KPMG

Global profiles of the fraudster

India outlook

The enemy within — profiling the fraudster

July 2025

KPMG. Make the Difference.

Contents

Introduction

Business environment today is complex, and so is the fraud landscape. Fraudsters have become more digital and sophisticated, putting organisations under pressure to strengthen their detection capabilities beyond conventional controls. Typically, a fraudster is not someone outside your gates, it is, rather, someone within your trust circle. According to KPMG's Global Profiles of the Fraudster, a **typical fraudster is a male** and has served his/her organisation for more than **six years**. So, the question that remains at the forefront is-who is the enemy within and what are his/her methods?

To understand and uncover the profile of the fraudster, KPMG conducted a wide-ranging global survey, revealing insights from **669 real-world cases**. The survey throws light on the nature of frauds and fraudsters, system vulnerabilities and cyber frauds. Both India and global editions of the report suggest that **weak controls** are the prime reason for frauds.

Through this survey, we intend to assist organisations to prevent, detect and respond to fraud, making it more difficult to commit. This will enable our clients to understand the complex field of fraud and how it is likely to change in the future.

We hope this survey will foster discussions around nature of fraudsters, and will help organisations, government and society, at large, to combat frauds.

Key insights from the survey

- The most prevalent type of fraud, both globally and in Indian context is **misappropriation of assets.**
- **Weak controls** are considered the prime reason for the frauds.
- The number one detection method is tip-offs via **whistleblowers or informal sources.**
- The most dominant motivating factor among the perpetrators is **financial gain/greed.**
- Insights gathered from global survey and India suggest that a typical fraudster is a **male** who has served his/her organisation for more than **six years.**

Profile of a fraudster

Clearly no two criminals are exactly alike, but our survey reveals some common traits. While globally, a typical fraudsters is male between 36 and 55 years old, India suggests otherwise. In India, the age range of a fraudster is between 26-45 years, reasonably long-serving, having worked for the victim organisation for more than six years. Globally, seniority was fairly evenly split between executives (31 per cent), management (30 per cent) and staff (24 per cent). And just over half (51 per cent) worked for multinational and/or global companies. There doesn't appear to be much in these individuals' characters to arouse immediate suspicion. They are generally described as 'highly respected', 'extroverted' and 'friendly', with a 'medium to-high reputation' — although they are characterised by a sense of superiority. Interestingly, they didn't show signs of having an obvious grievance against their employer.

In terms of organisational seniority, global data shows that non-executive management is involved in approximately 30.19 per cent of fraud cases, followed by staff members at 24.15 per cent and executive directors at 19.25 per cent.

India reflects similar trends, with non-executive management accounting for the highest proportion of fraud cases at 39.13 per cent, followed by executives at 28.26 per cent, and staff at 13.04 per cent. Notably, a significant portion of perpetrators, both globally and in India, had unlimited authority, which facilitated the commission of fraudulent acts.

