2025
FRAUD REPORT

Trustpair

Fraud in the Cyber Era: 2025 UK Fraud Trends & Insights

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

Table of Contents

Executive Summary 3.

01 5.
Cyber Fraud: The Primary Culprit in UK Payment Fraud

02 9.
AI-Powered Fraud: A New Era of Threats

03 13.
The Cost of Inaction: Payment Fraud's Financial Toll

04 17.
A Growing Confidence Gap in Fraud Detection

05 22.
Strengthening Defenses: A Unified Company-Wide Approach

Conclusion 26.

Trustpair

Executive Summary

Payment fraud is escalating in scale, sophistication, and impact - posing a significant threat to businesses across the UK. Despite 93% of companies experiencing attempted fraud in the past year, and 42% suffering at least two successful attacks, many executives remain overly confident in their ability to detect and prevent fraud.

This confidence belies a troubling reality: fraudsters are outpacing defenses by leveraging advanced technologies like generative AI, deepfakes, and business email compromise (BEC) to execute increasingly convincing attacks. Trustpair's research reveals that while 94% of businesses have increased their investment in fraud prevention technologies, the majority still rely heavily on reactive measures, such as fraud awareness training and manual checks during high-risk situations.

As 79% of executives cite cyber risks as their top concern for 2025, the financial stakes are higher than ever. This report explores the evolving threat landscape, uncovers critical vulnerabilities, and provides actionable strategies for businesses to stay ahead of sophisticated fraud schemes.

> 93% of companies experiencing attempted fraud in the past year, and 42% suffering at least two successful attacks

> We must acknowledge that cyber fraud isn't going away anytime soon. The real challenge isn't just asking if it's a significant issue—it's determining how we can effectively protect ourselves and remain cyber secure.

