Treasury Dragons
Payment Fraud

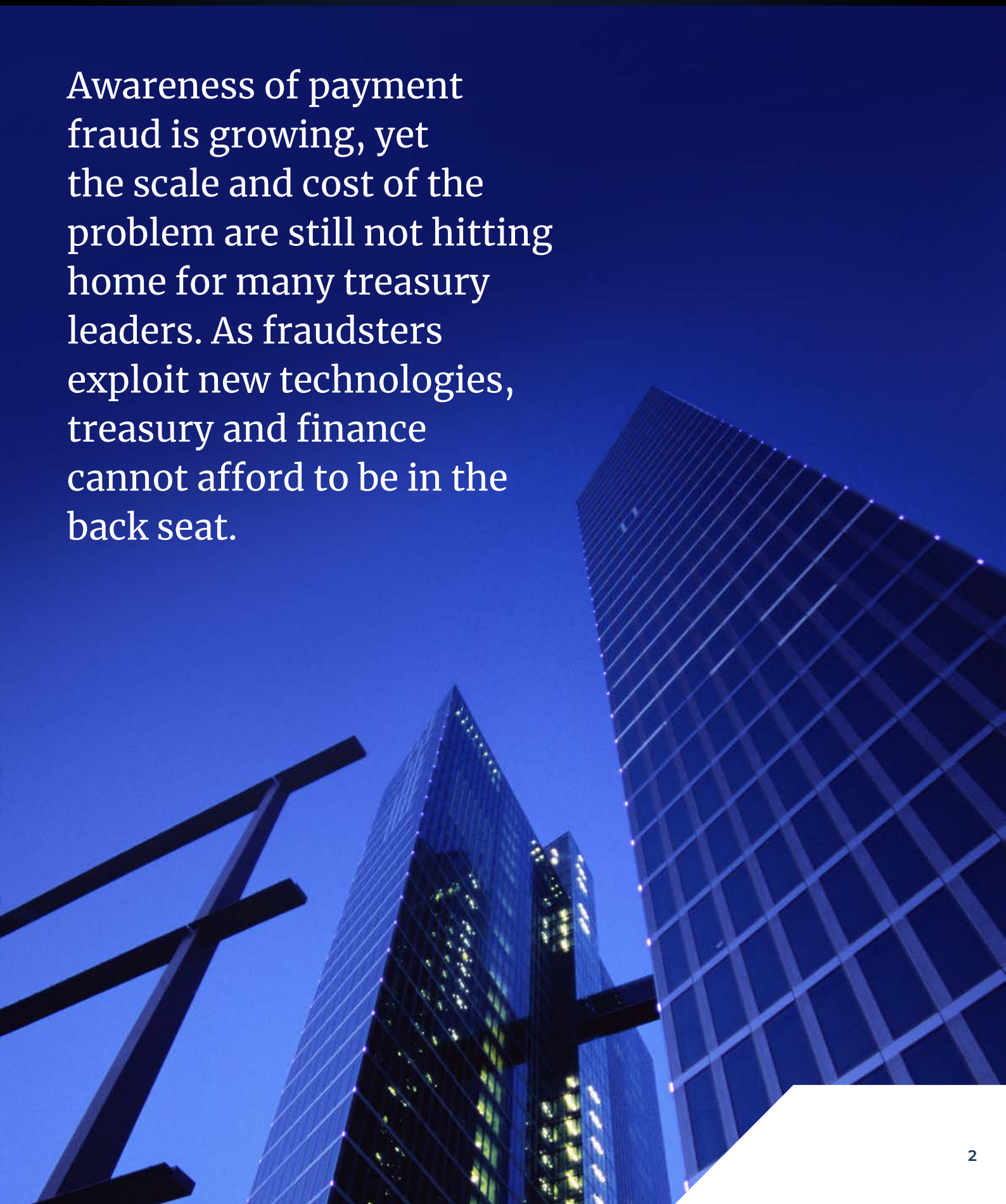
Research Report

Is treasury in denial on payment fraud?

sponsored by

nsknox

Awareness of payment fraud is growing, yet the scale and cost of the problem are still not hitting home for many treasury leaders. As fraudsters exploit new technologies, treasury and finance cannot afford to be in the back seat.