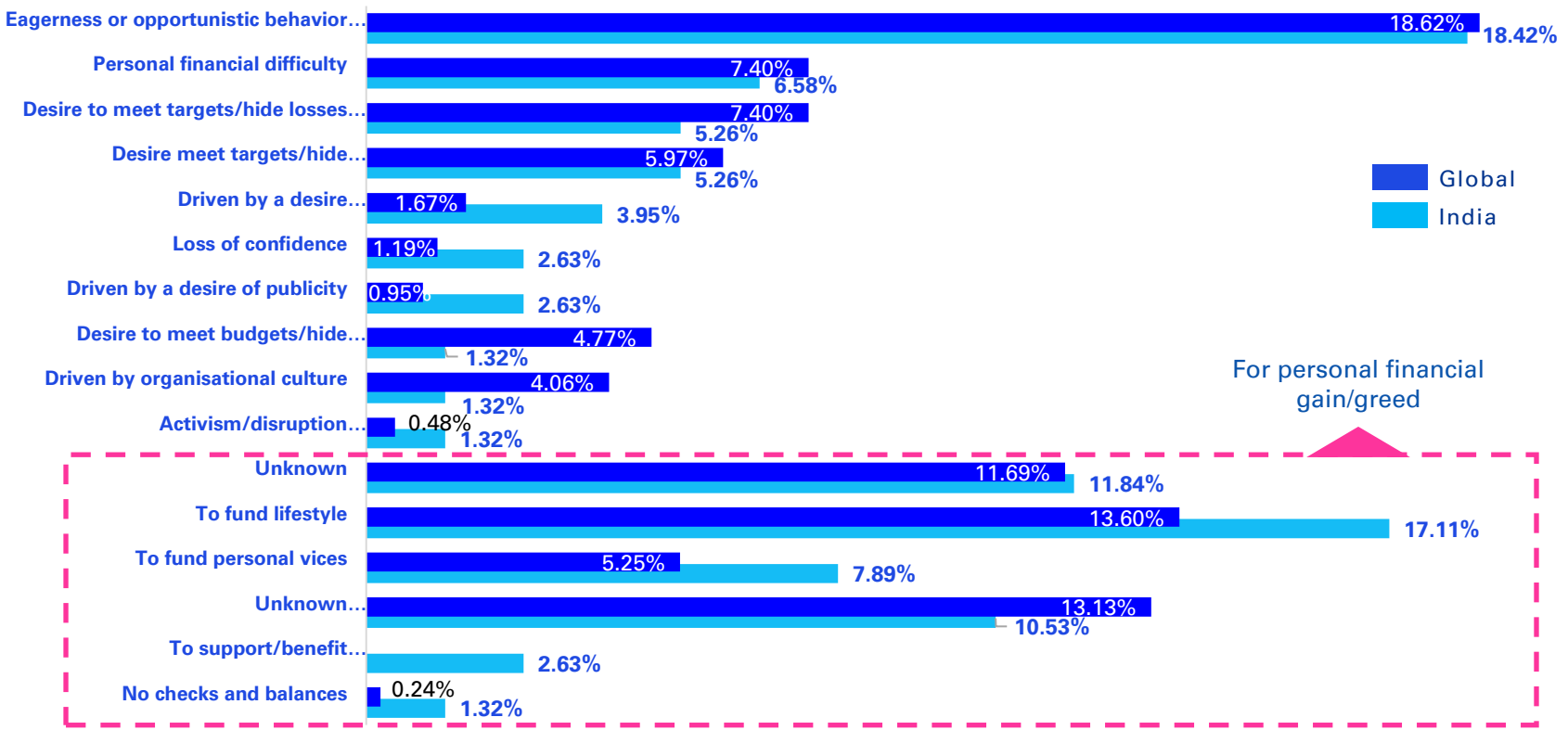
Key differences

- Financial loss from frauds studied in the global survey were **below USD 2 million** (69 per cent). Meanwhile, in India, 72 per cent of the frauds fell **below USD 0.2 million.**
- Globally, frauds occurred in a range of different departments. In India, more than 50 per cent of frauds in India were committed in **procurement and operations.**
- In India, a typical fraudster falls within the **26 to 45 years** of age range, in contrast to the age range of **36 to 55 years**, as highlighted in the global survey.
- As per the global survey, **80 per cent** of the collaborators were acting as an **agent**. Meanwhile, in India, this figure stood at only **19 per cent.**
- Globally, around **13 per cent** of the fraudulent acts involved **cross-border crime**. Meanwhile, just **two per cent** of frauds involved cross-border crime in India.

Motivational insights from India closely mirror global findings, with the primary driver being financial gain or greed. Opportunistic behaviour emerges as the second most dominant factor, followed by personal financial difficulties and the pressure to meet performance targets.

Motivation of the perpetrator

A breakdown of the underlying motivations for fraud, such as personal financial gain, pressure to meet performance targets, or other personal or professional reasons.

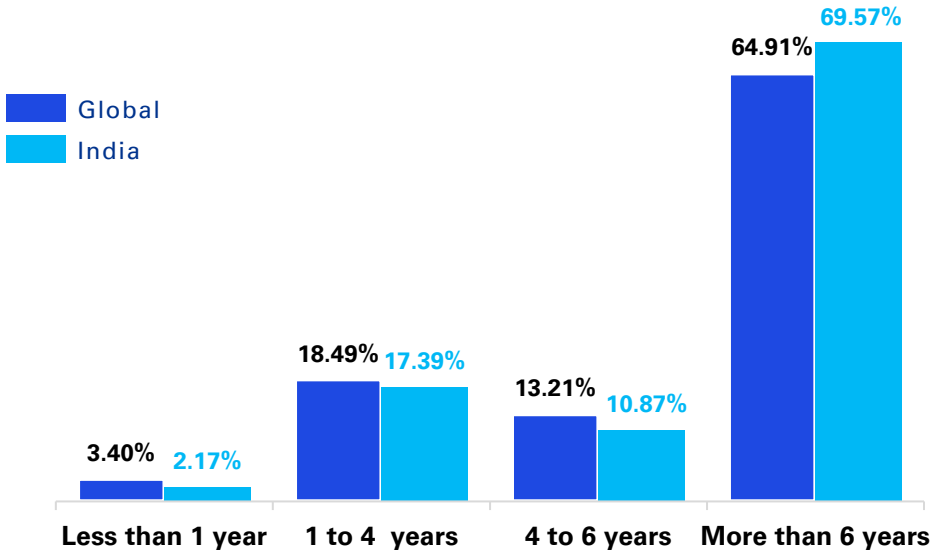


Insights from data relevant to India's fraud landscape closely follows those from the global survey. The **most dominant motivating** factor among the perpetrators is **principal financial gain/greed. Opportunistic behaviour** is the second most dominant motivating factor as per the results, followed by **personal financial difficulties and desire to meet targets.**

India and global respondents show **similar motivations in opportunistic behavior (18.5 per cent) and personal financial greed (11.8 per cent),** while **diverging on funding personal vices (India: 7.89 per cent, Global: 13.60 per cent) and desire for better ratings (India: 3.95 per cent, Global: 1.67 per cent).**