Royston Da Costa
Global Treasurer

With the expertise of:
Tom Abbey
Senior Fraud Consultant UK, Trustpair

Royston Da Costa
Assistant Treasurer, Ferguson

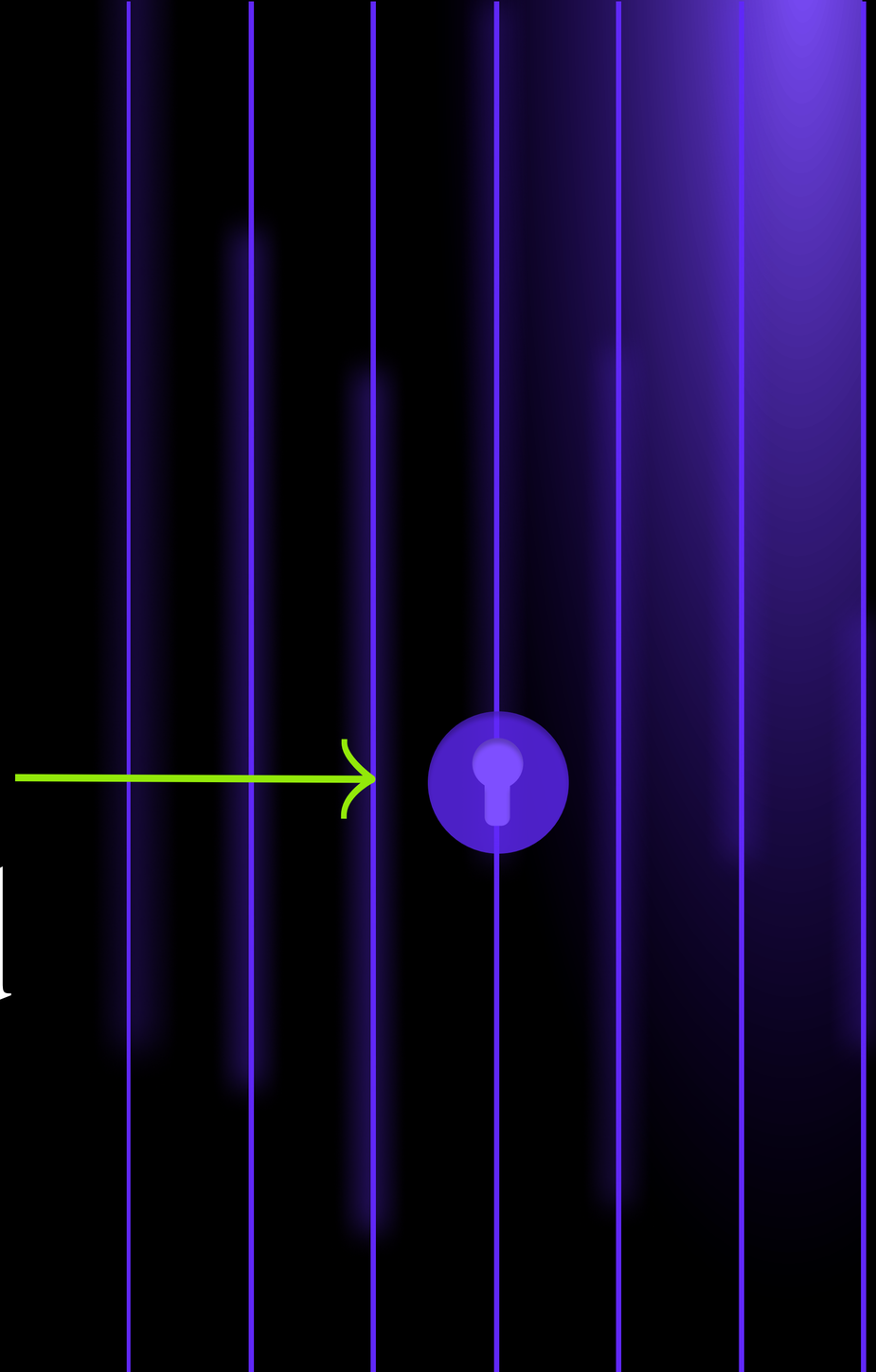
Methodology
Research group
OpinionWay

Number of respondents
150

Field dates
12.4.2024 - 12.11.2024

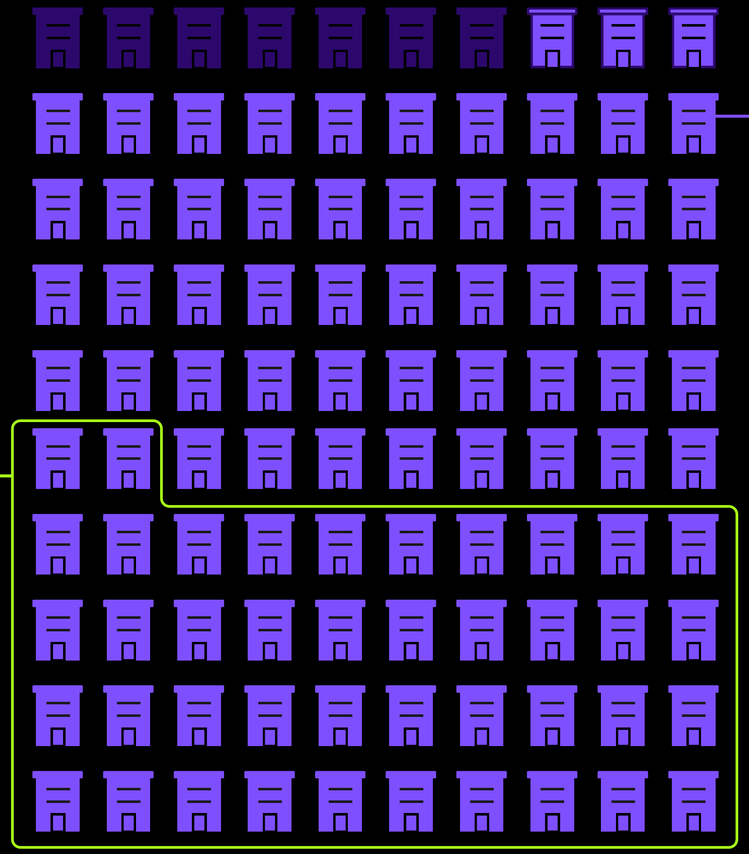
Geography
UK

01
Cyber Fraud: The Primary Culprit in UK Payment Fraud



Trustpair

The Rise of Successful Cyber Attacks



93%

of companies have been victims of attempted payment fraud in the last 12 months

42%

of targeted companies have suffered at least two successful attacks in the last 12 months

01. CYBER FRAUD: THE PRIMARY CULPRIT IN UK PAYMENT FRAUD

Cyber fraud has evolved from an emerging risk to the dominant force in payment fraud, affecting the vast majority of UK businesses. A majority (93%) of companies reported being victims of attempted payment fraud in the past year, highlighting the widespread nature of this threat.