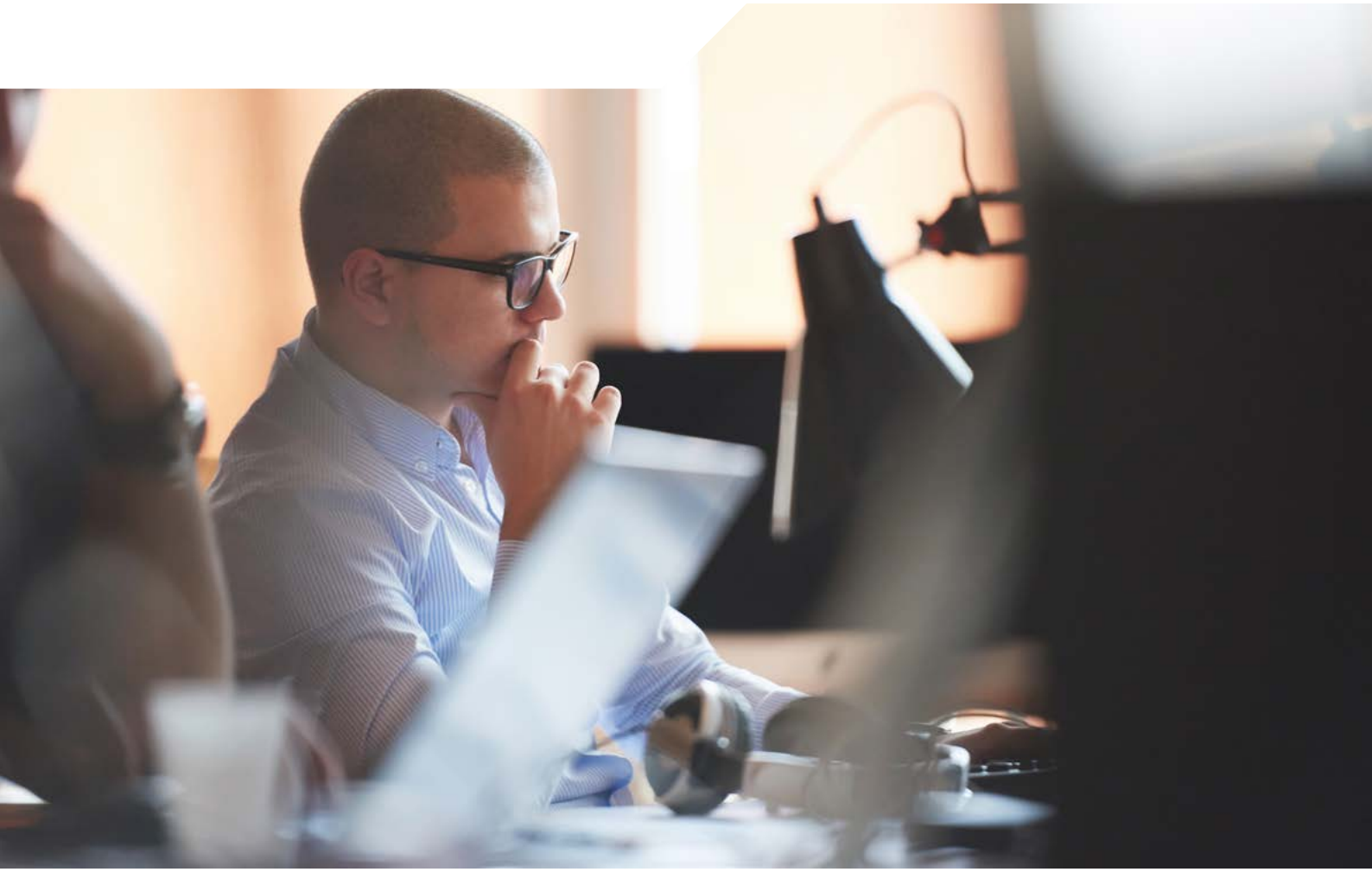


In today's rapidly evolving digital landscape, payment fraud has reached new heights, and the costs are staggering. This is particularly the case for business-to-business payment fraud, where the higher-value opportunity is drawing more sophisticated fraud techniques. Business e-mail compromise fraud alone reached $2.7bn billion in the US last year[1], while in the UK, the government estimates the cost of payment fraud in the private sector at more than £45 billion annually.[2]

Gone are the days when paper cheques and physical signature authorisation were the most relevant concerns. The transition from traditional paper-based payments to electronic systems has unlocked unprecedented efficiency and reduced the obvious fraud risk of paper checks. However, this digital evolution has not been without its challenges, particularly in the realm of payment fraud. As companies embrace electronic payments, finance leaders find themselves at the forefront of the fight against sophisticated fraudulent schemes.

