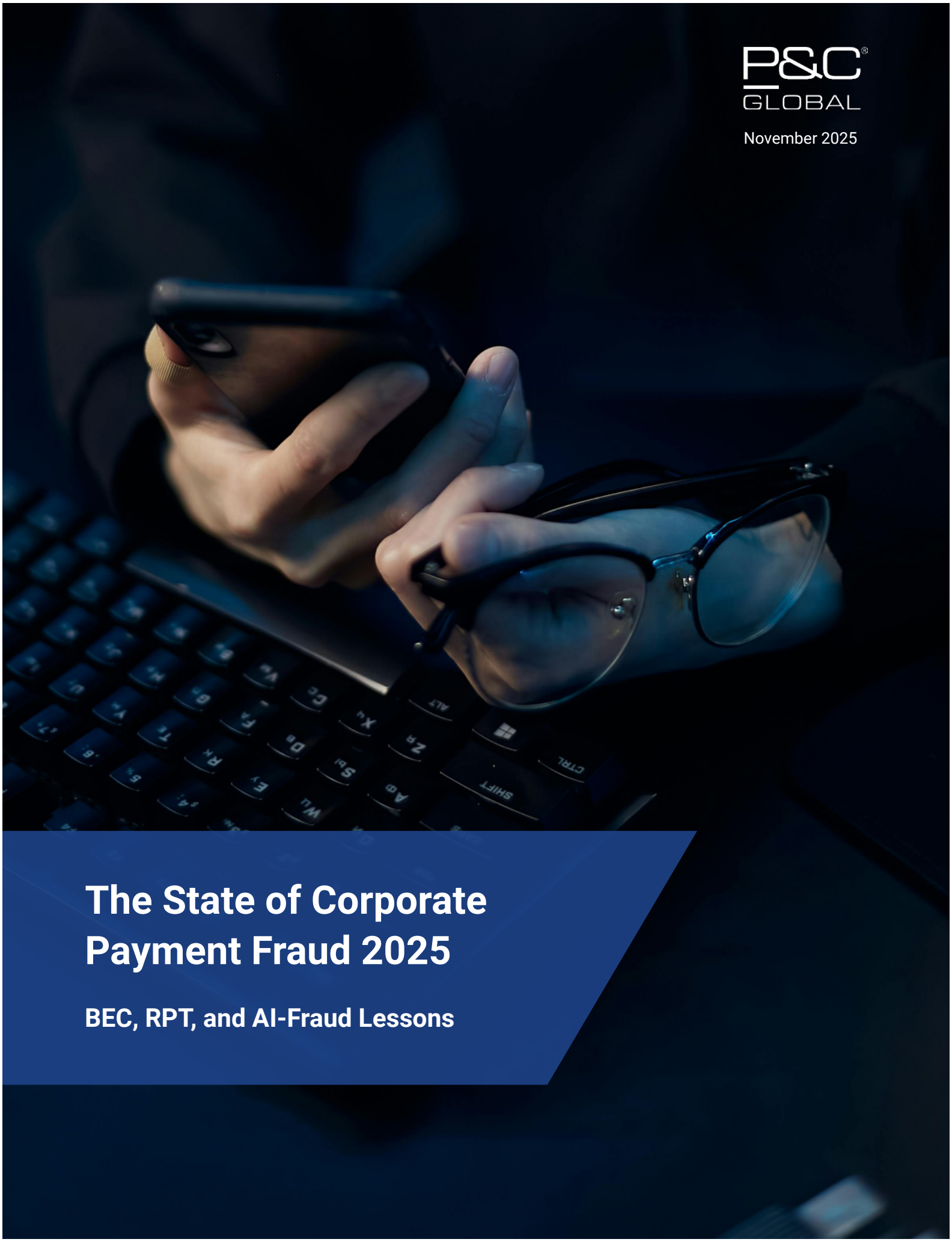


P&C GLOBAL

November 2025

The State of Corporate Payment Fraud 2025

BEC, RPT, and AI-Fraud Lessons

Table of Contents

2025 Fraud Landscape

Corporate Payment Fraud Risk Remains Elevated

Corporate payment fraud continues to surge globally in 2025, maintaining the historic highs reached in 2024 and underscoring the persistent vulnerability of even well-defended enterprises. Nearly 8 in 10 organizations were targeted by an attempted or actual payments fraud in 2024[1], essentially unchanged from the prior year's record highs. This persistence signals that fraudsters continue to outmaneuver traditional controls. Notably, even old-fashioned methods like check fraud are rampant – 63% of firms faced check-related fraud attempts in 2024[2]. Yet the fastest-growing dangers lie in digital and real-time payments, where criminals exploit speed and technology to bypass safeguards.

Key takeaway

Fraud risk in 2025 remains as elevated as ever, but its nature has evolved. Traditional defenses like dual sign-off and static verification protocols must be modernized to handle instant payment fraud, AI-enabled impersonation, and Business Email Compromise (BEC) attacks.

In this brief, we examine the dominant payment fraud trends, emerging attack vectors, and strategic actions Global 1000 executives—CFOs, CROs, and COOs—can take to strengthen organizational defenses.

How Attacks Are Evolving

BEC & Impersonation Fraud

Business Email Compromise (BEC) remains the most pervasive and costly form of corporate payment fraud in 2025. In 2024, 63% of organizations experienced BEC attempts, making it the number-one avenue for corporate funds-transfer fraud [1][3]. BEC schemes typically involve highly convincing impersonation of executives, vendors, or trusted business partners to trick employees into sending money or sensitive data.

