Pierag

Why Fraud Risk Matters More than Ever

Trends, Insights & the Way Forward

www.pierag.com

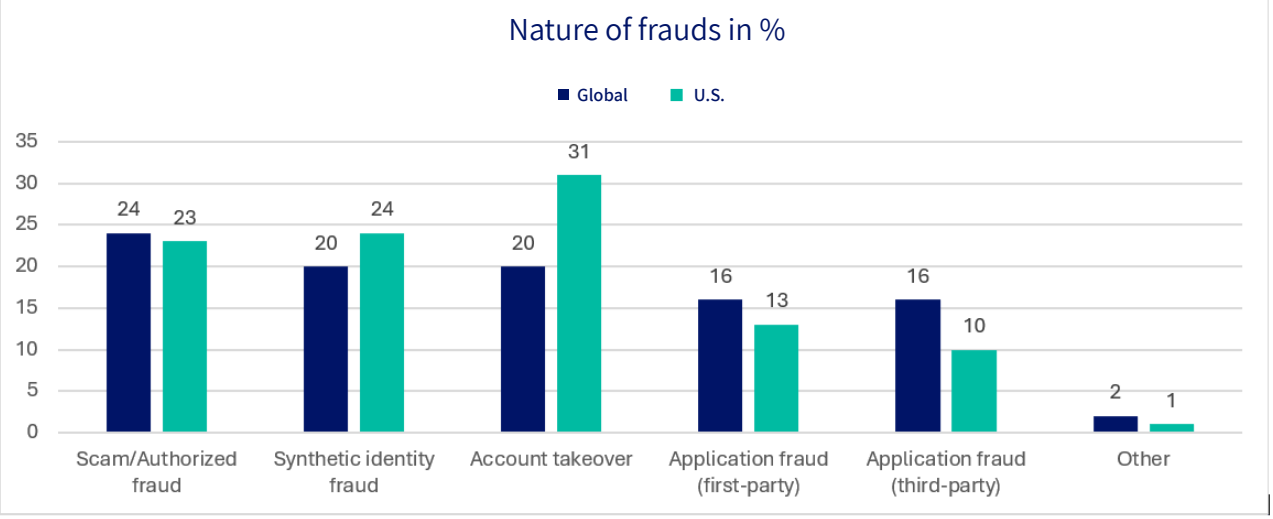
01

Introduction

Fraud has emerged as one of the most significant threats to organizations, regardless of size, sector, or geography. With rapid digitalization, interconnected supply chains, and increasing regulatory scrutiny, the risks associated with fraud have multiplied. According to global studies, Fraud continues to pose a major threat to organizations worldwide, with recent studies highlighting both its scale and evolving nature.

Recent global analyses conducted in 2025 by TransUnion indicate that organizations worldwide lost an average of 7.7% of their annual revenue to fraud over the past year, representing an estimated $534 billion among 1,200 surveyed business leaders. In some markets, the impact is even more pronounced—for example, businesses in U.S. reported average losses of 9.8% of revenue, marking a 46% increase from 2024 and 27% above the global average, amounting to roughly $114 billion among just the surveyed U.S. businesses.

The nature of fraud also varies by region. Globally, authorized scams (24%), synthetic identity fraud (20%), and account takeover attacks (20%) constitute the most significant loss categories. In the U.S., account takeover fraud emerged as the leading threat at 31%, followed by synthetic identity fraud (24%) and scam/authorized fraud (23%). Alarmingly, account takeover has surged 141% from H1 2021 to H1 2025, highlighting the rapid escalation and growing sophistication of cybercriminals.

