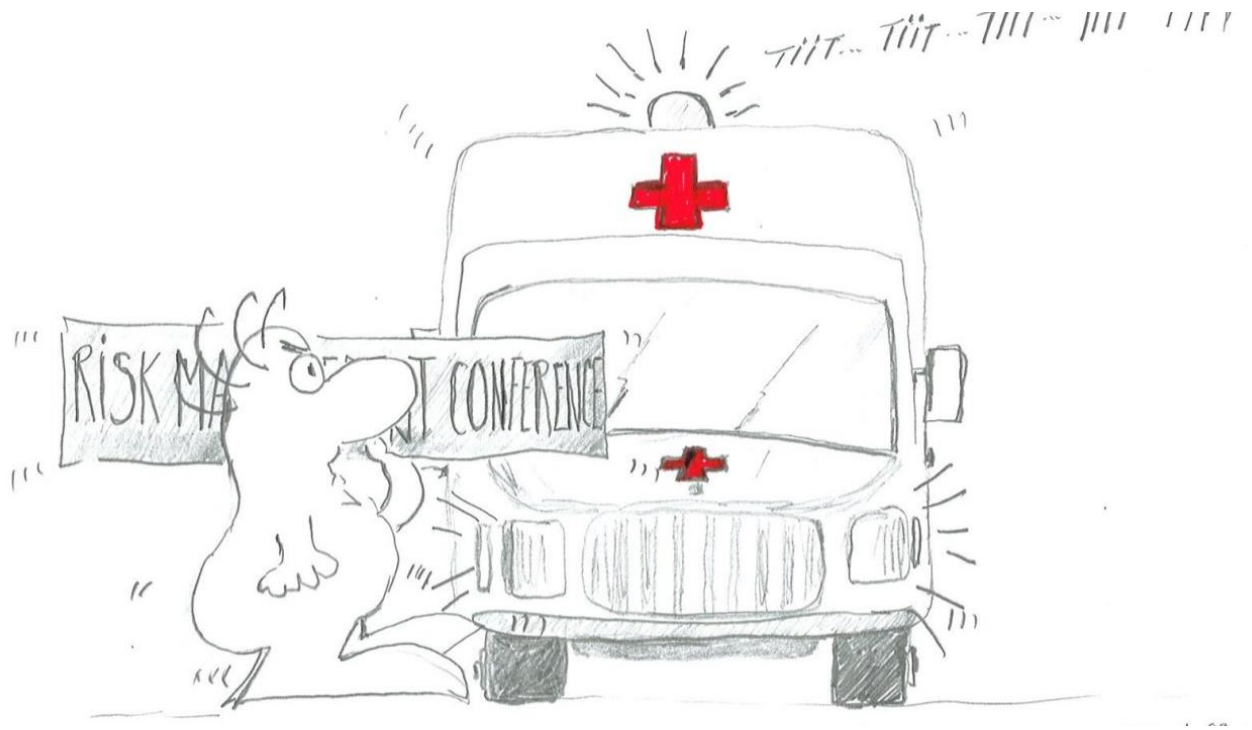


Pay Now, Regret Later: The Treasurer's Field Guide to Payment Fraud



François Masquelier
CEO
Simply Treasury

July 27, 2026

Treasury Fraud & Payments Security Watch 2026

If It Looks Like the CFO and Sounds Like the CFO, It Probably Isn’t: The Complete Treasury Fraud Compendium

François Masquelier | CEO, Simply Treasury | Chairman, ATEL | Chair, EACT

EXECUTIVE SUMMARY

Payment fraud is no longer a peripheral operational risk — it is a strategic threat that has destroyed careers, triggered SEC filings and cost multinationals hundreds of millions of dollars in a single incident. From the classic CEO impersonation email to AI-generated deepfake video calls indistinguishable from reality, the attack surface facing corporate treasury has never been wider or more sophisticated. We have tried

to map out every major fraud typology treasury professionals will encounter, anchors each to real disclosed cases — including Orion S.A.'s $60M loss and Arup's HK$200M deepfake disaster — and closes with the controls and best practices that can prevent the next headline.

1. THE SCALE OF THE THREAT: NUMBERS THAT DEMAND ATTENTION

The data is unambiguous. According to the 2026 AFP Payments Fraud and Control Survey, more than three-quarters of US organisations experienced attempted or actual payments fraud in 2025, with Business Email Compromise (BEC) affecting 74% of respondents — a significant increase from prior years. Nearly 60% of companies reported that the financial impact of payment fraud in 2024 exceeded $5 million, a figure 136% higher than the previous year, according to TRUSTPAIR research. The FBI's Internet Crime Complaint Center has recorded over $55 billion in cumulative BEC losses between 2013 and 2023.