The shift towards electronic payments has necessitated a paradigm shift in risk management that requires engagement from a spectrum of stakeholders. Effective payment fraud prevention requires a combination of technologies, processes, and people that go beyond a single organisation and require coordination, or at least a level of understanding, across multiple players in a supply chain or ecosystem.

As commerce and supply chains digitise, the risk grows, and new threats emerge with technologies like artificial intelligence (AI). With AI's potential for more human-like behaviour, deep-fake emails, documents, and video calls become more challenging to identify and are driving a new wave of business email compromise scams.[3]



1. FBI Internet Crime Report 2022
2. https://www.pymnts.com/news/b2b-payments/2020/tessian-deepfake-bec-scam/
3. https://www.gov.uk/government/news/cost-of-fraud-revealed-in-new-report

To highlight today's evolving challenges of corporate payment fraud, Treasury Dragons and nsKnox surveyed 100 treasurers and finance leaders worldwide.[4] With such a rapidly evolving threat, it is little wonder that awareness and ownership of payment fraud are still two critical themes.

Underestimating the prevalence and cost of B2B payment fraud

Corporate payment fraud is pervasive. Our survey showed that nearly 90% of companies experienced at least one corporate payment fraud attempt in the past year.

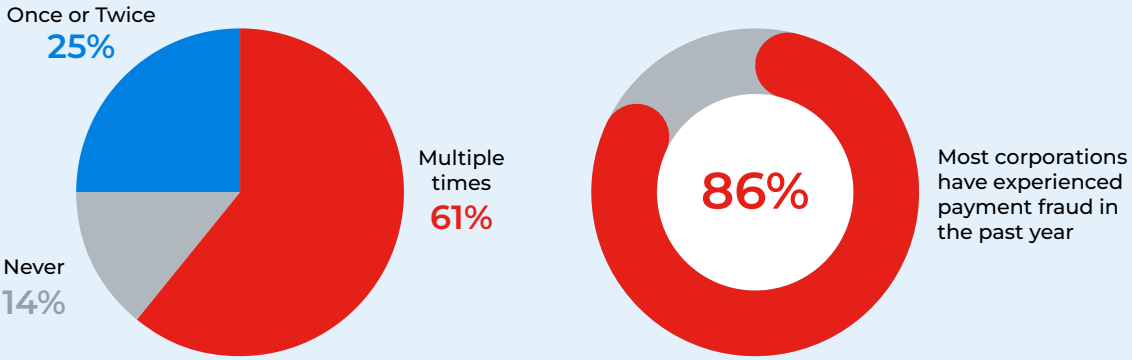
Yet perception is still a long way from this reality. When we asked our finance leaders what proportion of companies they believed experienced payment fraud, only half came close to the actual figure. Almost a third of respondents thought fewer than 50% of companies experienced payment fraud annually.

To bring home this point of perception versus reality, we asked our survey respondents about the importance of payment fraud prevention to each business. Side by side, the answers are revealing.

Most finance leaders (84%) said that they consider payment fraud a serious or critical risk to their business. Yet only 69% said that their organisation is actively managing payment fraud.

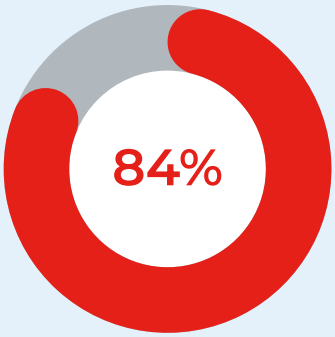
These figures reveal a worrying truth: despite the acknowledged seriousness of the threat, almost a third of finance leaders do not believe their organisations are managing it effectively. This may be due to a need for more awareness of the danger across the organisation: Only half of those we surveyed said that awareness was high enough.