The success rate of these attacks is equally alarming. Among targeted companies, almost half (42%) suffered at least two successful fraud incidents. This troubling statistic underscores the growing capabilities of fraudsters, who now use advanced technologies like AI to execute highly convincing schemes at scale.

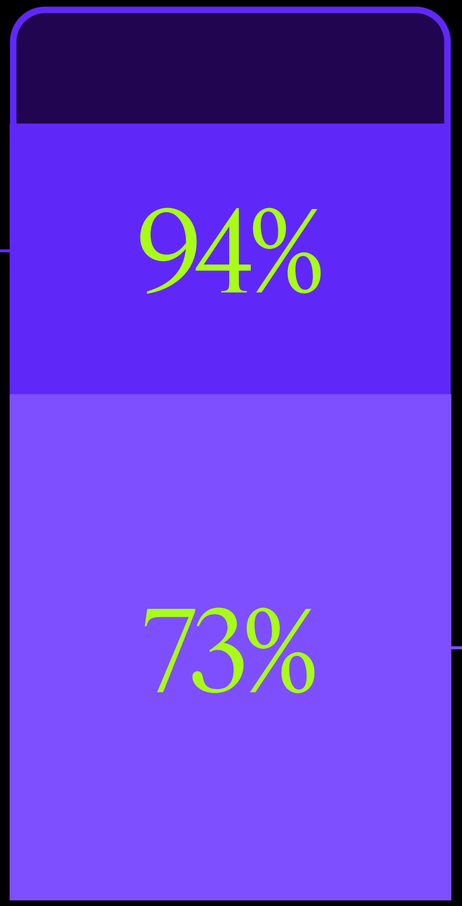
For UK finance leaders, this rapid rise in cyber fraud presents a significant challenge. Nearly 48% identify cyber attacks as their biggest hurdle in fraud prevention, emphasizing the need for more robust defenses. While some companies are making strides, the relentless evolution of cyber fraud calls for a proactive, technology-driven approach. Without comprehensive solutions, businesses remain highly exposed to the escalating risks of cybercrime.

> Cyber fraud has cemented its place as an unavoidable reality for businesses because it is incredibly lucrative for cybercriminals. Unlike physical crimes, cyber fraud offers criminals the ability to operate anonymously, at scale, and across borders with minimal risk of being caught.

Royston Da Costa
Global Treasurer

Investment in Fraud Prevention is Crucial

94% of companies have increased their investment in fraud prevention technologies in 2024



73% anticipate an increase in the risk of payment fraud this year

02
AI-Powered Fraud: A New Era of Threats

Directing Resources to Combat AI Fraud

65% Invested in Technology

65% of companies have invested in technology aimed at protecting against viruses and cyberattacks

62% Cybersecurity Awareness Training

62% are conducting dedicated cybersecurity awareness training for finance and treasury teams

43% Payment Processing Roles

43% of companies minimizing who can make payments to reduce points of exposure

Tools like generative AI, deepfake videos, and voice cloning have drastically altered the fraud landscape, enabling attackers to bypass traditional detection methods with precision and scale.

Fraudsters are increasingly turning to advanced AI technologies to execute highly convincing scams, with 88% of UK businesses identifying cyber fraud as a major driver of payment fraud attempts. Tools like generative AI, deepfake videos, and voice cloning have drastically altered the fraud landscape, enabling attackers to bypass traditional detection methods with precision and scale.

One prominent example is the evolution of Business Email Compromise (BEC) scams. What once involved poorly written emails has transformed into AI-generated messages that flawlessly mimic executive communication styles, company-specific language, and protocols. These attacks have surged in frequency and effectiveness, becoming the leading fraud channel due to their ability to evade standard verification measures.