The treasury function is both the primary target and the primary line of defence. AFP data confirms that treasury is the department most likely to discover attempted fraud (83%) and actual fraud (55%). That dual responsibility — front-line operations and first-responder — places an extraordinary premium on awareness, process discipline and technological readiness.

"Prevention today is an operating model, not a single control. Every treasury team needs a documented, tested, multi-layered defence against fraud." — AFP Payments Fraud Survey, 2026

In EU, we have less statistics about fraud cases. Nevertheless, treasurers are facing similar risks.

2. THE TREASURY FRAUD TAXONOMY: A COMPREHENSIVE MAP

The table below summarises the principal fraud typologies confronting treasury, mapped against attack vector, typical loss range and key control. Sections 3 through 7 then explore each category in depth.

Fraud Type	Attack Vector	Typical Loss	Risk Level	Key Control
BEC / CEO Fraud	Spear-phishing, impersonation	$100K – $60M+	CRITICAL	4-eye + out-of-band verify
Deepfake A/V	AI video/voice clone	$25M+ (Arup 2024)	CRITICAL	Code words + call-back protocol
Vendor Fraud (VEC)	Supplier email compromise	$50K – $5M	HIGH	Sis ID / bank acct validation
Payroll Diversion	HRIS account takeover	$50K – $500K	HIGH	Dual approval + HR/Finance split
Cheque Fraud	Counterfeiting, alteration	Variable	MEDIUM	Positive Pay, cheque truncation
ACH / SEPA Fraud	Mandate tampering, debit pull	$10K – $1M	MEDIUM	ACH debit blocks, whitelist
Internal Embezzlement	Fictitious vendor, rogue trader	Often >$1M	HIGH	Segregation of duties, audit
Supply Chain Finance	Invoice duplication/manipulation	$100K – $10M	MEDIUM	ERP 3-way match, limit controls

3. EXTERNAL FRAUD: THE DOMINANT THREAT

3.1 Business Email Compromise (BEC) and CEO Fraud

BEC is the defining payment fraud of the current era. Attackers compromise or spoof corporate email accounts, then impersonate executives, suppliers or legal advisers to instruct finance staff to execute urgent, confidential wire transfers. The social engineering is meticulous: attackers research organisational hierarchies on LinkedIn, study email tone, exploit travel calendars and invoke urgency and secrecy to override normal controls. The disclosed losses speak for themselves. Austrian aerospace components manufacturer FACC lost €42 million in 2016 after a fraudster impersonating the CEO tricked a finance employee into wiring funds for a fictitious acquisition. Dutch cinema chain Pathé lost €19 million in 2018 under near-identical circumstances. Google and Facebook collectively lost over $100 million when a Lithuanian fraudster submitted invoices impersonating a genuine hardware supplier they both used. The fraudster was eventually convicted, and partial recovery was achieved — but the reputational damage endured. However, as it remains taboo, we can hardly determine all fraud attempts and real losses.

Case Study: Orion S.A. — $60 Million BEC Loss (August 2024)

Orion S.A., a Luxembourg-headquartered global carbon black manufacturer and a listed NYSE company, disclosed in an SEC Form 8-K filing on 12 August 2024 that a non-executive employee had been the target of a criminal scheme resulting in multiple fraudulently induced outbound wire transfers to accounts controlled by unknown third parties.

The company estimated a one-time pre-tax charge of approximately $60 million for unrecovered funds.

No evidence of systems compromise was identified — the attack was pure social engineering targeting payment execution processes.

Orion engaged law enforcement and explored insurance recovery. The case illustrates that even well-resourced, listed MNCs remain acutely vulnerable to BEC when process controls are insufficient.

Source: Orion S.A. Form 8-K, US Securities and Exchange Commission, 12 August 2024.

3.2 Deepfake and AI-Augmented Fraud: The New Frontier

The emergence of generative AI has elevated social engineering fraud to a qualitatively new level of danger. Attackers now use voice cloning and real-time video deepfakes to impersonate executives with alarming fidelity — eliminating the typographical errors and linguistic tells that once allowed recipients to detect fraudulent communications.

Case Study: Arup Engineering — HK$200 Million Deepfake Video Call (2024)

British engineering firm Arup confirmed in 2024 that its Hong Kong office lost approximately HK$200 million (around £20 million / USD $25 million) after a finance employee participated in what appeared to be a video conference with senior company executives.

All participants on the call — including the apparent CFO — were AI-generated deepfake avatars constructed from publicly available video and audio footage.

The employee transferred funds to five separate accounts across 15 transactions before the deception was uncovered.