In the past year, fraudsters have refined their impersonation tactics, expanding beyond traditional executive spoofing toward vendor and third-party impersonation attacks that exploit operational trust within established payment relationships—a growing issue across the Law Firms and Financial Services sectors:

Shift from CEO Fraud to Vendor Impersonation

Classic BEC scams – where attackers pose as a CEO/CFO requesting a secret funds transfer – are *slightly less common* now, dropping to 49% incidence (from 57%) as companies got wiser to "urgent CEO email" ploys[4]. Instead, scammers are focusing on vendor impersonation fraud and third-party impersonation, which rose sharply. In 2024, 60% of companies reporting BEC saw impostors posing as vendors/suppliers, and 63% saw fraud involving other external parties (e.g. lawyers, clients)[4].

By hijacking or spoofing a vendor's email domain and requesting a change in payment account, criminals exploit the trust in established business relationships. Indeed, "vendor imposter" fraud spiked in 2024 – 45% of firms were hit by it, up from 34% the year prior[3]. Invoice-related scams (fake or altered invoices) also nearly doubled to 24% of companies[3]. This trend shows attackers leveraging the routine nature of accounts payable transactions to slip past defenses.

Beyond Email – Multi-Channel Social Engineering

While spoofed emails remain the primary BEC vector (used in 79% of incidents)[3], fraudsters are not limiting themselves to email alone. Many now follow up with phone calls or text messages impersonating the same party, adding pressure to "urgently process" a payment. Some have even been known to use live chat or messaging apps pretending to be a vendor or executive to add legitimacy. The most audacious are exploiting new technology (discussed below) to impersonate voices on the phone or faces on video calls. The common thread is social engineering – manipulating human trust and established processes.

Costly BEC Losses

Global Case Examples

The financial impact of BEC is enormous. The FBI's Internet Crime Center recorded over *$2.7 billion* in losses to BEC scams in 2024 alone, and nearly $8.5 billion lost over the past three years in the U.S.[5]. Globally, many individual companies – including large, tech-savvy firms – have fallen victim.

In mid-2024, for example, a Singaporean commodity company was tricked into wiring $42 million to a fraudulent account after receiving a convincingly forged supplier email (the email domain was just a letter off)[6][7]. The scheme was only discovered days later when the real supplier complained of non-payment. (In that case authorities, via INTERPOL, managed to freeze and recover most of the funds[8] – an extremely lucky outcome.) In another case, tech giants Google and Facebook unwittingly paid out over $100 million in fake invoices a few years ago[9].

These incidents underscore that no organization is too sophisticated to be targeted or deceived. Attackers often research public filings and social media to personalize their fraud, and they may patiently groom targets over time. High dollar sums, multi-national contexts, and even well-trained staff have not deterred BEC groups.

Strategic Takeaway

Strengthen BEC Controls and Culture

Defending against BEC and impersonation fraud requires *both robust process controls and cultural vigilance*. Best-in-class firms are re-examining their payment workflows with a fine-tooth comb. For example, many have implemented strict verification of payment requests and account changes: if any supplier asks via email to update bank details or a CEO emails wiring instructions, out-of-band confirmation (such as a phone call to a known number on file) is mandatory before execution.

Increasingly, companies use technology solutions to supplement this – such as vendor authentication portals or payee positive-pay services – but the human firewall is equally vital. Regular training and simulated phishing tests help reinforce a healthy skepticism in employees ("trust but verify" culture). The encouraging news is that greater awareness does thwart some fraud – the slight drop in CEO-impersonation scams suggests employees are double-checking unusual executive requests[4]. However, the surge in vendor fraud means fraudsters are pivoting to what works, exploiting any procedural gaps between procurement, accounts payable, and treasury.

CFOs and COOs should ensure those teams work jointly on fraud prevention, maintain updated authorized supplier lists, and flag any deviations from normal payment patterns for secondary review. Ultimately, combating BEC is an exercise in rigorous controls (segregation of duties, verification steps) combined with constant vigilance and cross-team communication.

Fraud Risks in the Age of Real-Time Payments (RTP & FedNow®)

The rollout of new real-time payment networks– such as the U.S. Federal Reserve's FedNow® service (launched in 2023) and The Clearing House's RTP® network – is transforming how money moves. These systems allow instant clearing and settlement 24/7, bringing undeniable efficiency benefits for businesses. However, they also introduce a double-edged sword: the *irrevocability* and speed of real-time payments can amplify fraud risks if not carefully managed. As one industry survey warned, once an instant payment is sent, it is nearly impossible to retrieve the funds[10]. Fraudulent transfers can vanish in seconds, before anyone realizes something is wrong.

How Instant Payments Increase Fraud Impact

The speed of settlement in real-time payment systems significantly shortens the detection and response window. In traditional ACH or wire transfer workflows, finance teams had hours—or even a full business day—to identify and halt suspicious activity. In contrast, FedNow® and RTP® transactions clear in seconds, offering virtually no recovery time if a fraudulent transfer occurs. Executives should be aware of a few key risk dimensions with faster payments:

Reduced Reaction Time in RTP Environments

The operational urgency created by instant payment systems is forcing companies to rethink traditional control frameworks. In the old days of ACH or wire transfers, finance staff might have hours or even a day to detect and stop a suspicious payment. With RTP® and FedNow®, that window shrinks to *minutes or seconds*. This means any oversight or delay in spotting fraud can result in irrevocable loss. Attackers know this and will try to time scams to occur outside of normal business hours or at quarter-end crunch, hoping real-time transfers slip through unchallenged. A small operational lapse can be costly when money moves at internet speed.