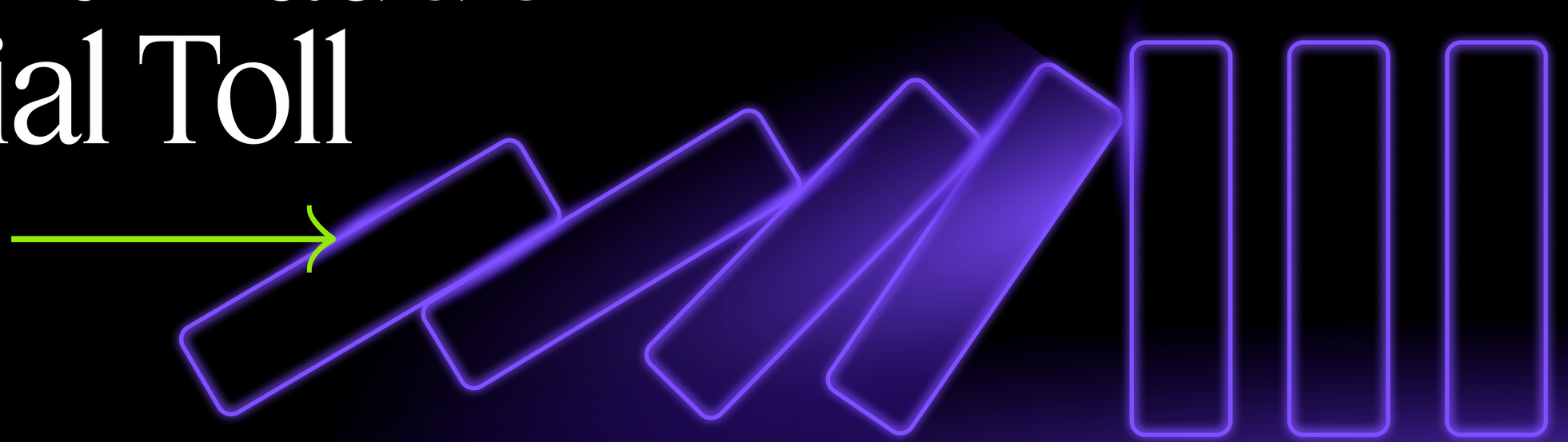
To counter this shift, companies must rethink their fraud detection strategies. Moving beyond traditional manual reviews, businesses need automated verification systems capable of detecting the nuanced patterns and anomalies inherent in AI-generated fraud attempts. Only by leveraging technology at the same pace as fraudsters can organizations safeguard their payment processes and stay ahead of these emerging threats.

Tom Abbey
Senior Fraud Consultant UK

> While businesses celebrate the advancements AI brings to efficiency and innovation, criminals are just as excited about its potential, albeit for entirely different reasons. AI equips fraudsters with powerful tools to operate more quietly, effectively, and at an unprecedented scale.

03

The Cost of Inaction: Payment Fraud's Financial Toll



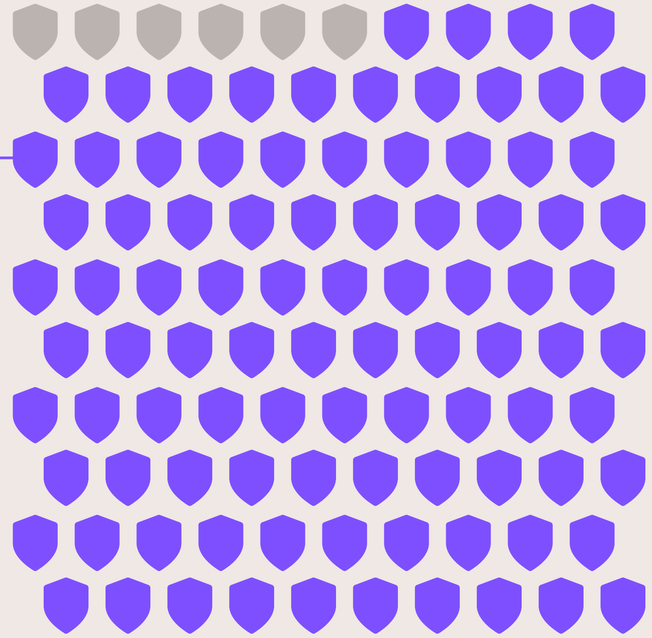
Financial Losses Are Steep

21% of Businesses That Fell Victim to Successful Fraud Incidents Reported Average Financial Losses of £500,000 Per Attack

The Significant Increase In Fraud Prevention Technology

94%

reported increasing their investments in fraud prevention technologies with 44% making significant upgrades



Payment fraud is not just a technological challenge - it's a financial one, with businesses across the UK feeling the strain. In 2024, the majority of companies (94%) reported increasing their investments in fraud prevention technologies, with almost half (44%) making significant upgrades. Yet, the cost of inaction remains staggering: 21% of businesses that fell victim to successful fraud incidents reported average financial losses of £500,000 per attack.

