Combatting fraud in a perfect storm: Thematic typology supplement.

ACCA

IN COLLABORATION WITH:

ACFE Association of Certified Fraud Examiners

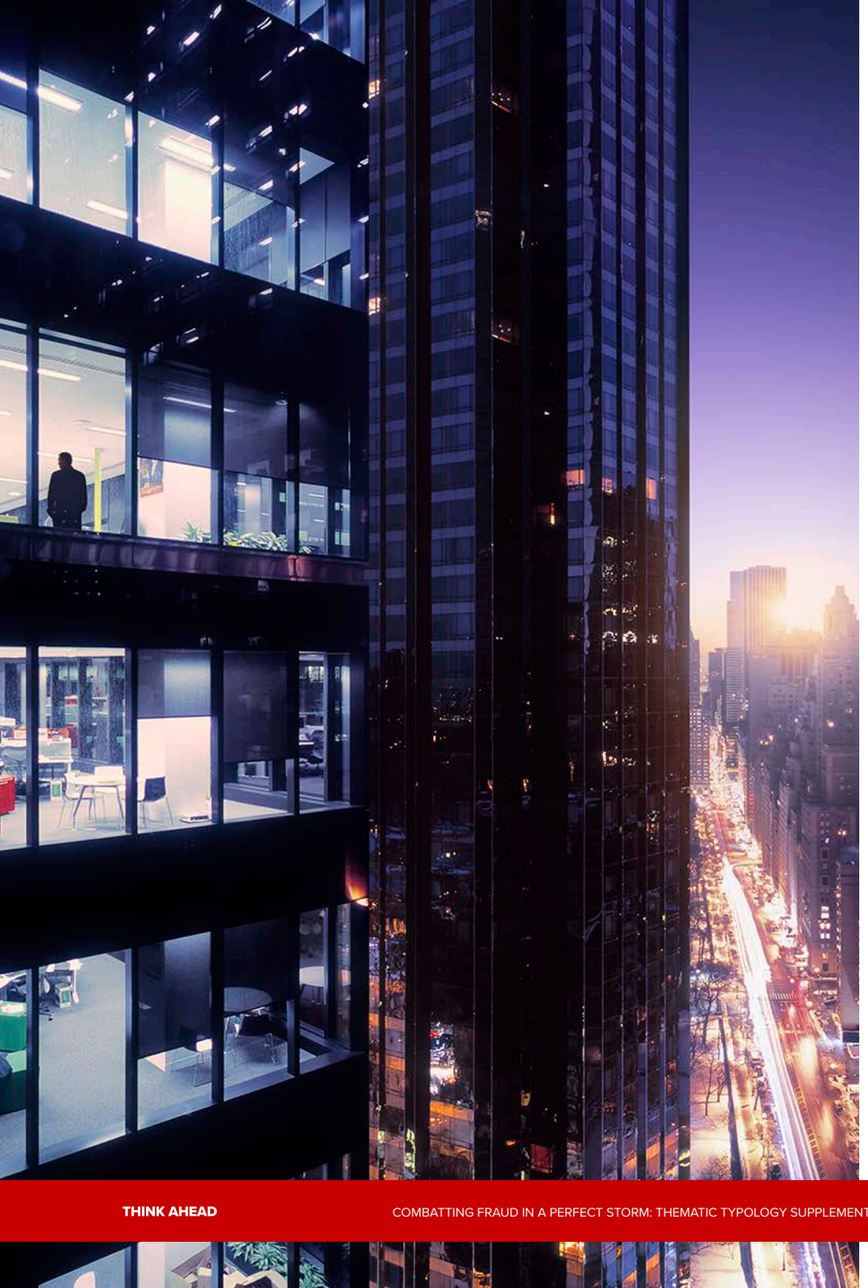
The Institute of Internal Auditors

ISC2

CISI CHARTERED INSTITUTE FOR SECURITIES & INVESTMENT

airmic

Association of Corporate Investigators



In our Calls to Action supplement, we set out the practical steps leaders can take to build fraud-resilient organisations. This companion piece offers a different lens. Here, we tune into the lived experiences behind the survey data: the practitioners, investigators, internal auditors, risk leaders and finance professionals who face fraud every day across regions and sectors.