Fraud attacks in the last year

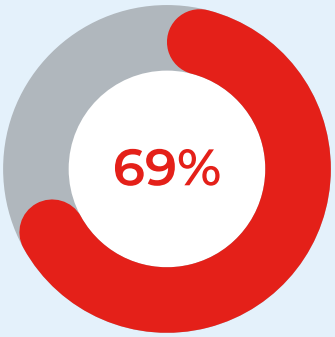


While almost 9 in 10 firms say they have experienced attempted payment fraud in the past year, treasurers' perceptions are that the amount is much lower. Almost a third of respondents thought fewer than 50% of companies experienced payment fraud annually.

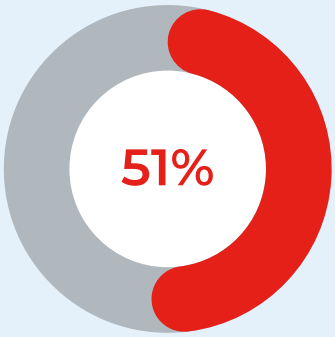
4. Survey conducted Feb-May 2023 among a global sample of 100 senior corporate treasury professionals in non-financial services companies with revenues above $300m



Those that consider payment fraud risk serious or critical to their business



Those that say they very actively manage payment fraud



Those that say awareness in their business is high or very high

84% think payment fraud risk is serious or critical to their business, but only 69% very actively manage it and only half say awareness of the problem is high.

The awareness challenge can go even deeper as technologies such as real-time payments and application programming interfaces (APIs) gain traction, and the speed and complexity of the techniques used by fraudsters increase. If finance leaders don't keep pace, they risk the Dunning-Kruger effect: overconfidence in a subject where their knowledge is low. In many cases, this lack of awareness means firms don't even know when they have been impacted or the true financial costs of payment fraud. Our survey illustrates this, as those with lower awareness levels consistently reported both fewer fraud attempts and fewer successful payment frauds.

The cost of payment fraud is also vastly underestimated. In comparison with the $2.7bn quoted in the introduction for BEC in the US alone, more than half of our treasury and finance leaders (58%) believed that the annual global cost of commercial payment fraud was less than one billion dollars.

This data points to an urgent need for finance and treasury to act. The first step in this process requires raising and maintaining technical awareness among leaders and practitioners. Without a clear vision of the scale of the problem, the setting of priorities and allocation of resources will fail to keep up with the growth of the threat.

Everyone is responsible, so no one is

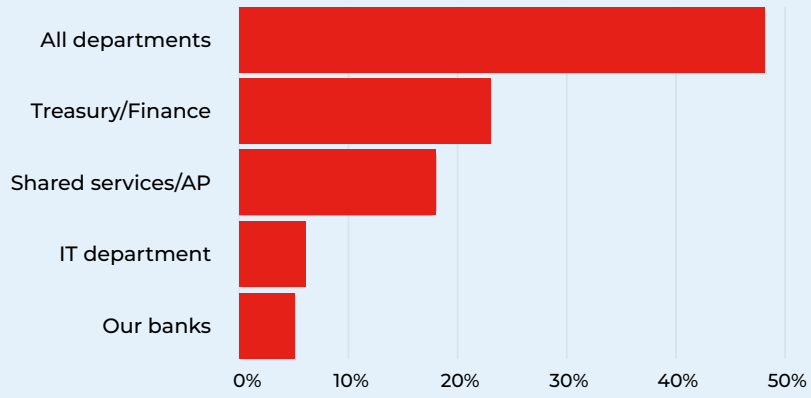
A second key theme from our survey is the challenge of ultimate ownership and accountability for managing payment fraud. On this subject, the BBC (UK) recently called payment fraud a "responsibility vacuum"' or "everyone's problem, but no one's priority".[5]

Our survey shows that many treasurers believe that finance, treasury, and accounts payable functions all have a role to play in combating fraud. However, the most popular answer, 'All departments, ' highlights a risk that everyone will believe that fraud prevention is not their personal responsibility.

