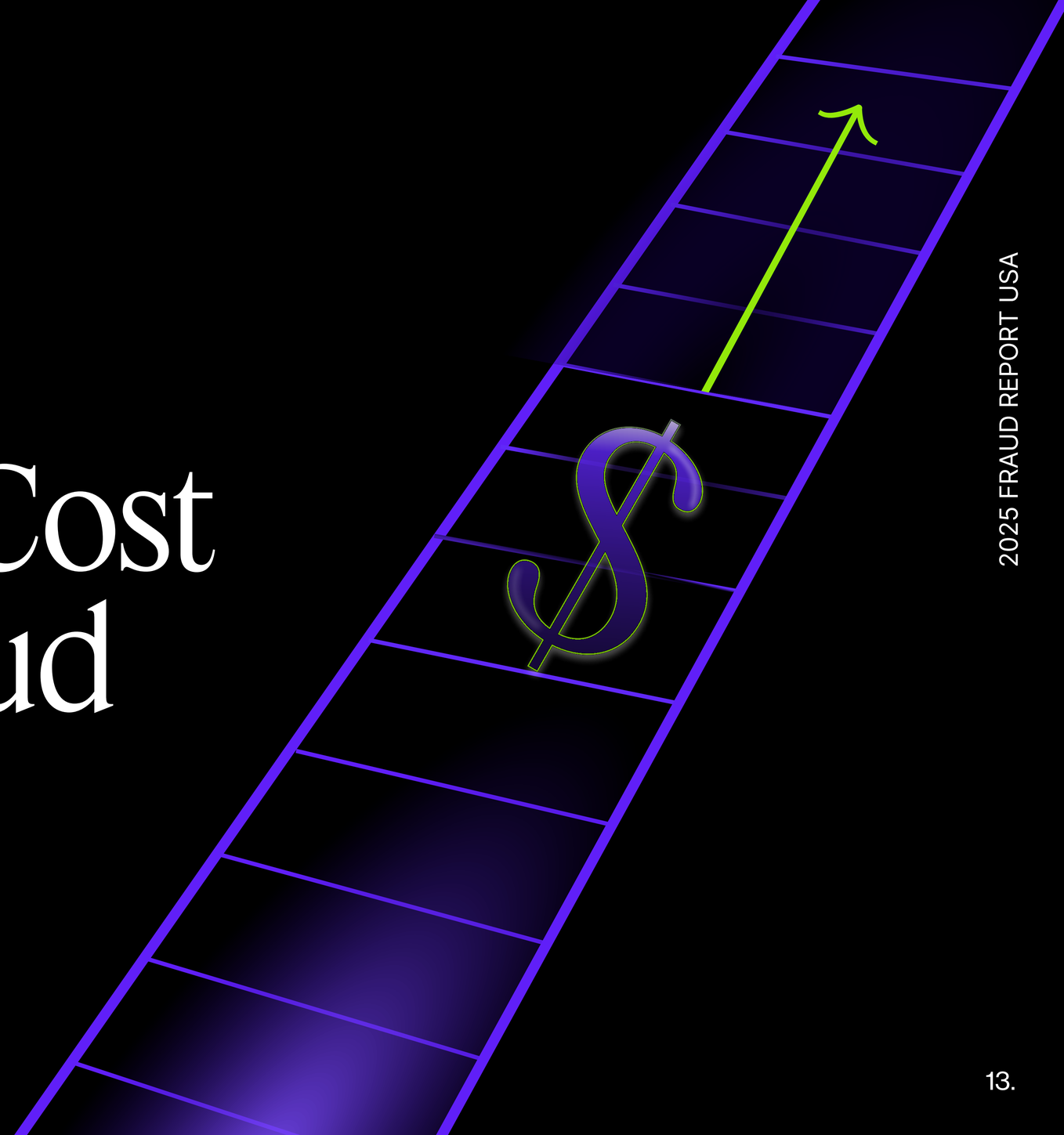
For example, economic uncertainty can lead to resource constraints and increased workloads for workers. This can cause stretched-thin employees to bypass standard payment controls and verification processes, either unintentionally because they are balancing multiple priorities or intentionally to save precious time. When teams are under pressure to maintain operational efficiency with limited resources, it's not uncommon to make mistakes or cut corners on security protocols, creating opportunities for fraudsters. Additionally, economic stress can make employees more easily manipulated and susceptible to social engineering tactics, particularly when dealing with urgent payment requests or sensitive financial transactions.