Their stories illuminate patterns that charts can't. We hear how pressures, gaps in governance, cultural blind spots and fast-evolving technologies combine to make fraud both pervasive and personal. We hear the tension between aspiration and reality – 'zero tolerance' statements that meet operational constraints; sophisticated controls that falter in the face of rationalisation; detection that often outpaces prevention.

What emerges is a thematic typology of the modern fraud landscape: not a taxonomy of offences alone, but a map of how fraud actually happens – how it's enabled, detected, disrupted or left to grow. Across payroll and procurement, data valuation and healthcare, cyber and romance scams, the comments converge on a simple truth: fraud is everyone's problem, and culture is the difference between looking for it and living with it.

This supplement complements the main report by further amplifying professional voices and providing thematic insights for practical application. It organises those voices around the lifecycle of fraud – **Types → Detection → Prevention** – and layers in regional context and behavioural drivers. It closes by revisiting the fraud diamond – pressure, opportunity, rationalisation and capability – reflecting how these forces show up in practice today.

We offer these pages as a set of signals to recognise, mindsets to adopt and questions to ask – because the fastest way to strengthen controls is to learn from what people are already seeing.

Thematic typology 'at a glance'

- Internal fraud surfaces where basic custody and segregation slip, and where conflicts of role create perverse incentives.
- External and third-party fraud exploits reply-thread trust, hurried change requests and unverified documents.
- Cyber-enabled fraud – deepfakes, synthetic IDs, AI-forged documents – requires verify-then-trust habits at every handoff.
- Speak-up credibility, not just channels, determines whether staff look for fraud or live with it.
- Boards see blind spots when they join up outsourcing, third-party resilience and culture with fraud exposure.
- Regulation and assurance are catching up; attackers already use AI at scale – defences must accelerate.

Types of fraud – lived experiences

‘In a labour-heavy plant, we uncovered several ghost employees. Headcount and badges reconciled on paper, but net pay didn’t match. Once we compared gate logs against shift rosters, the scheme collapsed within a week.’

Chief compliance officer, manufacturing, South Asia

‘We watched a branch manager bypass the four-eyes principle and close the branch alone. The next morning, the prepared cash bag worth about US$150,000 was gone. That wasn’t a design flaw; it was a “just this once” kind of culture.’

Chief risk officer (CRO), banking, Middle East

‘Dormant accounts are highly sensitive and must never be moved without strict controls and dual approvals. Every time we investigated, the paperwork had helpful gaps and cases got ignored.’

Head of compliance risk and risk management, Central Asia

‘Thin margin pressure drives misreporting. In one case, a CFO [chief financial officer] manipulated numbers to meet targets because he was also making commercial decisions. The [role] conflict was the fraud vector.’

CRO, multi-sector conglomerate, Middle East

‘We had an employee who kept transfers just under the daily approval threshold so nothing triggered review. Only a forensic sweep across daily limits lit up the pattern.’

Finance Manager, public sector, Canada

‘The [payroll] fraud was hiding in W2 prep-shaving reported income across employees and adding the delta to her own withholding. A surprise audit finally surfaced it.’

Accountant, fintech, US

‘Government contracts are always something to watch. The risk isn’t just policy, it’s relationships. Entertainment, “ESG sponsorships”, and soft expectations at officer level. If we don’t police it, we risk the brand in our [value and supply chains].’

Financial controller, infrastructure/construction Asia-Pacific

‘At the grassroots, every contract “needs someone inside”. It’s embedded and hard to unpick. Clean paperwork hides dirty work.’

Finance director, Malaysia

‘A “boss” on video pushed a large transfer – voice, backdrop, cadence all perfect. If your culture is “do whatever the boss says,” technical controls won’t save you.’

Partner, professional services, Hong Kong

‘On this [fraudulent] deal, the paper trail looked pristine – because it was synthetic. Fraudsters mass-produced contracts with AI. We then used AI to find the seams – metadata ghosts and signatures that didn’t “age” right.’

Accounting practitioner, US

‘We saw a private house slipped into a school’s BOQ [Bill of Quantities] via variations. Now every variation needs an independent quantity survey. The fraud died overnight.’

Public sector, South Africa

‘We warned a member about a romance scam. Despite clear advice, the member insisted on transferring savings. Legally, we could not block the transaction.’

Chief executive of a credit union in Ireland

‘Cyber-enabled fraud isn’t just an IT problem – it’s a culture problem. You can buy tools, but you cannot buy scepticism and follow-through.’