Early Fraud Patterns – Lessons from the UK, India, and Others

Other countries' experiences foreshadow what could happen as instant payments grow. The UK, which has had Faster Payments for years, saw Authorized Push Payment (APP) fraud surge to such levels that regulators intervened. (In 2022, APP scams cost UK victims nearly £485 million[11], leading the UK Payment Systems Regulator to mandate reimbursement for many scam victims in 2024.) In India – a leader in real-time UPI payments – fraud incidents rose 23% in one year as instant payments volumes grew[12].

The trade-off between speed and security is real: Plaid's head of product noted that the "flip side" of instant money movement is *more scams*, and stressed the need for safeguards to verify recipients' identities[13]. In short, if proper controls aren't built around faster payments, fraud will fill the void.

Controls for RTP and FedNow® Fraud

The industry isn't blind to these dangers. The U.S. Federal Reserve has made fraud mitigation a top focus as FedNow® gains users. Banks are demanding fraud tools – in early use, FedNow® volume was modest, but participant concern about scams was high[14][15]. FedNow's® team is rolling out configurable fraud controls (e.g. allowing banks to set limits on transaction velocity or value for certain clients) and considering an "alias directory" to mask account details[16][17].

On the corporate side, leading companies are implementing their own precautions. Many organizations choose to start with lower limits on real-time payments or restrict them to known, routine counterparties until confidence grows. Treasury teams are exploring technology that can perform instant account name matching and sanctions screening on outbound payments. (Indeed, Europe is requiring all Eurozone banks must offer free *"Verification of Payee" services so payers can confirm the beneficiary name matches the account before an instant transfer*[18][19].) Such measures add friction, but greatly reduce mistakes.

Takeaway

Balance Speed with Strong Controls

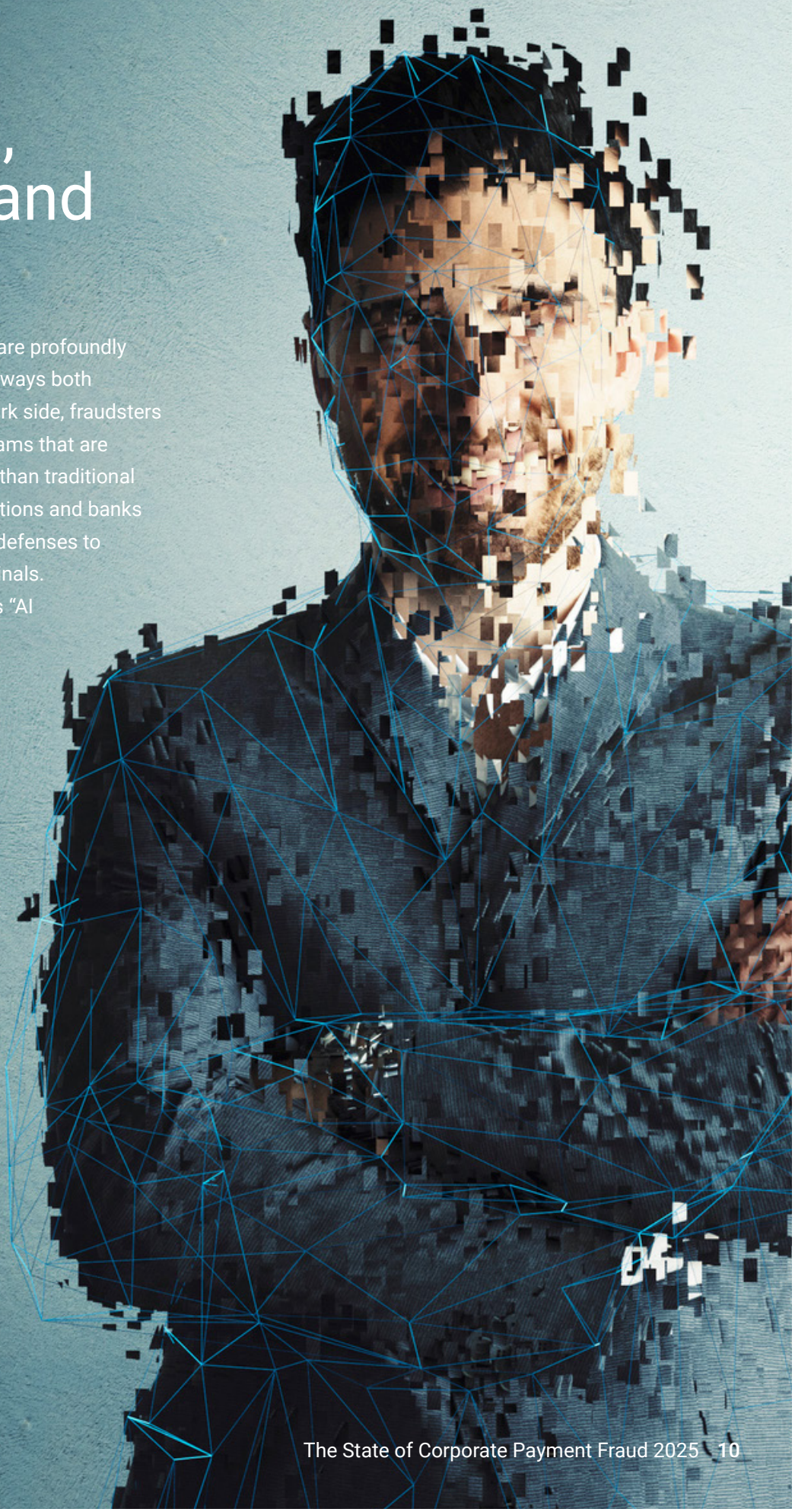
Embrace real-time payments for the competitive and efficiency advantages, but do so deliberately and with enhanced controls. Treat any instant payment like handing over cash – double-check the details every time. Concrete steps include: enabling transaction alerts and dual-approval workflows for RTP/FedNow® transactions (so that no single employee can push through a fast payment unilaterally), setting hard and soft limits on amount and volume (as a fraud "circuit breaker"), and utilizing bank services or third-party tools for account verification.