Given the growing financial and reputational impact of payment fraud - and the fact that these macroeconomic factors are likely to increase the risk of fraud - strengthening fraud prevention measures should be a top business priority next year. Companies need to move away from antiquated fraud prevention methods as these economic factors create new gateways for fraudsters.

Lee-Ann Perkins
Global Treasurer

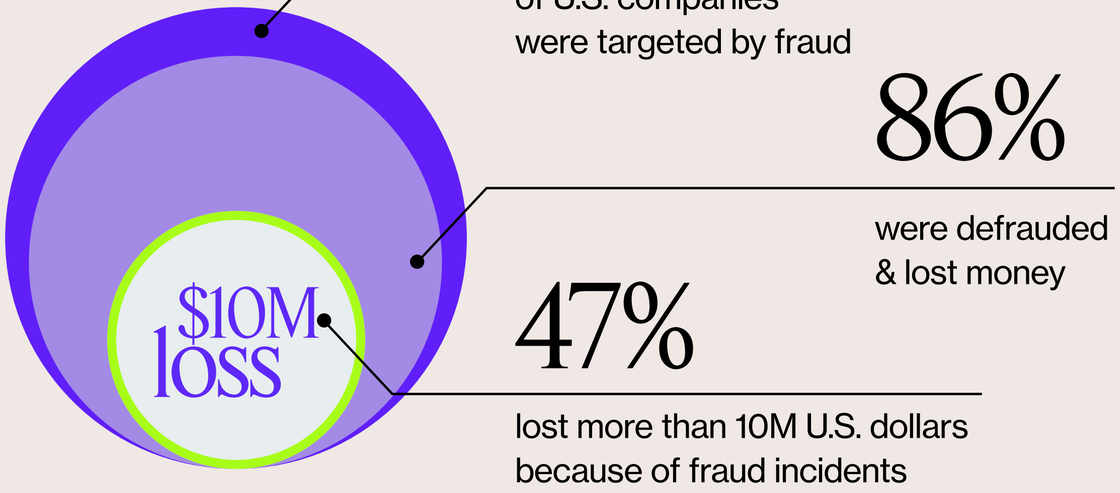
With economic uncertainty, people are more fearful and resources are stretched thin. Because you have fewer resources, you might take less time to consider all the details and processes you should respect. You don't go through all the essential steps and controls for payment processes. This emotional response to having less stability can lead to unintended risks.

03
The Escalating Cost of Payment Fraud



The Breakdown of Financial Impact

(r=200)



The financial impact of payment fraud reached unprecedented levels, with **86% of targeted companies experiencing monetary losses** and **47% losing over $10M in 2024.**

The Impact on Reputation is Worrying Executives

(r=200)

Outside of financial losses, executives worry most about their reputation with these key players.

The year-over-year increase is particularly striking, with the percentage of companies that reported losses of over $5M more than doubling between 2023 and 2024.

Beyond direct financial losses, payment fraud creates significant collateral damage to corporate relationships and brand reputation. Most executives cite reputational damage with customers, investors, and suppliers as a critical concern, highlighting how fraud incidents erode stakeholder trust and impact long-term brand reputation.

Thanks to AI and real-time payments, fraudsters can now move larger amounts of money much more quickly than what was previously possible, which explains the growing consequences of fraud. They work with much greater precision and speed than what was previously possible with paper checks and in-person fraud.