Years of service

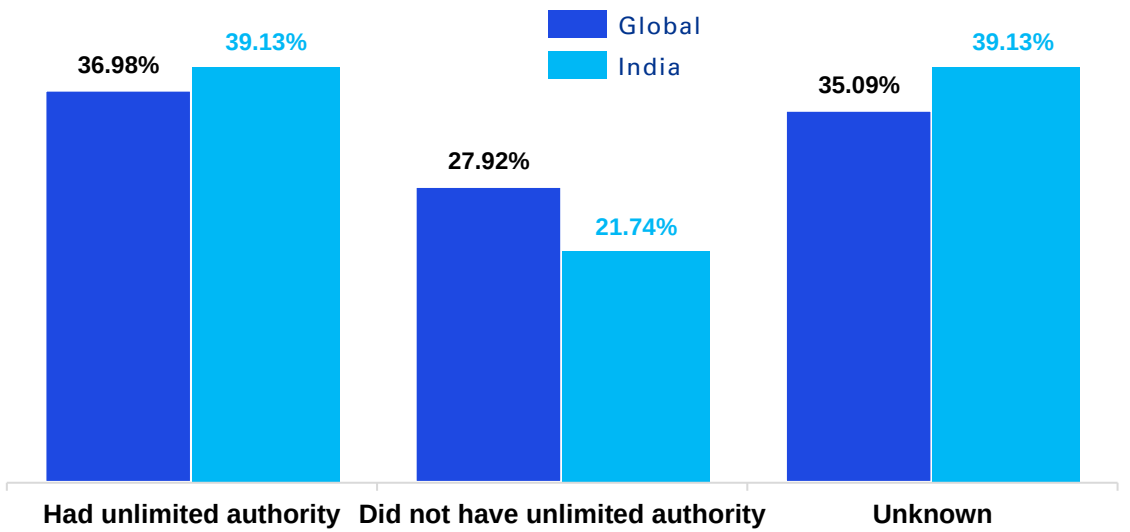
A breakdown of the perpetrator's tenure within the organisation, helping to identify patterns related to the duration of employment and its potential link to fraudulent behaviour.



Majority of the perpetrators were l**ong serving employees** of the victim organisation, having **served for more than six years**, suggesting that they hold a position of trust and have in-depth knowledge of internal systems and processes.

Authority level

An investigation into whether the perpetrator's access to unlimited authority within the organisation contributed to their ability to commit fraud, highlighting the risks associated with unchecked power.



The results of the investigations suggest that a **relevant portion of the perpetrators had unlimited authority** which facilitated the commission of the fraudulent acts both globally and in India