Cybersecurity manager at multi-national retailer

‘Threat actors used AI to create fake accounts and contracts. We had to deploy AI to detect anomalies and expose the forgery.’

Compliance lead, multi-national manufacturer

Detection – how they knew, what gave it away

‘Start with the boring stuff: round numbers, duplicate entries, shared addresses, month-end spikes. Teams chase “AI” before they master the five checks that catch most of the red flags.’

Forensic accountant, Europe

‘Our first phishing drills were scary – click rates we didn’t want to believe. Monthly micro-learning and live tests moved the needle.’

CRO, life Insurance, Luxembourg

‘A supplier handling HR/payroll was breached. Overnight, all employee data was exposed. We scrambled for weeks, and we still don’t know if it was weaponised later.’

Head of risk management, payments tech, Netherlands

‘Perfection at the teller window is a red flag. The drawer always “balanced” because of a personal coin jar under the desk.’

Internal audit manager, Ireland

‘WhatsApp voice note “from the CFO” – same display picture, same voice, urgent tone. A junior asked why vendor details changed twice that month. That pause saved us.’

Finance controller, manufacturing, India

‘Hong Kong boards disclosed “hotlines in place” yet reviewed zero cases. Only after a nine-figure [Hong Kong] dollar deepfake incident did outcomes get reported quarterly.’

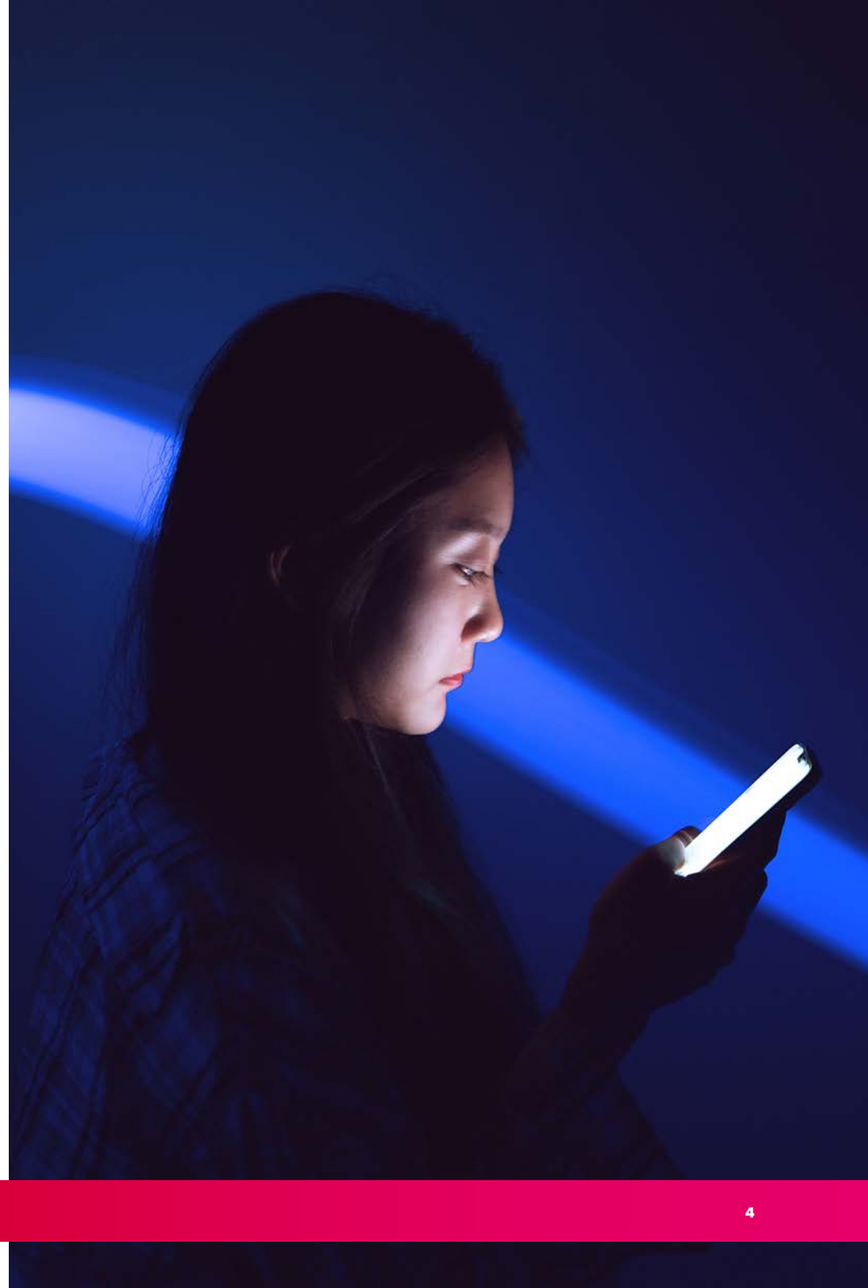
Independent director, financial services, Hong Kong