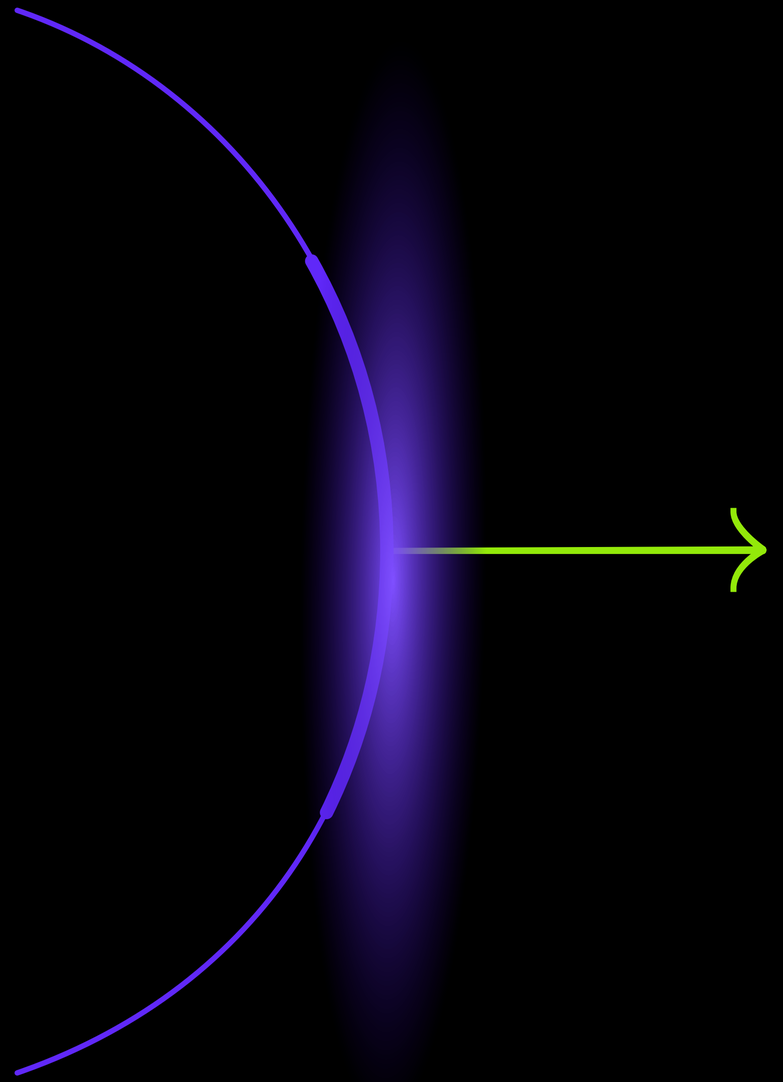
This combination of escalating financial losses and reputational damage underlines how payment fraud has evolved from an **operational issue to a strategic business risk** requiring CEO and board-level attention.

The average financial loss is huge, and rising. This alone is a clear signal for companies to take the right steps against fraud. With 42% of U.S. companies losing 10M dollars on average to fraud, it's safe to say we're facing a core business problem.

Baptiste Collot
CEO, Trustpair

04

AI: The Weapon of Choice for Payment Fraudsters



The Tactics Used By Fraudsters

1

63%
of Companies Reported BEC

(r=190)

Reported BEC as a tactic used by fraudsters, making it the #1 approach fraudsters are using against organizations, **up 103% YoY.**

2

24%
of Companies Reported Gen-AI Fraud

(r=190)

Reported increase of advanced Gen-AI tactics - like deepfakes and deepaudio

3

17%
of Companies Reported Video Conferencing Tools

...used by fraudsters

Fraudsters are rapidly adopting sophisticated technologies to execute more convincing scams. The increase in advanced generative AI tactics such as deepfakes and deep audio demonstrates how quickly fraudsters are leveraging these technologies to bypass traditional detection methods.