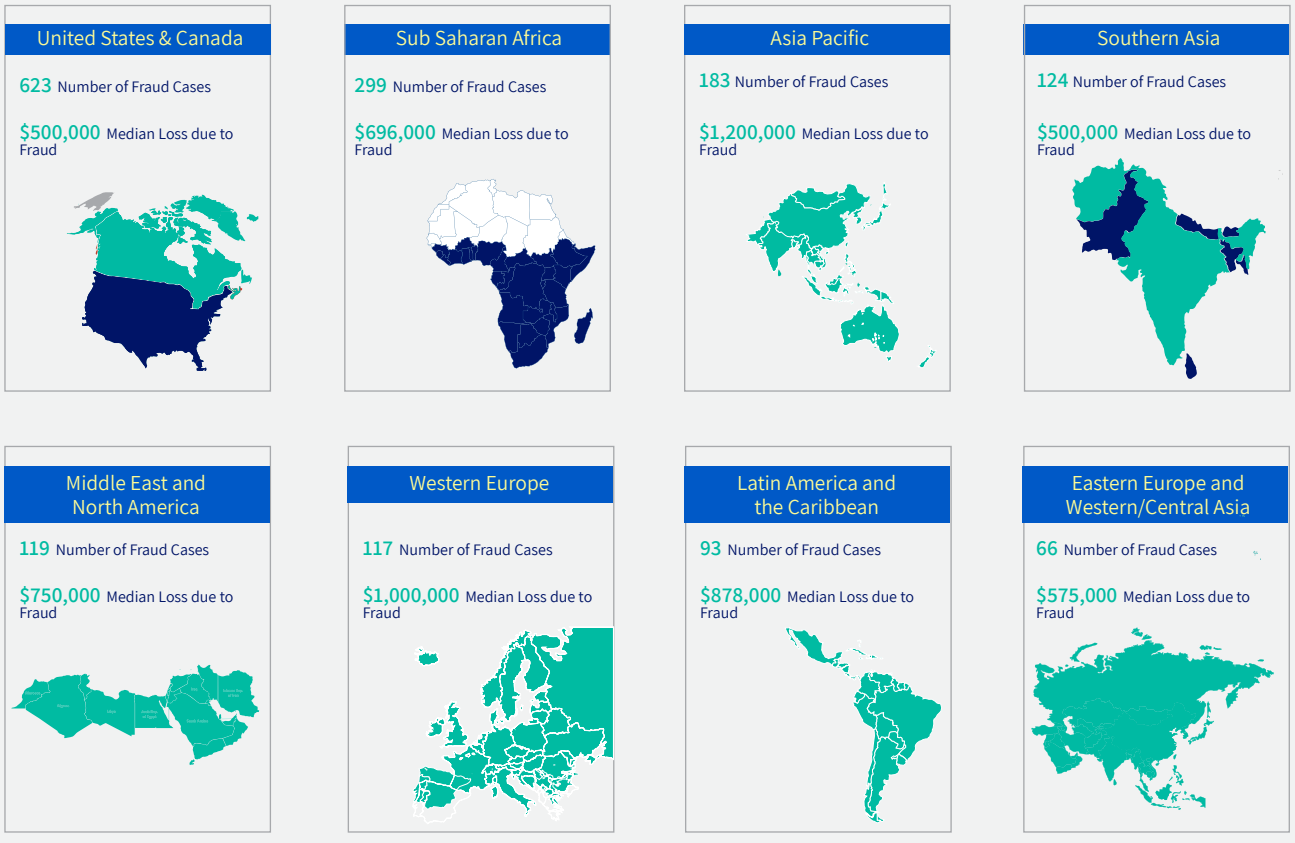


Additionally, consumer exposure mirrors these trends, with 48% of global consumers reporting they were targeted by email, online, phone, or text fraud, while 52% were unaware of any targeting. In the U.S., 51% of consumers were targeted, with 46% citing phishing and smishing, yet 49% remained unsure if they had been affected. These figures reveal both the scale of digital fraud and the critical gaps in awareness and prevention, underscoring the urgent need for businesses to adopt proactive, adaptive strategies to safeguard revenue, data, and customer trust.

Further, the ACFE's 2024 Report to the Nations found global fraud losses of $3.1 billion, with organizations estimated to lose 5% of annual revenue to fraud. A closer look at regional data shows sharp contrasts. While the U.S. and Canada account for the largest share of fraud cases, Asia-Pacific recorded the highest financial impact, with losses at the 75th percentile reaching $1.2 million, followed by Western Europe ($1.0 million) and Latin America & the Caribbean ($878,000). This variation reflects differences in control maturity, regulatory enforcement, and fraud detection capabilities across regions.