‘Third-party incidents now dominate. Smaller vendors can’t invest at our level – logs don’t lie.’

CRO, banking, Ireland

‘It’s only a matter of time before a senior executive appears on a Teams call – and it isn’t really them. Deepfake risk is real and growing.’

CRO, insurance, UK



Prevention – what they changed and why it worked

‘When people see that action follows reports, the cost–benefit of committing fraud changes. Fewer people try. We published anonymised outcomes internally and saw internal attempts drop.’

Internal audit, Ireland

‘We now validate payee details and require callbacks before processing bank changes. A few extra minutes have no doubt saved us millions.’

Finance lead, public sector, Europe

‘We lost money because a team trusted scanned documents and skipped the out-of-band call. Now notarised evidence is mandatory, and the callback ritual is drilled – no exceptions.’

CRO, Middle East

‘WFH [working from home] fraud surfaced when VPN [Virtual Private Network] logs revealed employees working from outside approved countries without disclosure. Pre-clearance and HR [human resources] cross-checks are governance fixes, not IT matters.’

Risk management lead, Middle East

‘Agent banking grew access – and fraud. Biometric KYC at counters, tighter agent onboarding and FIU [Financial Intelligence Unit] spot-checks bent the curve back.’

Retail banking operational risk lead, East Africa

‘We removed payroll prep from plant managers, mandated bank/mobile wallets, and rotated approvers. Not popular at first; then payday became fair and predictable.’