Traditionally, fighting payment fraud has been the domain of banks and credit card providers. As the threat has digitised, IT departments have come to the fore in managing email traffic, data integrity and system security. Yet, most successful payment fraud involves an element of social engineering, and as this has become clearer, the responsibility and liability for this risk have slowly shifted to users.

The challenge is: with whom does the buck stop? Everyone involved knows that managing payment fraud is essential, but it takes coordinated action and clear accountability to implement solutions that apply to end-to-end processes involving banks, finance, treasury, shared services, and IT. In reality, the buck often stops where the cost lies. As the politics play out, this means that treasurers and finance leaders have to step up to the plate and take as much accountability as possible.

Who is responsible for managing payment fraud?



Many treasurers understand that fighting payment fraud is everyone's responsibility. Yet a significant minority believe departments other than treasury should be taking the lead.

5. https://www.bbc.co.uk/news/business-55769991

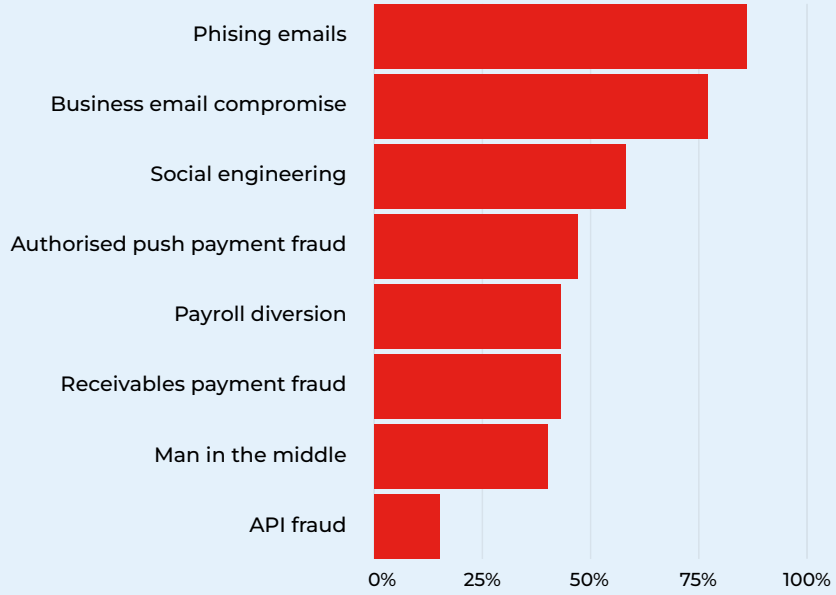
The emerging threat of receivables fraud

The overlapping challenges discussed so far are highlighted by the emerging threat of receivables (or incoming) payment fraud. Accounts payable and receivable are just two sides of the same coin, and the risk of incoming payment fraud aptly illustrates the challenge of accountability for payment fraud.

Some may perceive payment fraud as a risk only for the payer function, yet the legal implications are increasingly nuanced. Receivables payment fraud generally refers to diverting a customer payment where the fraudulent activity originated from within the receiver's organisation through a breached email or a bad internal actor. In this case, the receiver may be held accountable for the payment loss. Even in cases where the breach takes place in the payer's business, a "blame game" often ensues and the ultimate cost of lost business and cashflow rests on the corporate receiving the payment. This means diligent finance teams are now monitoring and actively managing upstream and downstream payment flows, and are increasingly using secured means of transmitting sensitive bank details to limit interception by fraudsters.

While most survey respondents were aware of more mature payment fraud concepts, like phishing emails and social engineering, awareness of the main types of B2B payment fraud was much lower. Awareness of emerging threats like receivables payment fraud was even lower, with less than half of those surveyed saying they understood the term. For the new digital threat of API fraud, the level of awareness was only 15%. This raises a fundamental question about how companies can sustainably keep pace with the new array of digital threats.

Which types of fraud are you aware of?



Phishing emails are the best-known type of fraud amongst corporate treasurers, with business e-mail compromise (BEC) close behind.

More education may be needed on lesser-known tactics such as Man-in-the-Middle or API fraud.