Below are the key insights or finding as per ACFE study:

Number of Fraud Cases by Region



Also, Fraud now affects every major industry—from security and financial services to e-commerce, retail, logistics, and manufacturing. In e-commerce, fraud has evolved beyond simple payment scams. Refund abuse, fake returns, identity theft, account takeovers, and first-party misuse create significant revenue leakage. In security-driven sectors, cyber-enabled fraud such as phishing, social engineering, and unauthorized access targets both systems and employees.

Traditional industries face procurement fraud, payroll manipulation, vendor collusion, and policy violations. Rising digital transactions and automation have increased fraud velocity, making early detection essential.

Across all studies, a consistent theme emerges that fraud is not only widespread but also financially and reputationally damaging, impacting revenues, investor confidence, governance, and long-term resilience. Organizations must strengthen anti-fraud controls, foster employee vigilance, and embed fraud risk management into core strategy to stay ahead of this growing challenge.

02

Categories of Fraud

There are **three main categories** of fraud such as :

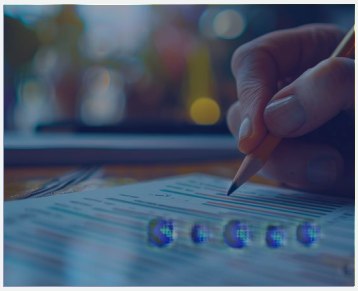
Asset Misappropriation

Misstatements or omissions in financial reporting (Net Income/Net Worth Overstatements or Understatements).

Corruption

Misstatements or omissions in financial reporting (Net Income/Net Worth Overstatements or Understatements).

Financial Fraud Statement



Misstatements or omissions in financial reporting (Net Income/Net Worth Overstatements or Understatements).

As per ACFE's 2024 Report to the Nations, **asset misappropriation** remains the most frequent type of occupational fraud, causing a median loss of around **$120,000 per case**. **Corruption** occurs less often but results in higher median losses of **$200,000 per case**. **Financial statement fraud**, although least common, has the most severe financial impact, with median losses reaching **$766,000 per case**.

The Changing Nature of Fraud – Emerging Trends

The **face of fraud has changed dramatically over the last decade.** While traditional schemes like asset misappropriation, payroll manipulation, and falsified expense claims persist, organizations today are confronting **more sophisticated, technology-enabled threats — from cyber breaches to AI-driven deception**.

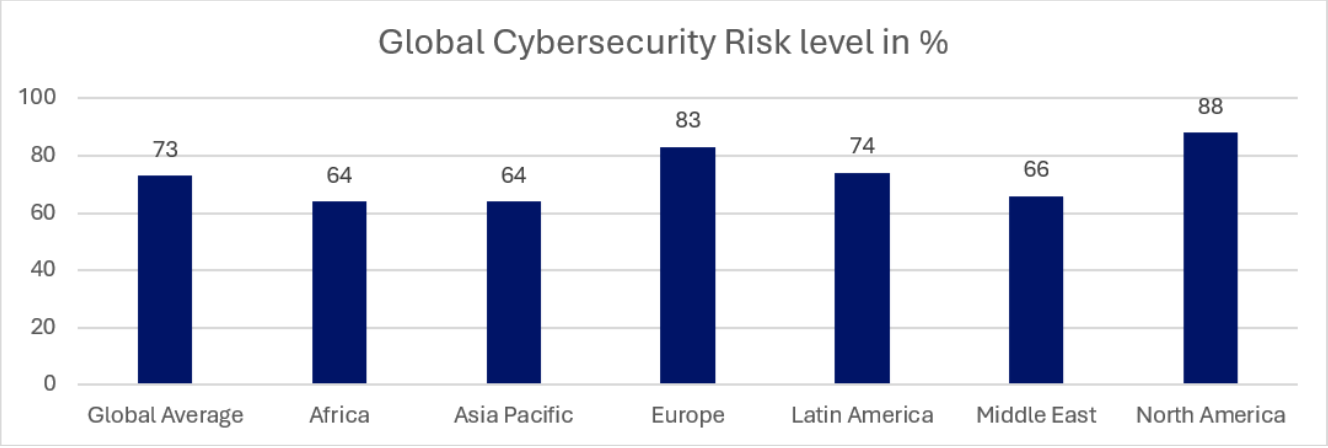
As fraudsters evolve, **corporate defences must evolve faster**. Embedding fraud risk management into business strategy, leveraging **data analytics and continuous monitoring**, and building a **culture of integrity and awareness** are now essential to protect organizational value, reputation, and stakeholder trust.