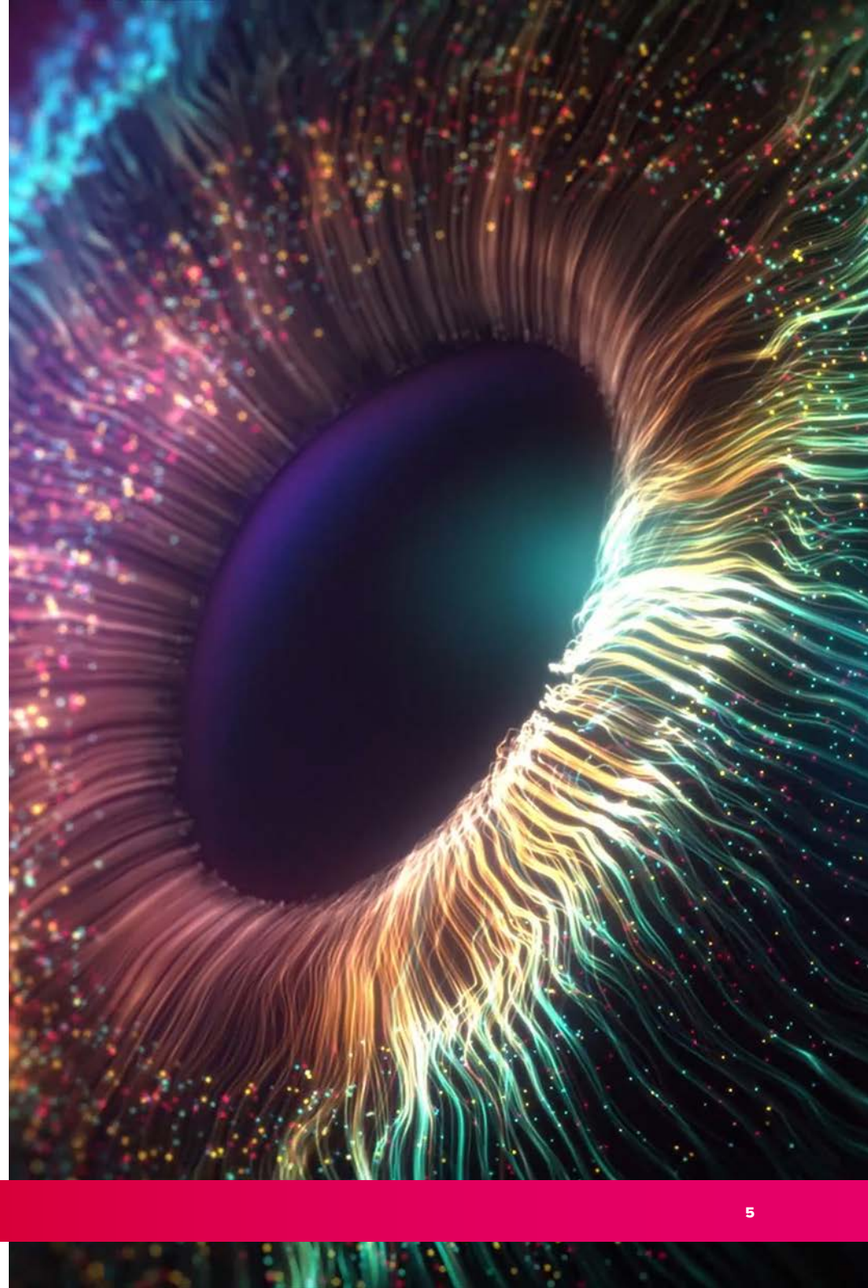
Internal controls lead, Central Asia

‘For procurement “efficiency fog” [where euphemisms obscure risk], the board now gets raw risk language – not massaged summaries. That’s where the euphemisms hide.’

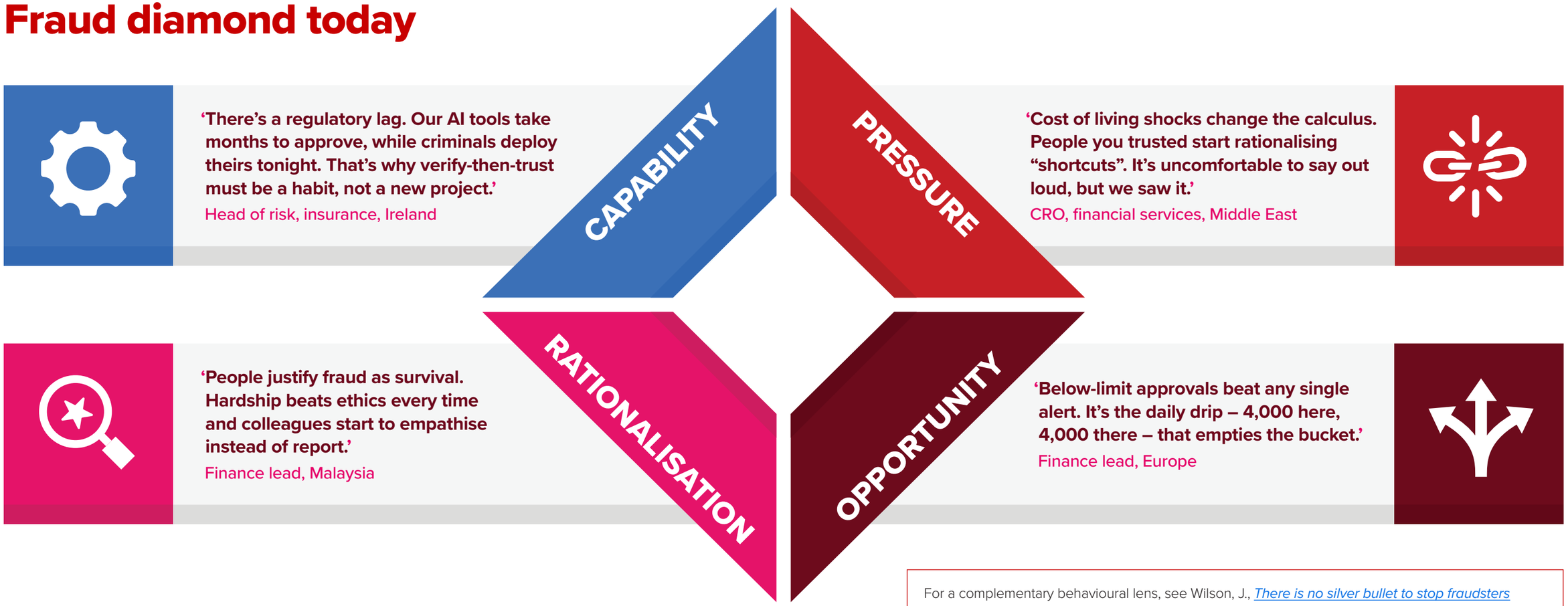
Non-executive director, Europe

‘We learnt that it pays to establish risk appetite before embarking on any digital transformation. Because when you’re in a difficult situation, your judgment might not be the same as when it’s all plain sailing. Risk appetite or risk tolerance should be set out before any discussions even begin.’