To combat this growing threat, companies are directing resources toward bolstering their defenses. Two-thirds (65%) have invested in technology aimed at protecting against viruses and cyberattacks, while 62% are conducting dedicated cybersecurity awareness training for finance and treasury teams. This dual approach targets both technological vulnerabilities and the human element of fraud, recognizing that education and awareness are as crucial as firewalls. Additionally, 43% of businesses are limiting payment authority to reduce points of exposure, minimizing the risk of unauthorized transactions.

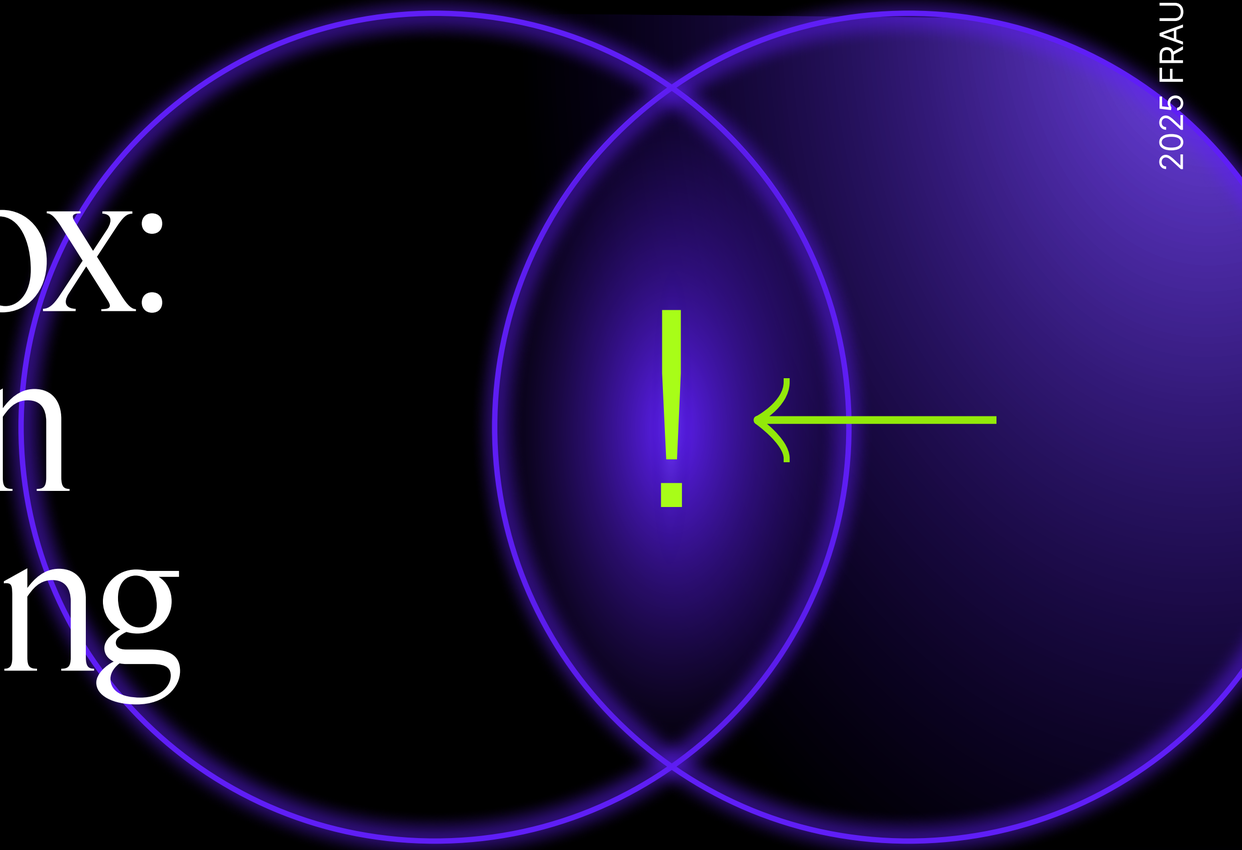
Despite these efforts, the financial toll of fraud underscores the importance of taking proactive measures. Every successful attack chips away at company profits undermines trust, and exposes critical vulnerabilities.