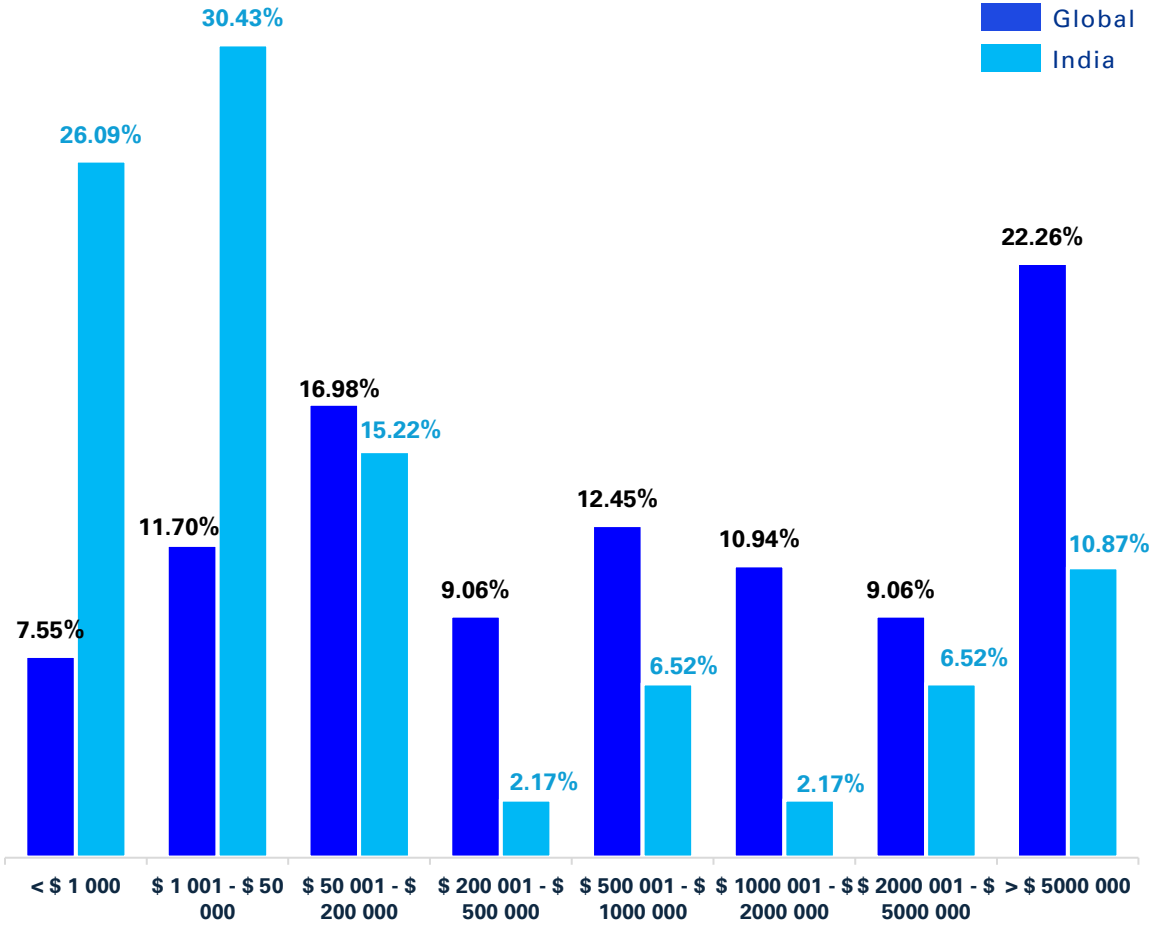
Approximate financial loss

A detailed look at the total financial loss experienced by the victim, measured in monetary terms, to assess the severity of the fraud's financial consequences.

Most of the frauds studied in the global survey were **below USD 2 million**. 20 per cent were between USD 1 million and USD 5 million. Around 22 per cent of frauds resulted in loss more than USD 5 million. **Just 13 per cent involved cross-border crime**, but these tended to be higher-value fraud — almost half incurring damages of USD5 million or more.

In the Indian context, about **72 per cent of the reported fraud involved financial loss below USD 200,000. Around 9 per cent of the loss amount lies between USD 1 million and USD 5 million.** This indicates that the scale of financial loss in India tends to be lower than in global cases. Only around **11 per cent of the loss amount was greater than USD 5 million**. Just 2 precent involved cross-border crime incurring damages more than USD 5 million.

While 72 per cent of Indian frauds are under $200,000 nominally, in purchasing power parity terms this translates to a much larger local impact—**potentially equivalent to nearly $1 million of spending power in India.**