Crucially, maintain strong incident response plans with your banking partners – know whom to call *immediately* if a suspicious instant payment is noticed, as law enforcement must be engaged within hours for any hope of recovery. With prudent risk management, companies can enjoy the speed of modern payments without becoming easy prey.

AI-Driven Fraud

Deepfakes, Chatbots, and Defense

Advances in artificial intelligence are profoundly impacting the fraud landscape, in ways both pernicious and positive. On the dark side, fraudsters are weaponizing AI to conduct scams that are far more convincing and scalable than traditional tactics. At the same time, corporations and banks are beginning to deploy AI-driven defenses to detect anomalies and outwit criminals. For the C-suite, understanding this "AI arms race" is now essential.



Deepfake Voice and Video Attacks

Criminals have enthusiastically adopted generative AI tools to enhance social engineering. Phishing emails can be auto-generated with perfect grammar and personalized details, making them harder for employees to recognize as fake. More alarming are deepfakes – AI-generated synthetic voices, images, or videos that mimic real people.

In 2024, fraud groups used deepfake audio and video to execute *startling* heists. One UK company, engineering firm Arup, fell victim to a sophisticated con in which an employee participated in what appeared to be a routine video call with senior managers – except the executives on screen and voice were AI-generated deepfakes. The impostors convinced the employee to transfer $25 million to their account[20]. No malware was involved; it was pure deception via technology. Separately, the CEO of a major advertising firm (WPP) was targeted by scammers who cloned his voice and image to impersonate him on WhatsApp and in virtual meetings – urging colleagues to initiate secret transactions (fortunately, that attempt failed)[21][22].

These cases, though still relatively uncommon, show what is now *possible*. As one media report noted, AI voice clones have already fooled banks and duped financial firms out of millions[22]. Deepfake scams are essentially BEC on steroids – if an email from "the CEO" can trick some employees, a live phone call from the CEO's exact voice or a video of an executive's face can be even more compelling. Beyond deepfakes, AI chatbots can be used by fraudsters to interact with victims in real-time (for example, pretending to be customer support to steal credentials), and AI can rapidly generate fake documents or website content to support a con. In short, criminals now have a potent kit: AI gives them *scale, personalization, and believability* that were hard to achieve before.

AI for Fraud Detection and Analytics

On the positive side, AI and machine learning technologies offer powerful capabilities to detect fraud patterns and anomalous behavior that humans might miss. Modern enterprise fraud management systems increasingly use ML models to analyze large volumes of transactions and communications, flagging those that deviate from normal patterns. For example, AI can learn the typical spending and payment habits in a company's accounts payable and alert if a new payee or an unusually large invoice shows up out of cycle.

Behavioral analytics can also monitor user actions in real time – if a finance officer suddenly logs in at 3 AM from a new location and initiates a wire, the system can pause the transaction pending verification. Banks are providing some of these AI-driven safeguards as services to clients, and third-party fintechs offer add-on solutions that integrate with ERP systems to screen payments. Despite the promise, corporate adoption of AI for fraud prevention is still nascent. According to the AFP survey, relatively few organizations have fully integrated AI into their fraud controls so far[23].

Business leaders remain cautious, but there is a growing recognition that legacy rule-based controls are not enough against agile, AI-enabled adversaries. In fact, the AFP reports explicitly calls out that while fraudsters are using AI to great effect, corporate adoption of AI tools to "predict and detect fraud" needs to accelerate[23]. Forward-looking CFOs and CIOs are starting to invest in these technologies – balancing the cost against the potentially massive losses (financial and reputational) that a major fraud incident could inflict?

Takeaway

Use AI to Counter AI

Awareness is step one – executives must acknowledge that seeing is no longer believing in the era of AI. A voice on the phone or even a video conference can be spoofed. Cultivate a healthy skepticism in your organization: as Arup's CIO remarked after their deepfake ordeal, employees now "*really do have to start questioning what we see and hear*."[24]

From a controls standpoint, consider adding multi-factor authentication for non-routine approvals (for instance, requiring a second manager's sign-off via a different channel if a request comes via voice call). Establish code phrases or verification questions for urgent requests made by executives over phone/video, to ensure authenticity. On the technology front, evaluate AI/ML-based fraud detection tools – many can integrate with your payment systems to provide an extra layer of real-time scrutiny. Additionally, stay abreast of emerging defensive tech: for example, some vendors are developing deepfake detection software that can analyze audio/video for signs of manipulation. While not foolproof, these could be valuable for high-risk transactions (e.g. a tool that alerts if a voicemail from a known executive doesn't quite match their past voice profile).

Lastly, plan for the worst: incorporate AI-enabled fraud scenarios into your incident response plans. If a deepfake attack hit your firm tomorrow, do employees know how to respond? The companies that have survived such attempts did so because alert staff spotted something "off" and acted quickly[25]. In summary, AI is raising the stakes on both sides – it can be a tremendous ally in parsing data and pinpointing fraud, but it's also turbocharging the tactics of criminals. Leaders must invest in *both* people and technology to stay one step ahead.