What concerns me most is the lack of decisive action to address payment fraud. Existing regulations often fail to cover the real threats businesses face, leaving them exposed without essential cybersecurity measures or cyber insurance. This inaction puts companies at risk of devastating financial and operational losses.

Royston Da Costa
Global Treasurer

04

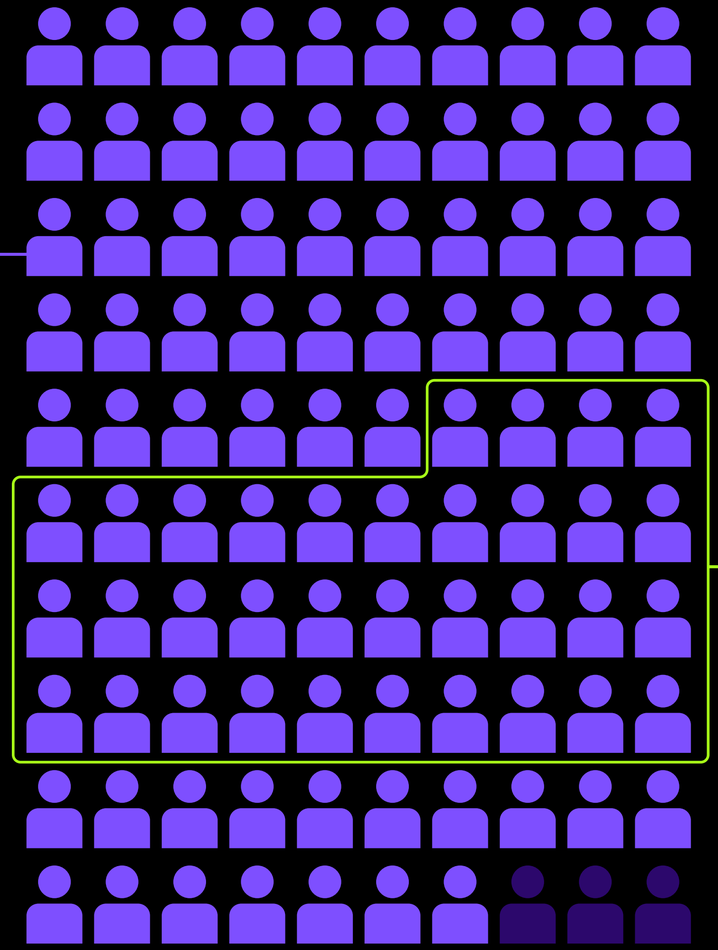
The Fraud Paradox: Overconfidence in the Face of Growing Cyber Risks



The Inbalance In Fraud Attacks vs. Prevention

97%

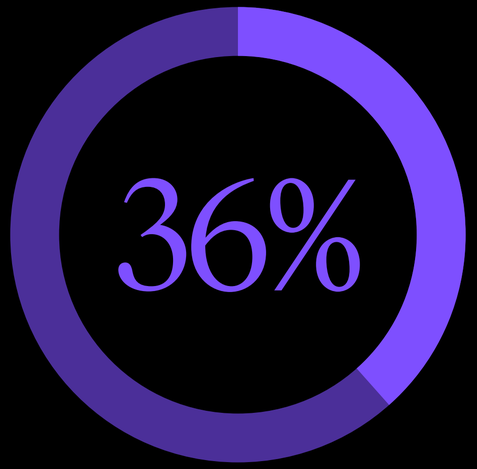
of decision-makers believe their team members can identify advanced fraud tactics...



44%

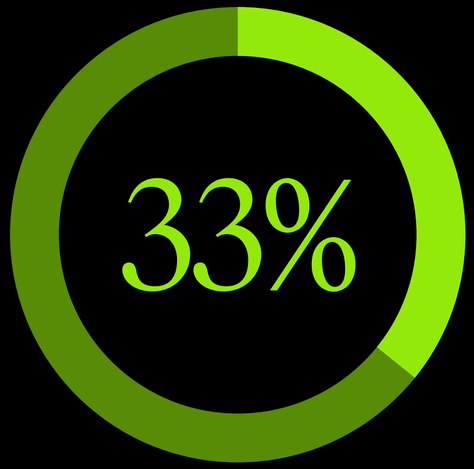
...with 44% claiming they are “very confident.”