Business Email Compromise (BEC) scams have evolved significantly, from basic emails filled with grammatical and spelling errors to AI-generated content that precisely mimics executive communication styles and company protocols. The year-over-year increase in BEC attacks, now the primary fraud channel, reflects how **AI has transformed previously manual schemes** into sophisticated ones that defeat standard verification procedures.

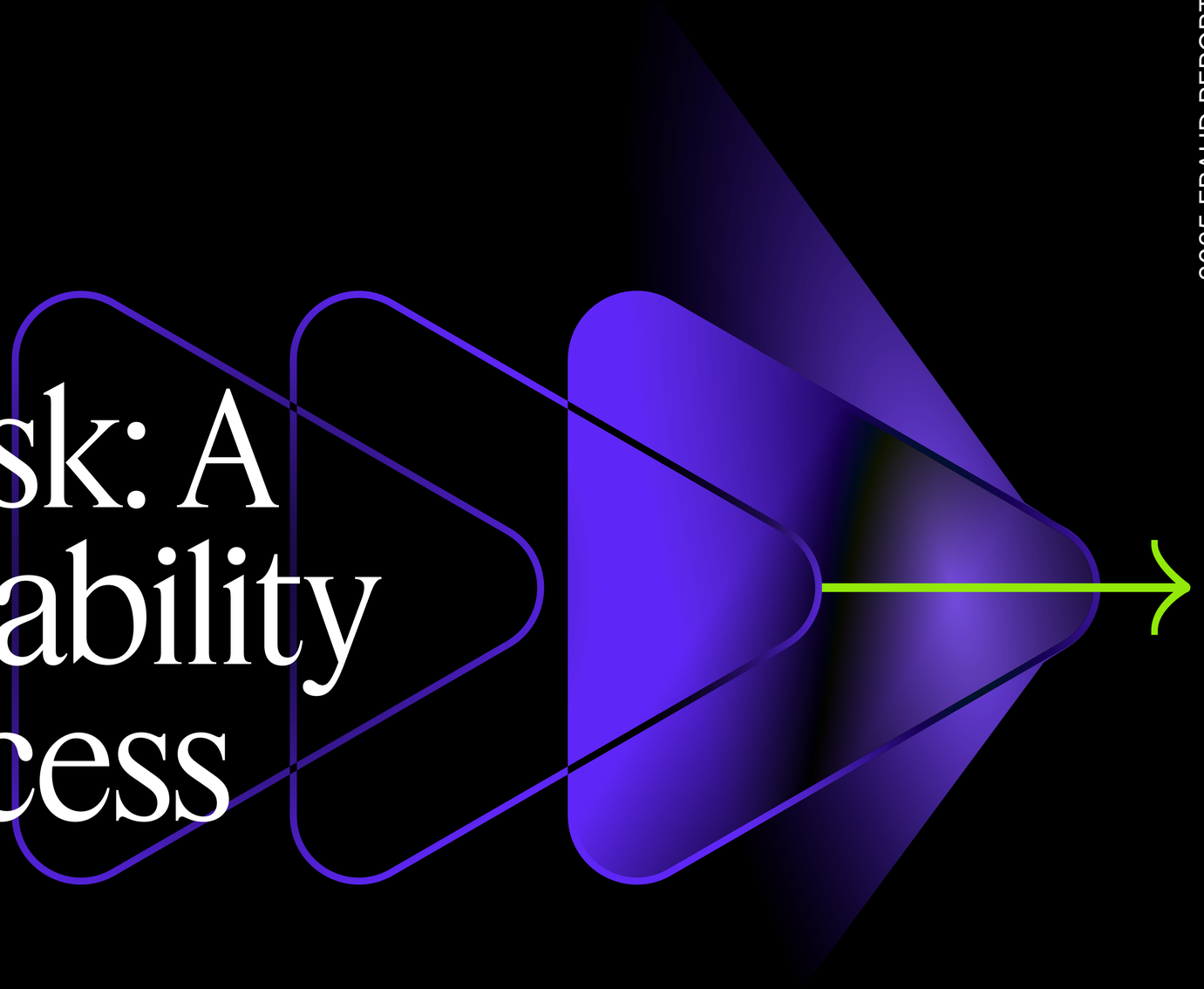
This shift requires companies to rethink their fraud detection approach, moving beyond conventional methods to implement automated systems that can identify and stop AI-generated fraud attempts.