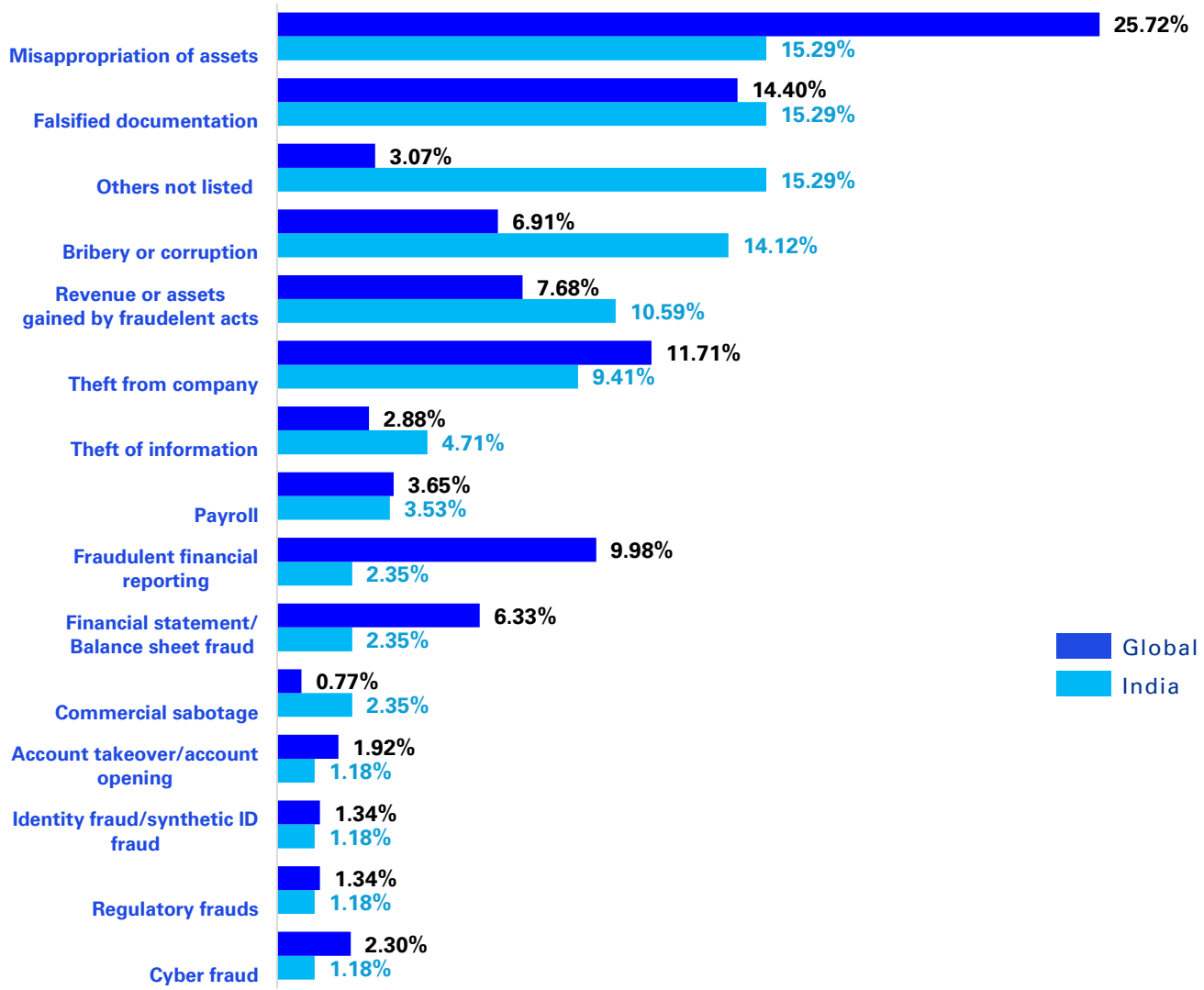


What kind of fraud was committed?

A detailed categorisation of the types of fraud committed, including misappropriation of assets, bribery, cyber fraud, and more, to understand the specific nature of the fraudulent actions.

According to a global survey, the **most prevalent form of fraud is asset misappropriation (26 per cent).** This is followed by **falsified documentation,** which accounts for **14 per cent of the cases**, while **theft from the company** ranks third at **12 per cent.**

Similarly, in India, **misappropriation of assets** and **falsified documentation** are the most common types of fraud, amounting to **30 per cent** of the total cases. Meanwhile, **bribery and corruption** holds the second spot in India, amounting to **14 per cent** of the total cases.

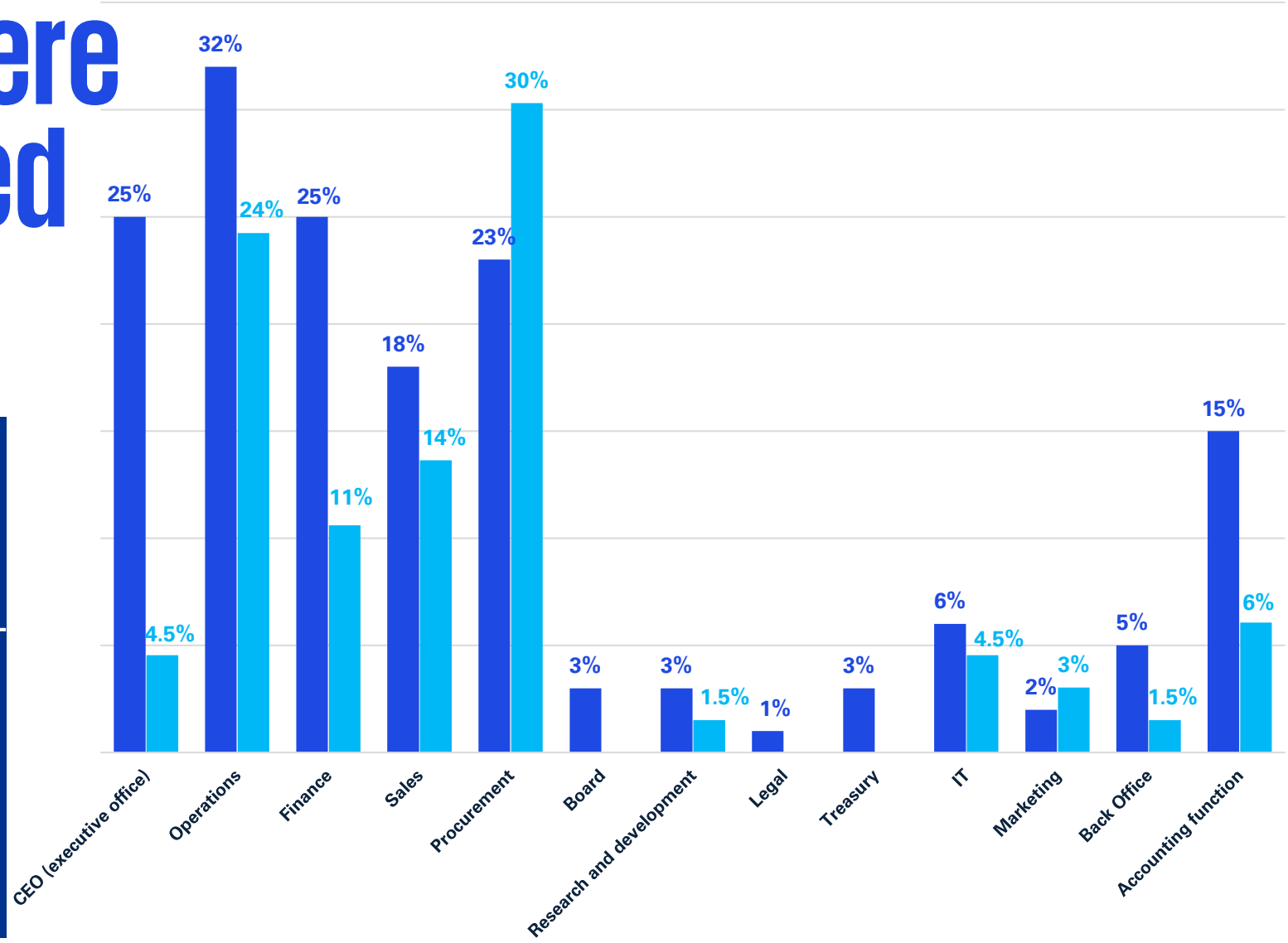


Departments where the fraud occurred

A summary of the specific departments within the organisation where fraud incidents occurred, offering a deeper look into which sectors are most vulnerable