The Inbalance In Fraud Education vs. Automation



Better Education May Reduce Fraud

36% of executives believe that better education and training would most effectively reduce fraud



Reducing Human Error

33% of executives emphasise increasing automation in fraud prevention processes to minimise human error

Most organisations are taking steps to address the issue - 90% report providing formal training on detecting and preventing cyber fraud schemes like phishing and deepfake attacks in the past year. This training has instilled a high degree of confidence: 97% of decision-makers believe their team members can identify advanced fraud tactics, with 44% claiming they are "very confident."

Yet, this confidence often contrasts sharply with reality. Payment fraud incidents remain prevalent, with 73% of businesses anticipating a rise in fraud risk this year. Meanwhile, 65% of organizations cite fraud prevention as a top concern for 2025. This disconnect suggests that while training and awareness are critical, they are not enough to mitigate the sophisticated strategies fraudsters employ.

Despite widespread awareness and investment in fraud prevention, a troubling paradox exists between companies' confidence in their ability to detect fraud and the actual frequency of successful fraud attacks.

Bridging the confidence gap requires a dual approach: empowering teams with deeper knowledge while leveraging advanced technologies to counter the evolving threat landscape.

There's a clear paradox: leaders are confident their teams can detect fraud, yet incidents remain alarmingly high. This overconfidence may blind companies to the evolving tactics of cybercriminals, as sophisticated schemes like deepfakes and business email compromise outpace traditional detection methods.

Tom Abbey
Senior Fraud Consultant UK, Trustpair

05 Strengthening Defenses: A Unified Company-Wide Approach

Companies Defense Measures to Protect Against Fraud

55%
Fraud Awareness Training

of companies invest in fraud awareness training

68%
Team Collaboration

of companies report collaboration between procurement, accounts payable, finance, treasury, and IT teams

49%
Prevention Software

deploy fraud prevention software alongside verification of vendor information

> As UK businesses confront the escalating risk of payment fraud, many are reassessing their defense strategies and focusing on enhancing both their internal controls and external verification tools.

The data paints a clear picture of where organizations are directing their attention to tackle this growing threat.

Automation was highlighted by 33% of companies as an area of focus, recognizing that reducing human error through automated fraud detection processes can improve accuracy and responsiveness, especially in fast-paced financial environments. Payment fraud follows closely behind at 65%, further demonstrating the pressing need for advanced fraud prevention mechanisms.

A bright spot in the landscape is the widespread use of Confirmation of Payee (CoP), with 77% of companies adopting this system and an impressive 96% agreeing on its effectiveness in preventing fraud. However, CoP alone is not sufficient for global organizations. While it works well in specific markets, companies operating across borders face unique challenges that demand more comprehensive solutions. To effectively safeguard against fraud on a global scale, businesses need to complement local security measures like CoP with advanced automation tools and technologies that provide broader, integrated protection.

Although many businesses implement multiple fraud defenses, such as double-checking procedures and raising staff awareness, situational checks remain central to the process, particularly in high-risk scenarios. 48% of companies focus on verifying payments when suppliers make unexpected requests, and 47% take extra precautions when working with high-risk suppliers or entering new markets. However, only a minority -

1 in 10 companies, conduct checks throughout the entire supplier payment process, underscoring the need for more consistent and proactive verification at every transaction stage.

We cannot approach cybersecurity from just one angle. It's not enough to say, 'Our staff is trained; we're fine.' It's about combining efforts—internal audits, processes, training, and stakeholder engagement—to build resilience.

Royston Da Costa
Global Treasurer

Conclusion

The 2025 fraud landscape demands a decisive shift in how businesses protect themselves. With 93% of companies targeted by cyber fraud and advanced tactics like generative AI on the rise, traditional methods like manual controls and training are no longer sufficient.

The stakes are high: businesses risk severe financial losses and reputational damage without robust defenses.

The CoP system stands out as a vital tool in combating fraud, yet despite its proven success, it is often underutilized, with checks primarily occurring in high-risk or unusual situations. However, for global businesses, relying on CoP alone may not be enough. Expanding its use across all stages of the payment process, while also integrating additional global security tools, could provide businesses with a more advanced, multi-layered defense.

This combined approach of education, automation, and robust verification systems is critical as companies continue to battle rising fraud risks in 2025. By strengthening these measures, UK businesses can better protect themselves from the increasingly sophisticated fraud tactics that threaten their financial security.

Trustpair

2025
FRAUD REPORT

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 SAS | contact@trustpair.com