> Sophisticated scams are increasingly hard to detect, as traditional routines and controls often fail against such convincing schemes. In the payment space, it's crucial to adopt proper processes, supported by automation, to stay vigilant. Success in combating fraud requires the right tools, time, and attention.

Lee-Ann Perkins
Global Treasurer

05

Third-Party Risk: A Critical Vulnerability in the P2P Process



The Growing Threat of Vendor Fraud

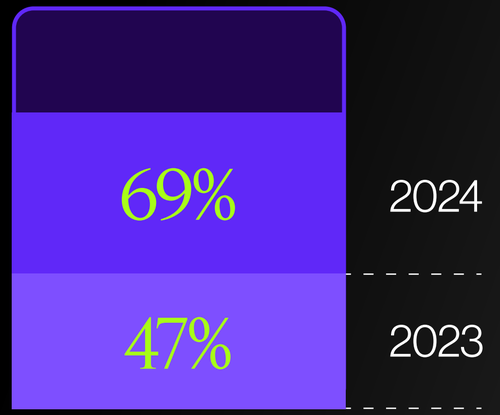
Beware of Third Party Changes!

1/4 of Executives

said supply chain and/or third-party relationship changes will most likely lead to a higher risk of payment fraud at their organizations in 2025.

(r=200)

Vendor Fraud Attempts Still Increased in 2024



Increase of U.S. companies targeted by vendor fraud attempts

(r=190)

05. THIRD-PARTY RISK: A CRITICAL VULNERABILITY IN THE P2P PROCESS

The sharp increase in vendor fraud reveals a critical vulnerability in third-party relationships. While companies have traditionally focused on securing the payment stage, data shows that the risk begins much earlier. Fifty-four percent of companies feel most vulnerable to payment fraud during supplier onboarding, 65% when a supplier requests credential changes, and 64% when a new invoice is submitted.

The risk of fraud extends across the entire supplier lifecycle, yet, only 8% of companies maintain consistent vendor verification throughout the entire procure-to-pay (P2P) process, creating significant exposure to fraud.

Companies now feel more vulnerable during the earlier P2P stages than at the payment stage. This shows the critical need for more collaboration with the Procurement department. Procurement should be more involved in payment fraud prevention: it isn't only a treasury matter.

Baptiste Collot
CEO, Trustpair

A quarter of executives anticipate supply chain and third-party relationship changes to increase fraud risk in 2025. This underscores the need for a more global approach to vendor management, requiring closer collaboration between finance and procurement teams to implement consistent verification across all stages of the P2P process, thanks to integrated fraud prevention tools.