The US Financial Crimes Enforcement Network (FinCEN) issued a formal alert in November 2024 specifically warning financial institutions of the growing threat of deepfake-enabled fraud.

Separately in 2024, scammers attempted to defraud WPP using a WhatsApp account bearing CEO Mark Read's photograph combined with a cloned voice on a fake Microsoft Teams call. WPP detected the fraud in time.

According to Resemble AI, financial losses from deepfake-enabled fraud surpassed $200 million in Q1 2025 alone. Deloitte forecasts US deepfake fraud losses could reach $40 billion annually by 2027. Treasury teams must assume that any unsolicited, urgent payment instruction received through digital channels — regardless of apparent source — is a potential attack.

3.3 Vendor Email Compromise (VEC) and Invoice Fraud

A variant of BEC, Vendor Email Compromise involves the genuine compromise of a supplier's email account — rather than mere spoofing. Attackers infiltrate the vendor's systems, monitor invoice cycles and, at the optimal moment, redirect payment instructions to fraudulent bank accounts. In 2023 alone, VEC attacks increased by 137% year-on-year. Recovery is significantly harder than in standard BEC cases because the communication appears entirely authentic.

In a particularly instructive case, Singaporean authorities recovered $42.3 million from a commodity firm after fraudsters impersonated a legitimate supplier in 2024 — an unusually successful recovery attributed to the INTERPOL I-GRIP stop-payment mechanism being activated within hours of detection.

3.4 Cheque Fraud and ACH/SEPA Mandate Manipulation

Despite the perception that cheques are archaic (and really American mean of payment), the AFP's 2025 survey found that 58% of organisations reported cheques as the payment method most subject to fraud. Counterfeiting, alteration and cheque washing remain widespread. For electronic payments, mandate fraud — impersonation of a supplier or employee to redirect ACH/SEPA direct debits or standing orders to fraudulent accounts — represents a consistent and underestimated threat.

4. INTERNAL FRAUD: THE THREAT FROM WITHIN

Internal fraud, while statistically less frequent than external attack, tends to generate larger per-incident losses and significantly greater reputational damage. The ACFE estimates that organisations lose 5% of annual revenues to occupational fraud, with a median duration of 12 months before detection.

4.1 Fictitious Vendor and Disbursement Fraud

Fictitious vendor schemes involve an employee with access to the vendor master file creating phantom suppliers and authorising payments to accounts under their control.

The fraud is enabled by weak segregation of duties — typically where the same individual can create a vendor and initiate payment. A comprehensive 2024 case in the healthcare sector resulted in a senior finance officer recovering over $3.5 million across four years by routing payments to a shell company registered in a family member's name.

4.2 Payroll Fraud and Ghost Employees

Payroll diversion fraud occurs when an insider — or an external attacker who has compromised HR/HRIS credentials — redirects salary payments to fraudulent bank accounts. Ghost employees (fictitious headcount added to payroll) and bank account substitution for real employees are both common variants. The increasing use of self-service HRIS portals without secondary authentication has created new attack surfaces.

4.3 Rogue Trader and Unauthorised Derivative Transactions

While rare at the retail end of the corporate spectrum, rogue trading remains a latent risk in treasury functions with active derivatives and FX programmes. The Société Générale case (€4.9 billion, Jérôme Kerviel, 2008) and the UBS loss of $2.3 billion (Kweku Adoboli, 2011) serve as permanent reference points. The control lesson from both: position limits are useless without independent valuation and real-time monitoring of collateral and margin calls. It is also advised to impose at least once a year a 15-day break (in a row), which helps detecting frauds, if any.

5. SUPPLY CHAIN AND TRADE FINANCE FRAUD

Supply chain finance programmes — reverse factoring, dynamic discounting, supplier finance — introduce specific fraud vectors. Invoice duplication (submitting the same invoice to multiple financiers), over-invoicing, and the manipulation of confirmation platforms are all documented risks. The Greensill Capital collapse in 2021, while primarily a credit risk failure, illuminated how supply chain finance structures can be used to obscure the true nature of receivables and concentrate risk invisibly. Treasurers administering supply chain finance platforms must ensure independent reconciliation between ERP invoice records, platform submissions and actual payment flows. A three-way match — purchase order, goods receipt and invoice — remains the foundational control, but must be enforced at the system level rather than relying on manual review.

6. BEST PRACTICES: BUILDING A FRAUD-RESILIENT TREASURY

No single control eliminates payment fraud risk. Defence must be layered, tested and continuously adapted. Internal controls are never strong enough and should be

reviewed once a year, at least. The following framework reflects current best practice across European and global MNC treasury functions.

Payment Process Controls

Four-eye principle: all outbound payments above threshold require dual authorisation from independent individuals. No single individual should be able to initiate and approve a payment.