Regulation & Insurance

Shaping Fraud Risk in 2025

Around the world, regulators and insurance underwriters are responding to the persistent wave of payment fraud with new requirements and standards. Global 1000 companies face higher expectations to have strong fraud controls, and those that fall victim may find less leniency (and less financial coverage) than in the past. Here are key developments on these fronts:

Regulators Expect Proactive Fraud Prevention

Regulators are increasingly treating cyber-enabled fraud as a systemic risk that must be addressed through policy. In the U.S., banking rules are being adjusted to improve fraud recovery. For instance, NACHA (which governs ACH payments) has approved rule changes effective 2026 to reduce BEC fraud and make it easier to claw back funds after a fraud incident[26]. While the details are technical, the thrust is that banks and payment operators will be taking more responsibility to quickly freeze and return stolen funds – a recognition of the growing fraud problem.

In Europe, as noted, the new Instant Payments Regulation mandates name-check services to curb misdirected payments[18][19], and ongoing regulatory discussions (like the proposed PSD3 directive) emphasize fraud prevention and customer authentication. Perhaps the most striking shift is in the U.K., where a "*failure to prevent fraud*" corporate offense was introduced in 2023 (and became effective September 2025). Under this law, large companies can be held criminally liable if they don't have reasonable fraud prevention procedures and an associated person commits a fraud benefiting the company[27][28]. While that law is aimed at internal and procurement fraud (preventing companies from unwittingly benefiting from fraud), its message resonates broadly: regulators want organizations to actively guard against fraud, not just react after the fact. Large firms are expected to perform fraud risk assessments, implement controls, train staff, and document their efforts to deter fraud[29][30]. Failing to do so could invite not only financial loss but regulatory sanctions and legal liability.

In practical terms, CFOs and CROs should ensure their fraud risk management programs align with the evolving regulatory guidance and coordinate with corporate data governance – e.g. regular control audits, board-level oversight of fraud risk (audit committees now often ask management pointed questions on this), and adherence to any industry-specific standards (such as SOX 404 internal control requirements in the US, which, while focused on financial reporting, also compel robust disbursement controls).

Cyber Insurance for BEC and Payment Fraud

Corporate insurance policies – both cyber insurance and crime bonds – have historically been a safety net for fraud losses. But the surge in social engineering fraud claims has insurers revisiting their terms. Recent insurance industry data shows that business email compromise and funds transfer fraud now drive over 60% of cyber insurance claims (by frequency)[31], even more common than ransomware. As payouts mount, insurers have tightened underwriting.

Many carriers now require clients to demonstrate specific controls (for example, multi-factor authentication, mandatory callback verification for fund transfers, employee training programs) to even qualify for coverage or to get affordable rates. Some insurers have introduced sub-limits on social engineering losses (capping the payout on a BEC loss well below the policy limit) or increased deductibles. In some cases, insurers have reduced coverage or withdrawn from certain high-risk markets due to the spike in fraud claims[32]. The result is that companies may not be as protected as they assume: a complacent "if we get hit, insurance will cover it" attitude is dangerous.

CFOs should review their policy language carefully – is "fraudulent instruction" or BEC covered under the cyber policy or crime policy, and what conditions apply? For example, a policy might only cover a social engineering loss if the client had independently verified the request – a clause that could void coverage if your team simply trusted a fake email. In 2025, the insurance market is stabilizing somewhat (premiums have plateaued after sharp rises in 2020-2023), but underwriters continue to be strict about required controls.

Businesses that can demonstrate a strong fraud prevention posture often secure better terms. Moreover, some large firms are opting to increase their self-insurance (retentions) for fraud risk, investing the savings in improved controls, rather than paying high premiums for limited coverage. It's a classic case of prevention vs. payout: underwriters are effectively telling clients that the best claim is the one that never happens.

Takeaway

Align Governance and Coverage

The external environment (regulatory and insurance) is effectively raising the floor for fraud control programs. For executives, this means you should treat robust fraud controls not just as an internal best practice but as a compliance and financial imperative. Ensure your governance documentation is in order – if a regulator or insurer asks for proof of your anti-fraud measures, you want to show a clear paper trail of policies, trainings, tech investments, and periodic reviews. Engage with your insurance brokers to stay ahead of any policy changes; consider scenario-testing your coverage (e.g., walk through a hypothetical BEC loss and confirm how/if it would be covered). And keep an eye on regulatory trends in all jurisdictions you operate in – global companies should meet the highest standard across the board, since a weak link in one region can be exploited by fraudsters and result in legal exposure or unrecoverable loss.

In summary, regulators and insurers are effectively signaling: fraud risk management must be on the C-suite agenda, not only to avoid losses but to satisfy obligations and protect shareholder value.

Strengthening Governance and Cross-Functional Response

Amid these evolving threats, one theme is clear: fraud prevention is not just a finance issue or an IT issue – it's an enterprise-wide concern. Best-in-class organizations are breaking down silos and treating payment fraud risk with the same rigor as other strategic risks. A holistic, cross-functional approach is key to staying ahead of cunning adversaries. Here's what that looks like in practice:

Tone at the Top and Executive Ownership

Leadership sets the stage. The board and senior executives must actively endorse fraud risk management – setting a tone that no one is "too important" to follow procedures. (For example, a CEO should openly encourage Finance leadership to double-verify their own payment requests; this reinforces that controls trump ego.)