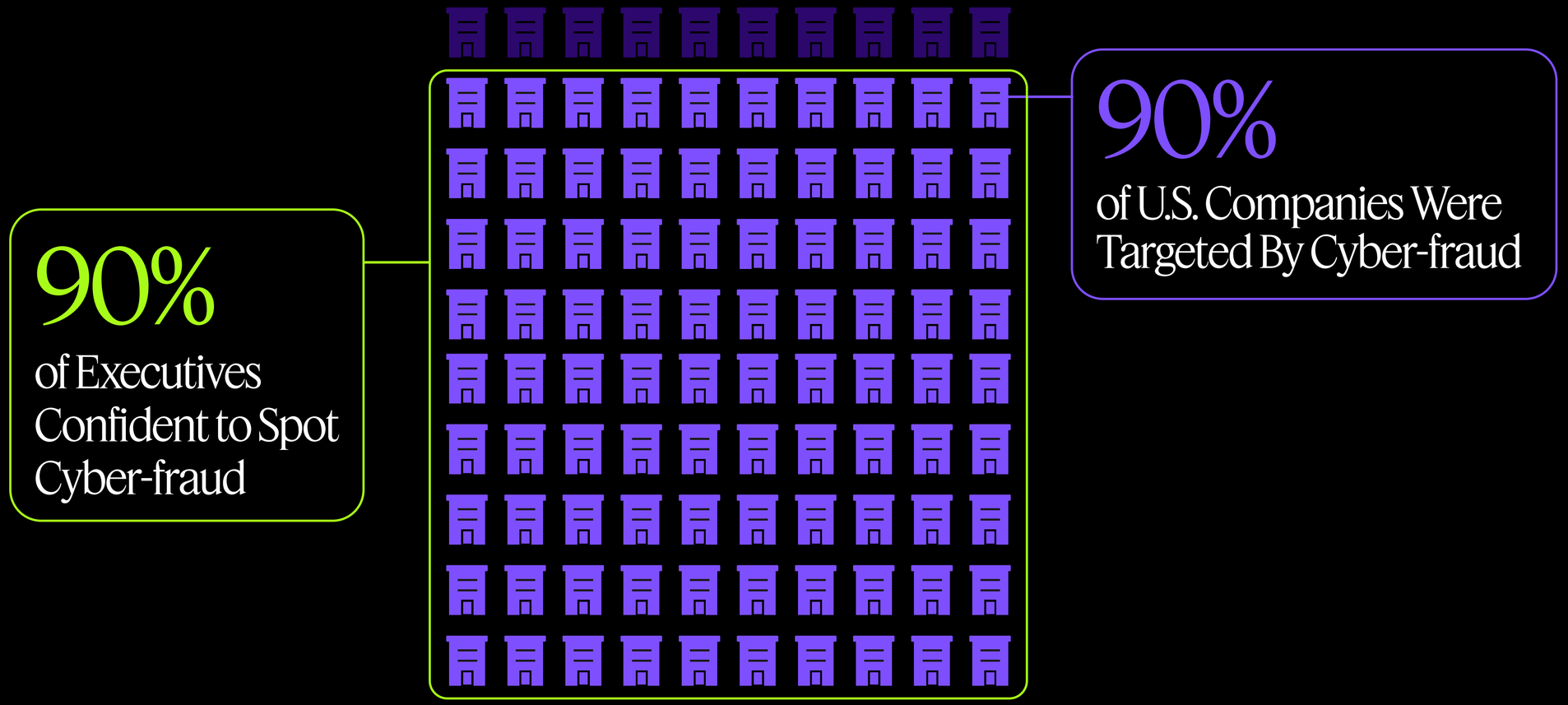
> Unfortunately, only 31% of companies reported having an automated account validation tool to verify supplier identities across the P2P process.

Fraudsters exploit third-party relationships by targeting under-resourced teams rushing through approvals. Everyone assumes someone else will catch mistakes, creating a false sense of security. Adding more approvers doesn't fix the issue—stronger internal controls and personal accountability do. If you'd triple-check a personal wire transfer, you should do the same for business transactions.

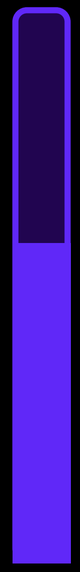
06

The Overconfidence Trap: Where Fraud Prevention Approaches Fall Short

The Paradox of Cyber Fraud Confidence

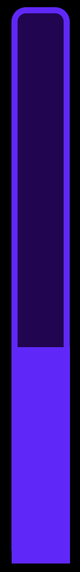


The Limitations of Manual Methods in Fraud Prevention Efforts



69%

of companies use manual methods (human callback or email) to handle bank account validations.



43%

almost half of companies have invested in fraud awareness training over the past 12 months, yet one of companies' biggest challenges is employees don’t always follow fraud prevention policies in place (39%).