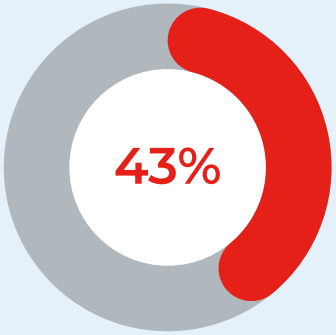
The growing role of technology solutions

This increasing array of digital threats requires digital solutions. With more sophisticated fraudsters, manual processes are no longer adequate. Yet, despite the technical nature of payment fraud and how critical the concern is to most businesses, there appears to be severe underinvestment in technology solutions.

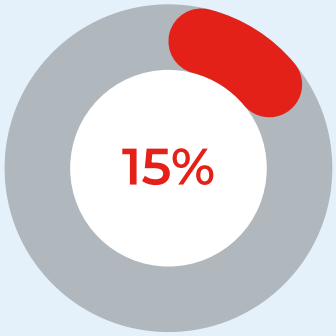
Our survey showed that just 43% of firms currently have a technology solution in place to reduce the risk of payment fraud. For newer threats like incoming payment fraud, the number of companies with technology in place that can mitigate this risk falls to just 15%. Nearly two-thirds of the firms surveyed said that their current response to managing incoming payment fraud was “extra vigilance”. Yet, given the themes highlighted in our survey and the challenge of maintaining the right level of technical awareness, this is not a sustainable approach.

Where automated systems are in place, they need to be integrated and progressive. Most of us understand the process of buying antivirus software for a computer and the importance of a solution that keeps up-to-date with the latest threats. That same principle should apply to corporate payment fraud solutions.

Our survey showed that technology solutions are currently focused on monitoring payments and on detection. Half of the current systems in place have anomaly detection as their primary function, with fewer systems focused on the accuracy of master data and verification of account details.



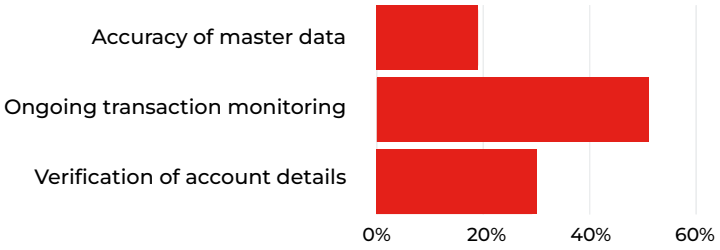
Have an automated system in place



Have an automated system for incoming payment fraud

Despite relatively high levels of awareness of fraud, fewer than half of treasurers say they have an automated system in place to help fight it - and fewer than one in six have a system that specifically targets incoming payment fraud.

Functions of automated systems



Where firms use automated systems to prevent fraud, half of them have ongoing transaction monitoring but far fewer check the accuracy of master data.

While anomaly detection is a mature technology application for payment fraud, it is arguably the last line of defence. Cybersecurity and payment fraud best practices increasingly advocate the importance of data integrity as a first line of defence. Thus, as verification of account details forms one of the most critical touch-points or handshakes in a payment, a robust fraud protection system needs to provide absolute surety of payment account data at the point of entry and before any payments are made.

Our research clearly highlights opportunities for improvement. While most business leaders acknowledge the importance of protecting against commercial payment fraud to avoid both financial and reputational damage, the true scope of the problem is still underestimated. This translates into underinvestment in the right technology to keep pace with the threat.

Executive attention and commitment are needed. Raising awareness of the scope and the evolving nature of the threat is a first step. As the threats evolve, only a coordinated approach that includes technology and business controls will succeed. Technology solutions need to start with data integrity and remain innovative to counter the ever-evolving tactics of fraudsters. Nevertheless, the most important element of all is accountability. The challenge of corporate payment fraud is an opportunity for finance leaders to take the driver's seat.