Many companies have formally assigned a executive owner for fraud risk (often the CFO or CRO) who reports to the board on fraud risk exposure and mitigation plans. This ensures accountability. In turn, managers across treasury, accounting, IT security, and operations know that preventing and detecting fraud is a shared mandate. As one guidance succinctly put it: "*The board and senior management must be actively involved. Tone from the top matters*."[33]

Cross-Functional Fraud Committees & Task Forces

Given the many touchpoints of payment fraud, leading firms establish cross-functional teams to coordinate efforts. A fraud prevention task force might include representatives from finance (accounts payable/treasury), information security, IT, legal/compliance, procurement, and HR. Each brings perspective: Finance knows payment processes, IT/security knows system safeguards and threat intel, Procurement knows supplier onboarding risks, etc. By working together, they can identify gaps and institute controls that span departments. In fact, with the new UK law on failure-to-prevent-fraud, companies are explicitly advised to "*bring together compliance, legal, finance, HR, and IT*" in a unified fraud risk team[34].

This group should meet regularly to review any incidents or near-misses, analyze new fraud modus operandi, and update the fraud response playbook. Cross-functional collaboration also speeds up incident response – if a potential fraud arises, the team can quickly convene to triage (security can trace any IT compromise, finance can contact banks, legal can alert law enforcement, etc.). Time is of the essence, and a practiced team makes a difference.

Robust Policies and Controls – Regularly Tested

Governance isn't just committees; it's also the concrete policies that employees follow. Companies at the forefront have detailed payment controls and verification procedures that leave little to chance. Examples include: requiring multi-person approval for any bank account master file changes, call-back verification for any payment over a certain threshold or to a new beneficiary, mandatory "cooling-off" periods or secondary review for urgent payment requests, and use of payee name match or positive pay services for checks and ACH.

Importantly, these controls should be *stress-tested*. Internal audit or independent control testers often run simulations – for instance, attempting a mock phishing email to accounts payable to see if money would go out, or checking if employees consistently follow the call-back rules. Any weaknesses can then be remedied with training or process changes. Strong governance also extends to vendor management: performing due diligence on new partners, maintaining up-to-date authorized contact information (so that an impostor using an old contact name raises suspicion), and leveraging vendor portals where feasible (so that banking details are exchanged securely, not over email).

Incident Response and Recovery Plans

Despite best efforts, incidents may occur. Leading organizations prepare for this by having a fraud incident response plan that is just as developed as their IT incident response or business continuity plans. This plan should define: Who needs to be alerted immediately (both internally and at your banking partners)? How do you rapidly assemble the cross-functional team? What steps to take in the first 24 hours (e.g. contact law enforcement, engage cyber forensics if an email account was compromised, notify insurers)? Companies have found value in rehearsing these scenarios. Just as IT teams do cyber breach tabletop exercises, the fraud team should run through a BEC scam scenario. For example, "What if we discover $5 million sent to fraudsters via instant payments – who calls the banks? Do we have after-hours contacts at law enforcement? Who handles communications to management and possibly the public?"

Practicing these steps can save precious time and avoid confusion in the heat of an incident. As Arup's CIO noted after their deepfake fraud, "*it's important to have rehearsed a response… so everyone knows what their role is.*"[35] A swift, coordinated response can sometimes limit the damage (as seen in the Singapore case where quick action led to fund recovery[36]) and will certainly be viewed favorably by regulators or courts post-incident.

Continuous Education and Culture

Finally, best-in-class governance fosters a company culture that prizes awareness and transparency around fraud. Rather than shaming victims or keeping incidents hush-hush, these companies treat fraud incidents (and near-incidents) as learning opportunities. They openly share sanitized stories of scams that were attempted, so that everyone from the CFO to junior analysts can learn the red flags. Regular training isn't a dry annual checkbox but an ongoing dialogue, often with fresh examples pulled from news headlines or industry reports. Some firms gamify the learning – e.g. internal phishing challenge competitions – to keep employees engaged.

The goal is to make fraud awareness part of the DNA of the organization, much like safety is on a factory floor. When employees at all levels feel responsible for being the "last line of defense" and are empowered to speak up (e.g. an AP clerk not hesitating to question a request from a top executive that seems odd), the corporate fraud immune system is working.

Takeaway

Build a Culture of Vigilance

Governance and controls are often the unglamorous part of business, but in the fight against payment fraud they are truly a strategic asset. As a Global 1000 executive, ask yourself: *Do we have clear ownership and accountability for fraud risk? Is every relevant function collaborating to combat this threat? When was the last time we audited our controls or drilled our response?*

By strengthening governance now, you not only reduce the likelihood of a costly incident, you also position the company to react effectively if one occurs. In a world where fraud tactics are constantly evolving, a nimble, well-governed defense is a decisive competitive advantage.

Lessons from Recent Major Fraud Incidents

High-profile fraud incidents in the past 1-2 years offer sobering lessons – and in some cases, hopeful examples – for large enterprises. We've touched on a few already, but it's worth summarizing key takeaways from these real-world cases:

Arup Deepfake Scam (2024)

Verify Authenticity

The $25 million theft from Arup via a deepfake video call[20] showed that even a tech-forward company can be caught off guard by a novel attack. The impostors exploited human trust in familiar voices/faces and the assumption that if a meeting invite and video look legitimate, they must be. The lesson is to verify sensitive requests through multiple channels.

After the incident, Arup reinforced multi-channel verification and urged staff to *pause* and validate when something feels even slightly unusual – for example, if a normally mundane payment request suddenly comes with secrecy and urgency. This incident also highlighted the importance of rapid response: once Arup realized the fraud, involving law enforcement quickly was crucial (though unfortunately the money was already gone). It's a reminder that time equals money in fraud recovery, and that employees should be trained to escalate suspected fraud *immediately without fear of blame*. Arup's openness about the attack (speaking at forums, sharing their story) is also commendable – it has helped other companies prepare for deepfake scenarios.