Executives have a surprisingly high confidence in the organization's ability to detect cyber fraud, which presents a striking paradox.

While 90% of leaders express high confidence in spotting sophisticated fraud attempts, the same percentage of companies faced successful attacks – suggesting confidence is largely misplaced.

Companies are still relying too much on manual processes for supplier onboarding—but that needs to change. Procurement, not accounts payable, should own the process, ensuring proper checks on ownership, financials, ESG, and bank details. In 2025, technology must replace manual work to create a scalable, efficient, and connected process.

Michael Van Keulen
CPO, Coupa

The continued reliance on manual prevention methods (which 69% of companies say they use today) and low adoption rate of fraud prevention software (26%), **reveals a concerning misalignment between defense strategies and modern threats.**

Additionally, 43% of companies have invested in fraud awareness training over the past year, which helps explain executives' confidence in spotting fraud. But training only goes so far. Even well-trained humans can make mistakes or fail to follow best practices. Thirty-nine percent of finance executives said their biggest challenge is employees not following fraud prevention policies. This dependence on human approaches against technology-driven fraud attempts exposes a critical vulnerability that fraudsters exploit.

Companies have a false sense of confidence and need to fight fraud with the right means - through automated account validation. The budget for investing in technology and automation to help prevent fraud is there and companies should think about where they are allocating budget so they can move beyond simple awareness to tangible action that stops fraud.

With automated account validation solutions like **Trustpair, payments are blocked even if employees haven't spotted the fraud,** protecting the organization's assets.

The first reflex in fraud prevention is still very manual. And this in itself is enough to question corporates' confidence in detecting and handling cyber fraud. When faced with such high levels of technology and sophistication, answering fraud with a human approach only - human callbacks, manual controls, etc - just isn't enough.

Baptiste Collot
CEO, Trustpair

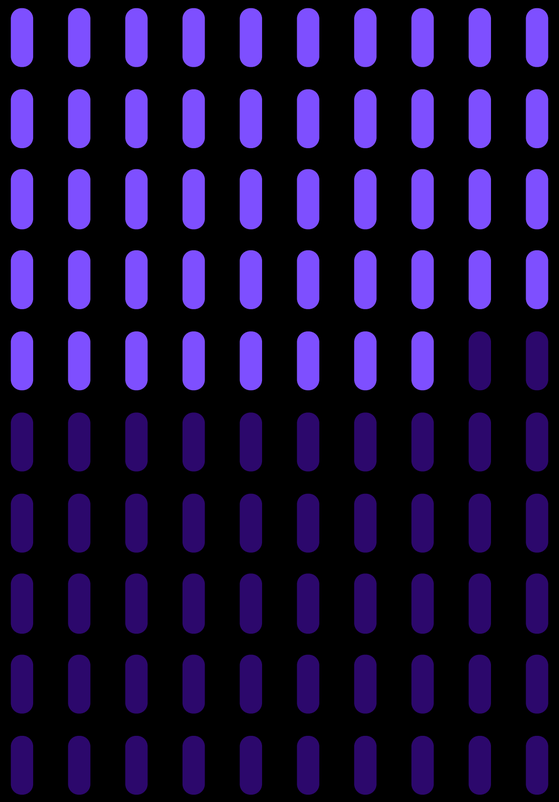
07
Breaking Down Silos: Why Fraud Prevention Demands Company-Wide Ownership

The current approach to fraud prevention **reveals a misalignment in organizational strategy,** with only 9% of executives recognizing it as a multi-department responsibility.

In today's rapidly evolving digital landscape, it is crucial for business executives to develop a comprehensive understanding of the latest payment fraud landscape and how it could apply to or impact your respective industry. While adopting digital tooling to enable data-driven decision-making and to enhance operational controls against fraud incidents, it is equally important to foster a culture of awareness across the organization.