As per the global survey, frauds occurred across a range of departments, most **notably operations (32 per cent), finance (25 per cent), the CEO's office (25 per cent) and procurement (23 per cent).**

In the Indian context, it was observed that **more than 50 per cent of the fraud was committed in procurement (30 per cent) and operations (24 per cent) departments.** This indicates that within these departments, **the opportunities to commit fraud are greater.** Involvement of finance department was only **11 per cent. CEO's office was involved in only 5 per cent of the cases.**



The nature of the fraud — and where it happened

Fraud exhibits differently across geographies, shaped by organisational structures, regulatory environments, and internal controls. Globally, fraud tends to be higher in value and more complex, with 22 per cent of cases resulting in losses over USD5 million and 13 per cent involving cross-border elements. In comparison, India sees a dominance of lower-value frauds, with 72 per cent of cases involving losses under USD200,000 and only 2 per cent involving cross-border activity.

The most common types of fraud globally was misappropriation of assets, representing 26 per cent of all the reported cases, followed by falsified documentation (14 per cent) and theft from the company (12 per cent). India displays a similarity, with asset misappropriation and falsified documentation accounting for almost 30 per cent of cases. However, bribery and corruption are more predominant in India (14.12 per cent) rather than theft from the company being the third highest globally, indicating a different set of systemic vulnerabilities.

Globally fraud is evenly distributed across departments like operations (32 per cent), finance (25 per cent), the CEO's office (25 per cent), and procurement (23 per cent). However, in India, procurement (30 per cent) and operations (24 per cent) dominate, while finance (11 per cent) and the CEO's office (5 per cent) play a smaller role. This suggests that Indian fraudsters are more likely to exploit in operational and procurement loopholes, possibly due to weaker supervision or process inefficiencies in these areas.

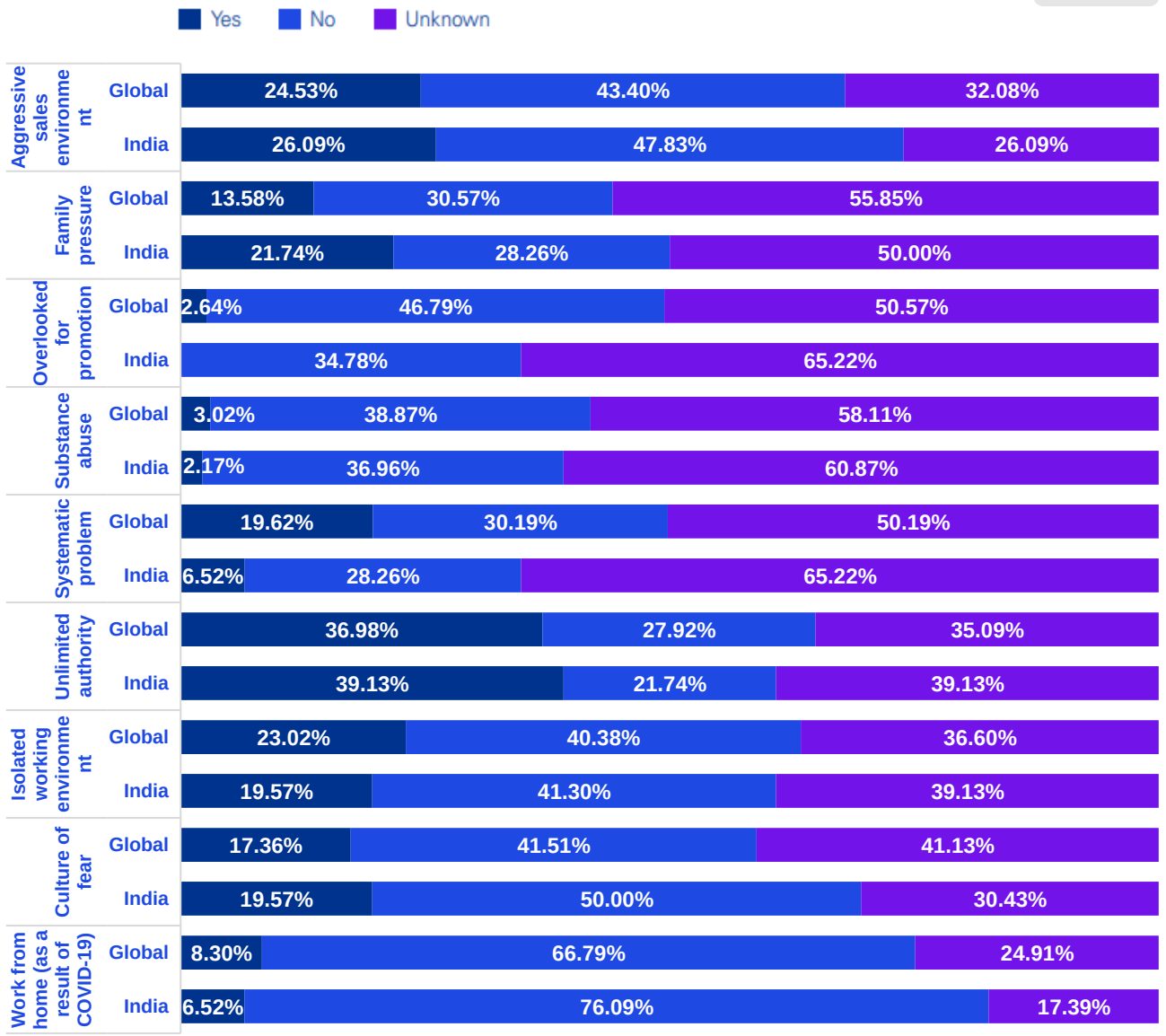
The Indian fraud landscape is different regarding to scale, scope, and departmental concentration. While global fraudsters profile operates across borders and departments with high financial stakes, Indian frauds are more localised, lower in value, and more focused in procurement and operations.