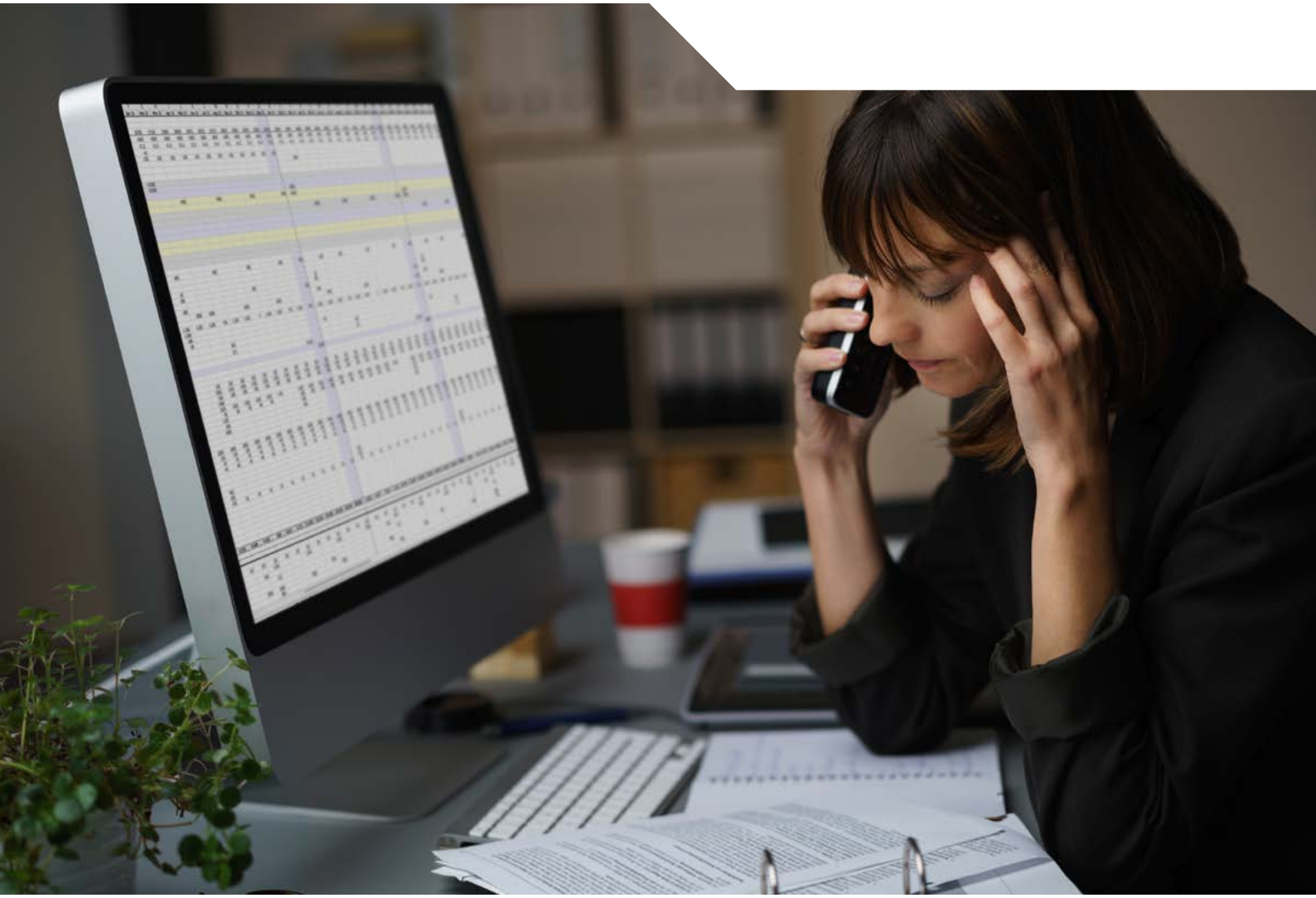
Key takeaways

1. **Awareness** – Executive and practitioner awareness of the scope and technical nature of corporate payment fraud is an ongoing process and is central to ensuring the proper allocation of resources in finance and treasury.