Gloria Wan
Executive Director,
Kinexys by J.P. Morgan

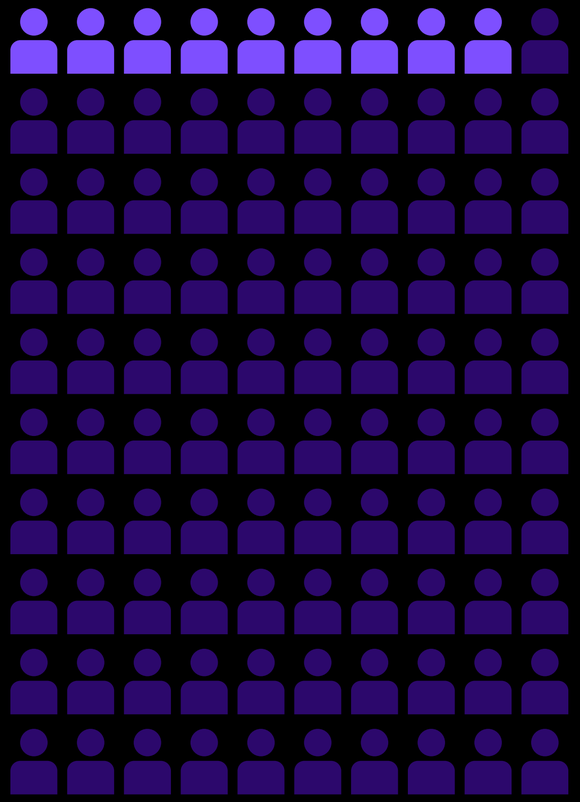
Team Collaboration is Critical for Combatting Fraud



48%

of companies identified the top challenge in fraud prevention is siloed processes that inhibit collaboration, communication, and team alignment.

(r=200)



9%

of executives said fraud prevention should be the responsibility of multiple departments.

> 48% of companies reporting that siloed processes hamper their anti-fraud efforts through reduced collaboration and communication.

This narrow ownership perspective directly contributes to one of the most significant challenges in fraud prevention, with **48% of companies reporting that siloed processes hamper their anti-fraud efforts through reduced collaboration and communication.** Delegating fraud prevention solely to finance teams creates dangerous blind spots, as fraud schemes now target various departments and exploit communication gaps. There are also multiple steps in the payment process where things can go wrong.

Leadership's role in fraud prevention is crucial. C-level commitment sets the tone for organization-wide vigilance and enables the development of comprehensive security protocols that span departmental boundaries. A successful fraud prevention strategy requires dismantling these silos and fostering a culture where every employee, from C-suite to front-line staff, understands their role in protecting the organization.

Gloria Wan
Executive Director
Kinexys by J.P. Morgan

Fraud prevention in a business starts with a clear strategic commitment at the leadership level. This often translates into an investment commitment to digitize solutions for fraud prevention and risk management, modernize operational processes to adopt additional controls, and work with partners and vendors in the broader business ecosystem to build out a feedback loop and continuously improve processes or tooling based on new market trends and learnings.

Conclusion

The 2024 payment fraud landscape presents an urgent wake-up call for U.S. companies. With 42% of organizations losing over $10M to fraud and 90% targeted by cyber fraud, the threat has evolved beyond human detection capabilities.

Traditional manual controls and siloed approaches are insufficient against AI-powered fraud tactics.

Organizations must shift toward automated, technology-driven fraud prevention solutions that can match the sophistication of modern threats. **Tools like Trustpair offer comprehensive protection across the entire procure-to-pay process, addressing vulnerabilities from vendor onboarding through payment execution.** As fraudsters continue to leverage advanced technologies, companies that fail to automate their fraud prevention processes risk significant financial and reputational damage.

Investment in automated fraud prevention tools is no longer optional but a strategic imperative for protecting corporate assets and stakeholder trust.

Trustpair

2025
FRAUD REPORT
USA

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

Trustpair USA Inc | contact@trustpair.com