Exposing systemic vulnerabilities

Looking at the global survey, **unlimited authority** was the biggest factor that shaped the perpetrator's context. This was followed by **aggressive sales environment, isolated work environment** and **systematic problems.**

Unlimited authority was the biggest factor that shaped the perpetrator's context in India. This was followed by **aggressive sales environment, family pressure**.

Both in India and globally, employees align on the importance of systemic processes and work-from-home flexibility, while the difference lies in the culture of fear and overlooked for promotion.

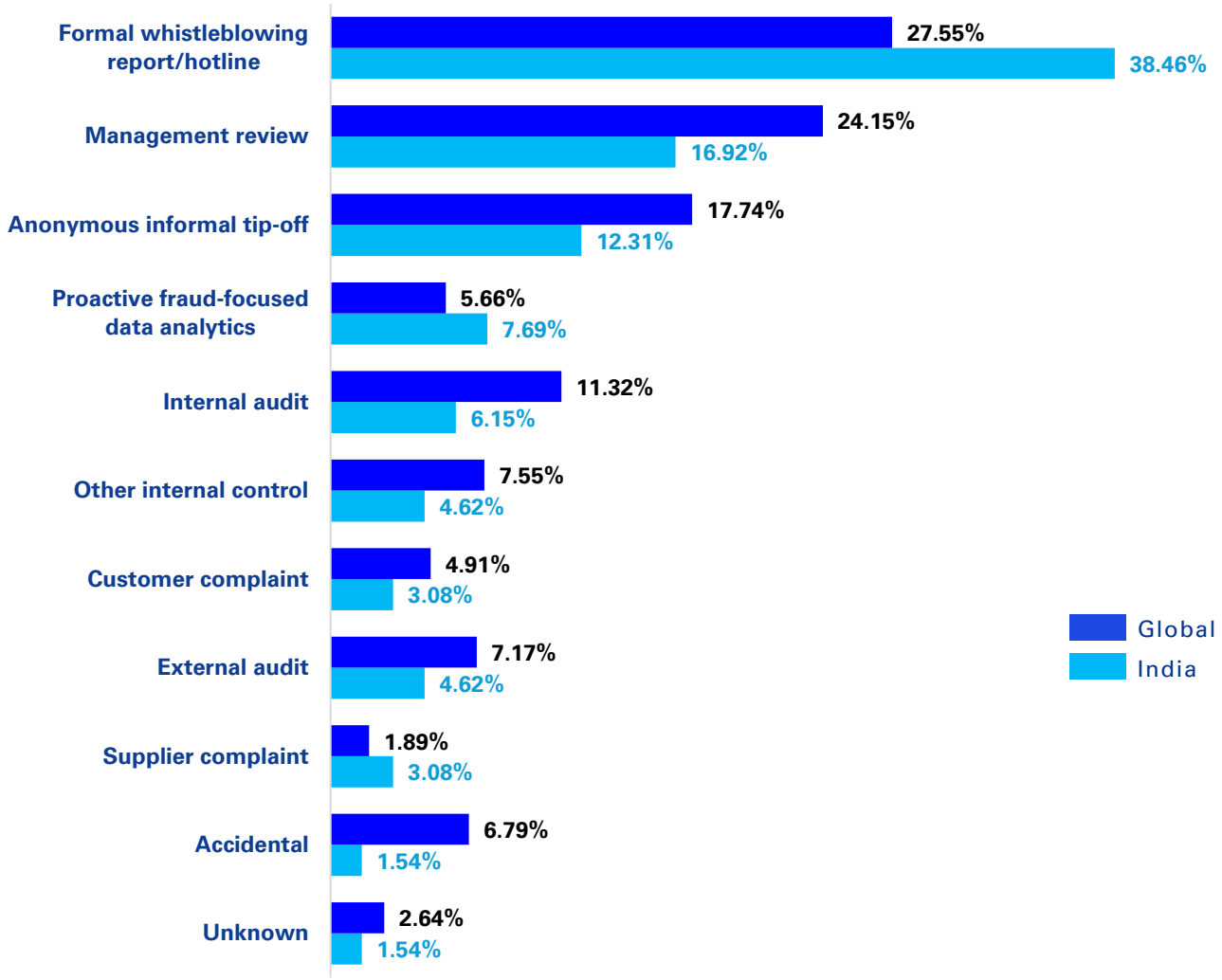


What led to the detection of fraud?