WPP Deepfake Attempt (2024)

Importance of Employee Vigilance

In WPP's case, an attempted CEO impersonation via AI voice was foiled by an attentive employee who sensed red flags (such as requests for unusual secrecy and personal data)[21][37]. WPP's follow-up communication to all staff listed specific red-flag behaviors (e.g. any request for confidential payments "no one else knows about") and emphasized that "just because an account has my photo doesn't mean it's me."[38]

The takeaway is that creating a culture where employees at all levels feel empowered to question and halt a transaction – even if seemingly ordered by the CEO – can stop fraud in its tracks. WPP's case also shows the value of internal awareness campaigns immediately after an incident or near-miss. Reinforcing the warning signs while they are fresh greatly increases retention of the lesson.

Singapore Commodity Firm BEC (2024)

Controls and Global Cooperation

The Singapore firm that nearly lost $42M to a vendor BEC scam teaches two lessons. First, *basic controls might have prevented it*: the fraud succeeded because an email domain was "slightly different"[6] and the company didn't catch it before making the payment. A careful look or an automated domain monitoring tool could have flagged the discrepancy.

Also, had the firm confirmed the account change with the supplier via a known phone number, the fraud would have been exposed.

The second lesson is more positive – it showcased an unprecedented success in recovering funds through rapid global action. INTERPOL's coordination through its new I-GRIP network froze much of the money within days[8], and multiple suspects were arrested[39]. This illustrates that law enforcement is adapting new methods to combat fraud post-incident.

Companies should leverage such channels by reporting crimes immediately; building relationships with law enforcement before anything happens (e.g. participating in info-sharing initiatives) can also help. Not every case will see funds returned, but this one provides a template for how swift reporting and inter-agency cooperation can make a difference.

Coalition Cyber Insurance Data (2024)

Small Losses, Big Cumulative Impact

A somewhat different "incident" is the aggregate data from cyber insurer Coalition's 2024 claims. They found the *average* BEC loss for their clients was around $35,000, relatively small per incident[40], but the frequency made it a huge overall cost (60% of claims). This suggests that many fraud attempts aim for amounts just below what might trigger intense scrutiny – a tactic to fly under the radar.

For large enterprises, losing $30K might not make headlines, but dozens of such incidents or a successful $300K scam can easily occur if lower-tier controls are weak. It's a prompt to not ignore "small" fraud alerts and to track all attempts, as they may indicate systemic issues. Moreover, insurers noted BEC claim severity rising ~23%[41], implying the problem is worsening. Organizations should treat near-misses or minor frauds as a wake-up call to fortify controls before a bigger hit comes.

In reflecting on these incidents, one common thread emerges: preparation and agility are everything. Companies that had drilled responses, educated their people, and forged links to external partners (banks, law enforcement, insurers) fared better in navigating the crisis. Those that were caught unprepared suffered greater losses and chaos. As one executive quipped, fraud isn't a matter of "if" but "when and how." Learning from others' experiences shortens your response time and can illuminate blind spots in your own defenses. At the executive level, fostering a culture that candidly analyzes failures (whether your own or others') and continuously improves from those insights will greatly enhance your fraud resilience.

Strategic Takeaways for Global 1000 Leaders

Corporate payment fraud is not just a technical nuisance – it's a strategic business risk that demands executive attention and action. As we head into 2026, here are the key takeaways and proactive strategies for C-suite leaders:

1

Champion a Fraud-Resilient Culture

Set the tone that security is everyone's responsibility. Encourage a "trust but verify" mindset for payment requests, no matter the source or seniority. Reward employees who spot and stop suspicious transactions. Regularly communicate fraud awareness messages from leadership, so vigilance becomes part of the corporate DNA.

2

Fortify Payment Processes with Multi-Layered Controls

Review all payment initiation and approval workflows across the company. Implement strong authentication and verification steps at every critical point – from supplier onboarding (bank account verification, sanction screening) to payment execution (dual approvals, callback confirmations for changes or large sums). Leverage available banking services like payee name matching and positive pay. Remember that speed should not trump security: introduce friction strategically for high-risk payments (e.g. short delays or additional sign-offs for first-time payees or unusually timed requests) to create opportunities to catch fraud.

3

AI and Analytics for Real-Time Detection

Invest in modern fraud detection tools that use AI and analytics to monitor transactions and user behavior in real time. These can be a game-changer in spotting anomalies (a sudden overseas payment, a login from an unusual IP, etc.) that warrant intervention. At the same time, continue to train and test your people, as they are often the last line of defense. Conduct periodic phishing simulations and deepfake awareness drills. Ensure your IT, finance, and risk teams stay updated on emerging fraud tech – both the threats (AI deepfakes, malware) and the defenses (new software, threat intelligence feeds).

4

Strengthen Governance, Committees, and Board Oversight

Break down silos – establish a cross-department fraud risk committee or working group that meets routinely. Integrate fraud scenarios into enterprise risk management discussions and crisis simulations. Validate that your incident response plan for fraud is current, with clear roles for each department. If a major fraud attempt hit tomorrow, your team should be able to respond like a well-oiled machine (and if you're not confident of that, invest in training and drills to make it so). Active board oversight is also crucial: engage your Audit/Risk Committee in reviewing fraud controls and incident logs at least annually.

5

Engage Externally – Partner with Banks, Insurers, Regulators

Develop strong relationships with your banking partners' fraud departments – they can provide counsel on the latest schemes and assist in recovery efforts if an incident occurs. Revisit your insurance coverage in detail; clarify any ambiguities about social engineering fraud coverage and ensure you meet all prerequisites to claim (insurers often require specific controls to be in place). Be prepared that insurance alone is not a panacea, given tightening terms. Additionally, stay in communication with industry groups (like the AFP, NACHA, or sector-specific info-sharing forums) and even law enforcement outreach programs. Being plugged into a network will help you learn about new threats quickly and respond collaboratively if a broad fraud campaign targets multiple firms.