Below are some of the emerging fraud trends reshaping the risk landscape:

Emerging Scheme	Typical Scenario
Cyber-enabled frauds	Phishing, identity theft, ransomware, and digital payment frauds have become increasingly common.
Deepfake & AI-driven frauds	Fraudsters using synthetic voice/video to impersonate executives and authorize fraudulent transactions (e.g., deepfake CEO voice scams).
Business email compromise (BEC)	Fraudsters impersonating vendors or executives to trick employees into transferring funds.
Cloud & SaaS abuse	Exploiting vulnerabilities in cloud-based platforms to gain access to sensitive financial and operational data.
Synthetic identity fraud	Fraudsters combining real and fake personal data to create new identities used for loans, credit, or insurance claims.
Insider threats	Employees with privileged access colluding with external parties to exploit gaps in controls.

As these emerging schemes grow in scale and sophistication, one pattern stands out clearly — fraud is increasingly being powered by technology. Among all the new-age threats, Cyber-Enabled Fraud has rapidly become the most pervasive and high-impact risk, cutting across industries, geographies, and organizational sizes. Recent independent studies by leading bodies such as the IIA and other global institutions further validate this trend, highlighting why Cyber-Enabled Fraud now demands focused attention.

As per the latest IIA report, Cybersecurity remains the foremost risk, consistently ranked #1 with 73% concern last year and this year. Below is the comparison of global cybersecurity risk trends:



03

Fraud Risk Management is a **Culture, not a Control**

Too often, organizations equate fraud prevention with stronger internal controls. While controls are essential, they are not sufficient. A well-designed control framework can still be overridden if the organizational culture tolerates unethical practices or if leadership fails to set the right tone.

Tone at the top matters:

Leadership behavior strongly influences employee conduct. If leaders prioritize short-term gains over integrity, employees are more likely to bend rules.

Zero tolerance must be demonstrated:

Merely having a fraud policy is not enough — consequences of unethical behavior must be visible and consistent

Culture of openness:

Employees should feel safe raising concerns through confidential whistle-blower programs without fear of retaliation

True fraud risk management lies in shaping a culture of integrity where doing the right thing is rewarded and misconduct is never ignored. Controls prevent incidents, but culture prevents patterns.

04

Forensics as a **Strategic Enabler**

Fraud forensics is no longer about investigating fraud after it occurs — it is about using forensic techniques and analytics to predict and prevent fraud. Organizations today leverage forensic tools to detect anomalies, trace suspicious transactions, and monitor high-risk areas continuously.

Some examples of how forensic practices are evolving:

Forensic data analytics:
Using algorithms to detect unusual payment patterns, duplicate invoices, or round-dollar transactions that may indicate manipulation.

AI and machine learning:
Training models to identify red flags in real time, such as abnormal user access behaviour or vendor anomalies.

Digital forensics:
Recovering deleted evidence, analysing emails, and securing electronic trails that may reveal collusion.

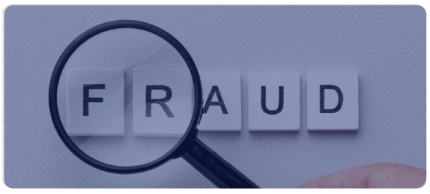
Behavioural analytics:
Monitoring employee patterns (e.g., excessive overtime, sudden lifestyle changes) as potential fraud indicators.

Forensics is no longer a reactive service — it is a strategic enabler that helps organizations build resilience by detecting risks earlier, saving costs, and protecting reputation.

05

Building a Proactive Fraud Risk Framework

Organizations need a structured approach to proactively manage fraud risks rather than reactively responding after damage has occurred.
A comprehensive framework typically includes:



Fraud Risk Assessment

- Periodic assessments to identify high-risk processes, geographies, and third parties.
- Mapping of fraud scenarios and quantifying potential impact.

Whistleblower Programs

- Confidential and accessible reporting channels.
- Independent case management and assurance to employees of non-retaliation

Data Analytics Integration

- Embedding fraud monitoring scripts within ERP systems.
- Continuous transaction monitoring for high-value or unusual transactions.