Out-of-band verification: any payment instruction received by email or digital channel that changes bank account details or involves an unusual amount must be verified by phone to a pre-registered number — never the number provided in the request.

Payment whitelist / positive pay: approved beneficiary registers for wire transfers; any new payee triggers an enhanced approval workflow regardless of instruction source.

Bank account validation tools: platforms such as Sis ID, Trustpair, and Coupa (procurement) enable automated real-time validation of IBAN/BIC combinations against authoritative registries before payment execution (despite the VoP impose in EUR payments since Instant Payment introduction end of 2025).

Transaction monitoring: TMS and ERP anomaly detection (via AI) for payment patterns deviating from established behaviour (unusual amounts, new beneficiaries, atypical timing).

Digital Identity and AI Defence Controls

Code words and callback protocols: establish pre-agreed verbal verification codes for executive-instructed transactions. If a CFO requests an urgent transfer, a set phrase known only to authorised parties must be used — trivially defeats deepfake impersonation.

Multi-factor authentication (MFA): mandatory for all payment portals, TMS access and HRIS self-service. Resistance to phishing-resistant MFA (FIDO2/passkeys) is the emerging standard.

Email authentication: DMARC, DKIM and SPF deployment to prevent domain spoofing; DMARC in reject/quarantine policy significantly reduces CEO fraud exposure.

AI-based fraud detection: real-time NLP analysis of payment instruction emails for urgency language, domain anomalies and writing style deviations. Only 17% of organisations currently use AI for fraud mitigation (AFP, 2026) — a stark capability gap.

Deepfake awareness training: employees in finance and treasury must be trained to treat any video call or voice instruction requesting a payment as potentially synthetic. ‘See and hear’ is no longer sufficient verification. Prevention and education remain the best ways to continuously keep employees informed and alerted on (new) dangers.

Governance, Segregation and Internal Audit

Strict segregation of duties across vendor master maintenance, payment initiation and payment release — ideally mapped to distinct personnel with incompatible system permissions.

Quarterly reconciliation of vendor master to approved supplier lists, with automated alerts for dormant vendors reactivated or bank details changed.

Regular rotation of treasury staff handling payment execution and independent surprise audits of payment runs.

Incident response plan: pre-defined escalation path, bank contact protocols and law enforcement liaison for suspected fraud — speed of response is the primary determinant of fund recovery.

Cyber insurance: treasury should engage with risk management to ensure crime/cyber policy coverage is adequate for the organisation’s payment volumes and explicitly covers BEC and social engineering losses. Although premium could be high and insurers will control clients to assess the risks around payments.

7. THE AI INFLECTION POINT: WHY 2026 IS DIFFERENT

Generative AI has not merely incremented the sophistication of existing fraud vectors — it has created qualitatively new attack surfaces that invalidate controls previously considered robust. Voice cloning requires less than three seconds of audio to produce a convincing replica. Real-time facial deepfakes can sustain a live video call for minutes. AI-generated BEC emails no longer carry the grammatical markers that trained employees once relied upon to detect fraud.

Treasury professionals must internalise a fundamental shift in threat model: the identity of the person apparently instructing a payment can no longer be verified by sight or sound alone. The only reliable authentication mechanisms are out-of-band verification against pre-registered contact details, cryptographic authentication, and formal process controls that are independent of the communication channel carrying the instruction.

“The question is no longer ‘does the email look genuine?’ It is ‘does our process prevent execution of fraudulent payments regardless of how convincing the instruction appears?’” (Francois Masquelier, CEO of Simply Treasury)

TREASURY AS THE LAST LINE OF DEFENCE

Payment fraud is not diminishing — it is accelerating, professionalising and industrialising. The fraudsters who targeted CARITAS Luxembourg for €60 million, Orion S.A. for $60 million and Arup for HK$200 million were not opportunists; they were sophisticated criminal enterprises using research, patience and advanced technology. The response must match that sophistication. Treasury teams that maintain documented payment policies, invest in bank account validation technology, enforce unconditional out-of-band verification for sensitive transactions, and train their people to treat urgency and secrecy as red flags — not accelerants — will be materially better positioned than those relying on process inertia and good fortune. The cost of prevention is a fraction of a single successful attack. The reputational cost of an SEC disclosure announcing a $60 million fraud loss is, for most organisations, incalculable. Treasury’s role has evolved from cash manager to payment security superintendent. Own that responsibility before a fraudster claims it for you. The ROI and pay-off of such prevention solutions and internal controls enhancement are always high and short.

“In treasury, the best internal control is a sceptical mind and a process that does not bend under pressure.” (Francois Masquelier, Chair of EACT)