Board director, UK



Fraud diamond today



‘There’s a regulatory lag. Our AI tools take months to approve, while criminals deploy theirs tonight. That’s why verify-then-trust must be a habit, not a new project.’

Head of risk, insurance, Ireland

‘Cost of living shocks change the calculus. People you trusted start rationalising “shortcuts”. It’s uncomfortable to say out loud, but we saw it.’

CRO, financial services, Middle East

‘People justify fraud as survival. Hardship beats ethics every time and colleagues start to empathise instead of report.’

Finance lead, Malaysia

‘Below-limit approvals beat any single alert. It’s the daily drip – 4,000 here, 4,000 there – that empties the bucket.’

Finance lead, Europe

For a complementary behavioural lens, see Wilson, J., *There is no silver bullet to stop fraudsters* (The Conversation, 2016). Dr Jennifer Wilson, FCAA, argues against one-size-fits-all ‘profiles’ and emphasises tailored interventions based on multiple offender pathways. One of her comments for this research: ‘*Criminal records checks risk a false sense of security; most fraudsters have no prior record.*’

Regional highlights

Asia-Pacific

‘Laws exist but let’s face it, enforcement and protection don’t. People fear speaking up, so silence wins at the grassroots.’
Ethics and compliance lead, Malaysia

‘The deepfake threats changed us. We hard-wired verify-then-trust for high-risk instructions, and the board now reviews case counts, cycle times and substantiation quarterly.’
Finance lead, financial services, Hong Kong

‘Romance scams are exploding among seniors. One case cost an elderly woman A$20,000. The real issue? Platforms with zero identity verification. We need systemic fixes, not just sympathy.’
CFO, Australia

‘Banks here face thousands of cyberattack attempts daily. Commonwealth Bank spent A$500m last year on fraud prevention. The regulator’s teeth are growing – soon, liability for scams will sit squarely with us.’
Controls officer, Australia

Africa

‘Fraud is not always opportunistic. People plan it from the start. They put activities in the budget that they know they will never implement, or they inflate costs to absorb personal benefits later. If you’re not very inquisitive, they will play you around.’
Risk oversight lead, Kenya

‘Fraud becomes more complex every passing day. We’ve reduced internal fraud through training and consequence management – zero tolerance and serious penalties send a strong message. But external attempts keep coming, and that means governance must be intentional, not just compliance on paper.’
CRO, Uganda

Europe

‘Zero tolerance remains a slogan until you resource it. We rewrote risk appetite with limits and triggers the front line can live with.’
Risk management lead, Europe

‘Audit committees here get five minutes on fraud in a 600-page pack. For the stipend you pay, that’s misaligned from the start.’
Audit committee member, UK

‘Investors now demand provenance checks for AI-forged artifacts – signature “age”, metadata, and independent re-computation of performance claims.’
Board director, Europe

‘DORA [the Digital Operational Resilience Act in the EU] made us map every critical service and sub-supplier – a real eye-opener given the materiality of cyber risk today.’
CRO, financial services, Ireland

North America

‘Threshold gaming only surfaced when we stitched a month’s transactions. We’ve moved to pattern KRIs [Key Risk Indicators], not just single-event limits.’
Controller, Canada

‘The W2 scheme [Wage and Tax Statement] ended when we split duties inside the payroll system and added unannounced audits.’
Finance director, US

Middle East and South Asia

‘Hyperinflation and salary erosion triggered insider attempts. We had to relaunch whistleblowing and focus on enforcing consequences. Our message – fraud is everyone’s risk – and we are beginning to see attempts fall.’
CRO, banking, United Arab Emirates

‘Bank-detail changes matter – notarised originals, callbacks to a known number, and a “first-time beneficiary” hold. We now publish avoided-loss numbers to keep belief high.’
Head of finance, Qatar

‘We treat urgent voice-note instructions as hostile by default. If it’s emotional and “now,” it waits for verification.’
Finance lead, multi-sector, India