Fraud Awareness & Training

- Regular employee training on recognizing red flags.
- Simulation exercises to test organizational readiness.

Response & Investigation Protocols

- Defined forensic investigation playbooks.Clear accountability on who investigates, who reviews, and how outcomes are reported.

Proactive fraud risk frameworks shift the conversation from “who committed fraud” to “how can we prevent fraud from happening in the first place

06

The Future of Fraud Risk Advisory

Fraud risk management is evolving from being a compliance-driven function to a strategic pillar of corporate governance. Advisory professionals play a critical role in this shift.

Predictive and Real-Time Monitoring

Moving from post-incident detection to continuous, data-driven monitoring using AI and analytics.

Integration with Governance

Moving from post-incident detection to continuous, data-driven monitoring using AI and analytics.

Use of Advanced Technologies

Leveraging machine learning, blockchain, and automation for fraud detection and prevention

Behavioural and Cultural Focus

Building a strong ethical culture and promoting awareness through training and tone at the top

Third-Party and Cyber Risk Oversight

Expanding focus beyond internal controls to monitor vendors, partners, and digital ecosystems.

The future of fraud risk advisory lies in being a strategic partner to leadership — enabling not just compliance but building stakeholder trust and protecting organizational value.

07

Closing Thought

Fraud prevention today demands far more than strong controls—it requires the right culture. As fraud techniques evolve rapidly across digital, financial, and operational domains, organizations must stay alert, act decisively, and promote integrity in everyday decisions. While technology, analytics, and automation play a crucial role in detecting anomalies and strengthening defences, they deliver meaningful impact only when supported by a culture grounded in honesty, transparency, and accountability.

At Pierag Consulting, we combine both dimensions to build truly resilient organizations. Our Fraud Services provide end-to-end support—from fraud risk assessments, forensic investigations, whistleblower frameworks, and e-commerce fraud management to cyber and identity fraud controls, continuous monitoring, and awareness training—ensuring businesses are protected across every layer.

Supported by our Business Risk Advisory and Technology Risk Advisory practices, we help clients design robust fraud-risk frameworks while simultaneously embedding strong cultural foundations. In a world where trust can be lost instantly, we enable organizations to stay secure, responsible, and future-ready.

Reference and Further Reading:

1. COSO Fraud Risk Management Guide – COSO principles and guidance: COSO-Fraud Risk Management Guide-E Summary_8 5x10 875_r1 (3).pdf
2. ACFE White Paper Library: White Paper Library
3. ACFE Occupational Fraud 2024: Report to the Nations: ACFE Press Release

Pierag Consulting

Pierag Consulting was founded in February 2021 by Abhishek Gupta, Thomas Raffa and Pierian Services as a unique business model to serve clients globally by blending domestic proficiency with global expertise. Since then, we have been serving prominent clients across the US, SEA, India and UK in the field of Assurance, Accounting & Transactions Advisory, Business Risk, Technology Risk Advisory and ESG & Sustainability.

With more than 150+ team members and offices across India (Gurugram, Jaipur, Chandigarh, Mumbai and Bengaluru), US, Australia and Singapore, we are fueled by our purpose of 'Inspiring people to do things that inspires them' and our values of 'Excellence, Equity & Empathy'.

www.pierag.com | info@pierag.com

Gurugram
Level 18, DLF Square, DLF Phase II, Gurugram, Haryana - 122002

Mumbai
One International Centre, Tower 1, 8th Floor Lower Parel, Mumbai – 400013

Bengaluru
Brigade Software Park 27th Cross Rd, Banashankari Stage II, Bengaluru, Karnataka - 560070

Jaipur
Level 5, Jaipur Centre, Tonk Road, Sector B4, Jaipur, Rajasthan - 302018

Chandigarh
W4-G, Level 4, Tower A, Godrej Eternia Towers, Industrial Area, Phase I, Chandigarh - 160002

Washington, D.C.
1899 LST NW, Washington, D.C. - 20036

Singapore
12 Marina Boulevard Marina Bay Financial Centre, Singapore - 018982

Melbourne
2.14, 111 Overton Road, Williams Landing, VIC Australia - 3027