6

Plan for Resilience and Continuous Improvement

Despite best efforts, assume that at some point an incident may slip through. Focus not only on prevention but also on resilience – minimizing damage and bouncing back. This means having playbooks for business continuity if funds are stolen or systems compromised, and public relations plans if a fraud incident becomes public. It also means learning and evolving: perform root-cause analyses on any fraud or near-miss and adapt your controls thereafter. Organizations that treat each incident as a chance to get stronger will, over time, far outpace those who treat it as one-off bad luck.

In Conclusion

Corporate payment fraud in 2025 is a high-stakes challenge fueled by fast-moving technology and crafty adversaries. Yet, the landscape is not hopeless. Global 1000 companies that take a proactive, informed stance – led from the top – can significantly reduce their risk and even turn robust fraud controls into a competitive advantage (through safer operations and trust with partners). For executives across industries, the message is clear: payment fraud resilience must be a strategic priority. By combining the right culture, controls, technology, and partnerships, you can keep your organization one step ahead of fraudsters and protect the hard-earned assets and reputation of your enterprise in the years to come.[10][5]

About P&C Global

At P&C Global, we don't just deliver consulting—we deliver transformation with guaranteed outcomes, backed by our $250 billion in annual client value creation, 95% Global 50 penetration, and 93% client referral rate that validates our unique approach. Unlike traditional consultancies that hand over recommendations, we own the entire journey from boardroom strategy to frontline implementation, leveraging our 8,500+ experts across 40+ countries, proprietary 4D methodology, and Visage™ AI platform to ensure breakthrough results.

With over 15,000 individual certifications surpassing traditional consultancies including MBB firms, 100% on-time delivery across 15,000+ engagements, industry-leading 97% employee retention ensuring team continuity, and billions of dollars in annual investment in professional development, we bring stability, expertise, and innovation that transforms ambitious visions into measurable success. As part of a conglomerate with deep operational expertise across multiple industries, P&C Global combines insider-operator perspective with vendor independence—receiving zero remuneration from third parties, our only allegiance is to our clients' strategic objectives—making us not just your consultant, but your transformation partner for sustained market leadership.

References

[1] [2] 2025 AFP Payments Fraud and Control Survey Report
https://www.financialprofessionals.org/training-resources/resources/survey-research-economic-data/details/payments-fraud

[3] [4] [10] [23] PAYMENTS FRAUD AND CONTROL SURVEY REPORT | Truist
https://www.truist.com/content/dam/truist-bank/us/en/documents/info/cci/2025-afp-payments-fraud-control-survey-report-key-highlights.pdf

[5] [26] FBI's IC3 Finds Almost $8.5 Billion Lost to Business Email Compromise in Last Three Years | Nacha
https://www.nacha.org/news/fbis-ic3-finds-almost-85-billion-lost-business-email-compromise-last-three-years

[6] [7] [8] [36] [39] INTERPOL Recovers $41 Million in Largest Ever BEC Scam in Singapore
https://thehackernews.com/2024/08/interpol-recovers-41-million-in-largest.html

[9] Exposing Business Email Compromise: How Fraudsters Infiltrate ...
https://delta-cgi.com/exposing-business-email-compromise-how-fraudsters-infiltrate-trusted-relationships/

[11] Over £1.2 billion stolen through fraud in 2022, with nearly 80 per ...
https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app

[12] FedNow instant payments: what are the risks? - Trustpair
https://trustpair.com/blog/fednow-instant-payment-what-are-the-opportunities-and-risks-for-your-business/

[13] [14] [15] [16] [17] Fraud emerges as concern for FedNow users | Payments Dive
https://www.paymentsdive.com/news/Fednow-fraud-banks-real-time-payments/702527/

[18] [19] Instant Payments Regulation Update | Mason Hayes Curran
https://www.mhc.ie/latest/insights/instant-payments-regulation-update

[20] [24] [35] Cybercrime: Lessons learned from a $25m deepfake attack | World Economic Forum
https://www.weforum.org/stories/2025/02/deepfake-ai-cybercrime-arup/

[21] [22] [25] [37] [38] CEO of world's biggest ad firm targeted by deepfake scam | Technology | The Guardian
https://www.theguardian.com/technology/article/2024/may/10/ceo-wpp-deepfake-scam

[27] [28] [29] [30] [33] [34] Failure to Prevent Fraud: What the Sept 2025 Law Means for Firms - AccessPay
https://accesspay.com/knowledge-hub/fraud-error-prevention/new-fraud-prevention-laws-what-the-september-2025-failure-to-prevent-offence-means-for-firms/

[31] [41] BEC and FTF drove 60% of 2024 cyber claims – Coalition | Insurance Business Canada
https://www.insurancebusinessmag.com/ca/news/cyber/bec-and-ftf-drove-60-of-2024-cyber-claims--coalition-534996.aspx

[32] Rising Social Engineering Crimes Changing Cyber Coverage - Tools and Intel | CRC Specialty
https://www.crcgroup.com/Tools-and-Intel/post/rising-social-engineering-crimes-changing-cyber-coverage

[40] Ransomware Claims Stabilized in 2024, Though Still the Costliest ...
https://www.carriermanagement.com/news/2025/05/08/275004.htm

P&C® GLOBAL

pandcglobal.com

P +1 (214) 624-9575
E info@pournader.us