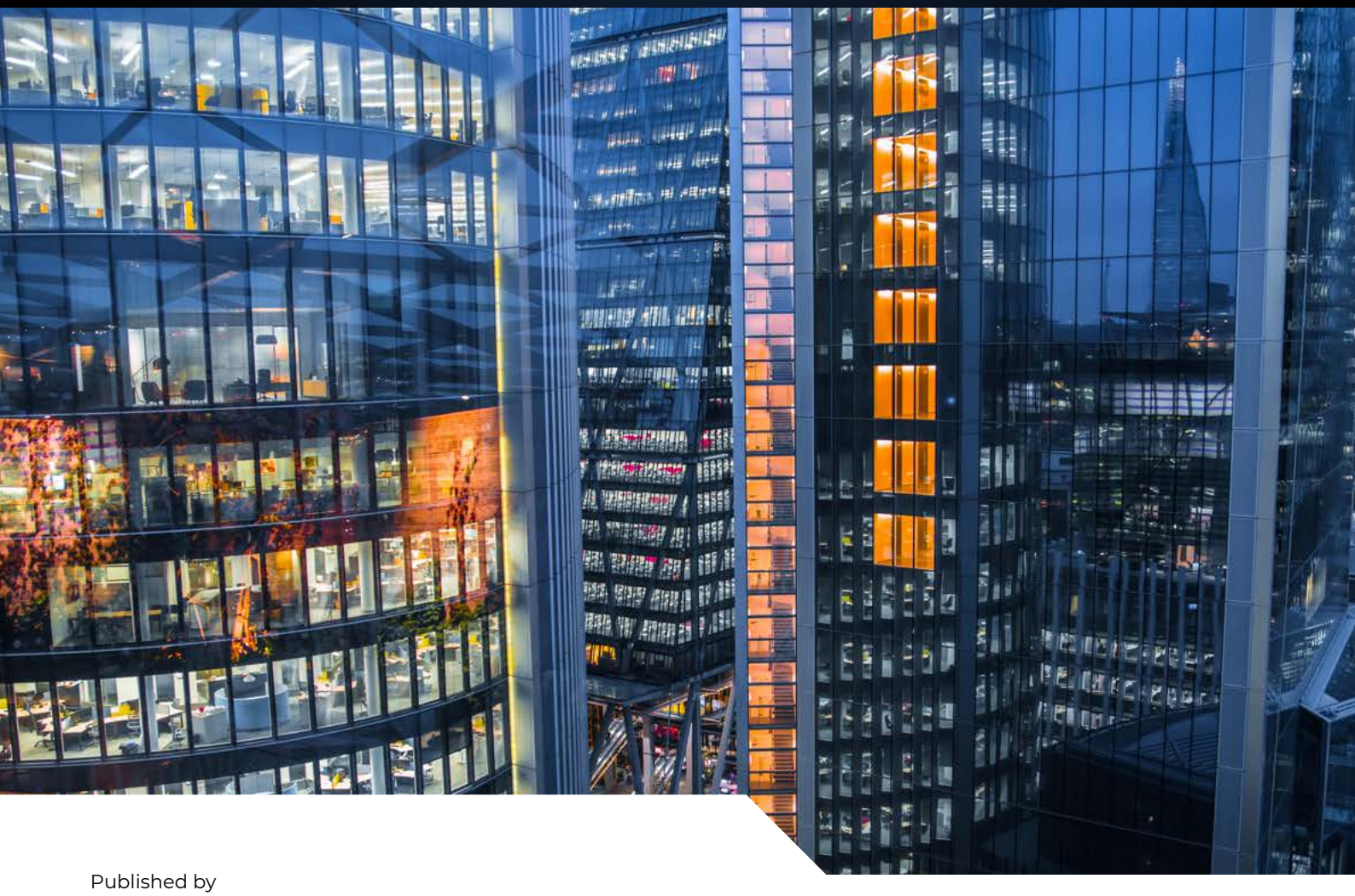
2. **Accountability** – Corporate payment fraud impacts all areas of the business and ecosystem, which can lead to a lack of ownership. For finance and treasury, the buck stops where the costs lie. This represents an opportunity to take the lead.

3. **Investment** – While awareness is critical to ensure the right business controls and industry engagement, only investment in comprehensive and progressive technology solutions will keep pace with modern fraudsters.

4. **Data integrity** – Any technology solution needs to look beyond "last-line-of-defence" anomaly detection to payer bank account validation, master data accuracy, and incoming payment fraud mitigation.



Treasury Dragons
Payment Fraud



Published by

Treasury Dragons, the global network for buyers, specifiers and users of corporate treasury technology.

Adaugeo Media Ltd
Blackwell House
Guildhall Yard
London EC2V 5AE

treasurydragons@adaugeomedia.com

In association with

nsKnox, a fintech-security company, enabling corporations and banks to prevent fraud and ensure compliance in B2B Payments.

contact@nsknox.net

sponsored by

nsknox