An overview of the various methods and channels through which fraud was detected, including anonymous tip-offs, internal audits, external audits, and more.

As per the global survey, formal **whistleblowing report/hotline** accounts for the **highest share of fraud detection** at **27.55 per cent**, followed by **management review** at **24.15 per cent**, while **17.74 per cent** of cases are detected through **anonymous informal tip-offs.**

Even in India, formal **whistleblowing report/hotline remains at top with 38.46 per cent** of cases, mirroring global trends. This was followed by **management review at 16.92 per cent** and **anonymous informal tip-off at 12.31 per cent**, with **top three means** to detection of fraud being identical in both context.



Exposing systemic vulnerabilities(1/2)

Fraud typically results from a series of overlooked indicators; it is usually the result of a much deeper issues within an organisation. When we look at global trends and compare them with India's, some similarities and a few important differences appear.

Globally, the most significant contributor to fraud is the presence of **unlimited authority**. When individuals holds significant power without accountability, the possibility of misconduct escalates substantially. This is often compounded by an **aggressive sales environment, isolated work settings,** and broader **systemic issues** within organisations. These factors collectively promote a culture where performance is prioritised over integrity, and ethical boundaries are easily compromised.

In India, the picture is quite similar, with some distinctive variations. While **unlimited authority** remains one of the biggest concerns, **family pressure** also plays a significant role. When financial success is tied to family expectations, the pressure to meet those standards sometimes lead to desperate actions which can be immense. In an **aggressive sales environment,** such pressure can easily push individuals towards making an unethical decision.

Exposing systemic vulnerabilities (2/2)

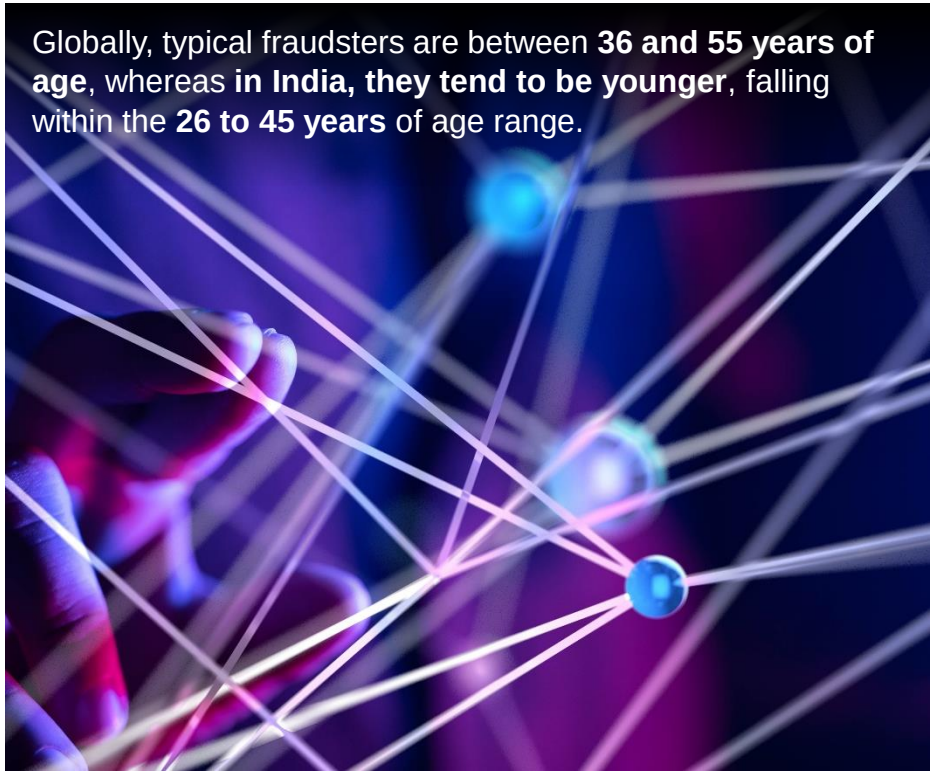
When it comes to how fraud is uncovered, both globally and in India, **whistleblowing systems/hotlines** are leading the way. Globally, about 27.55 per cent of fraud cases are detected through official hotlines or reports. In India, that number jumps to 38.46 per cent, which is encouraging. It shows that more people are willing to speak up when they see something wrong. **Management reviews and anonymous tip-offs** also play a big part, showing that both formal processes and informal vigilance are essential.

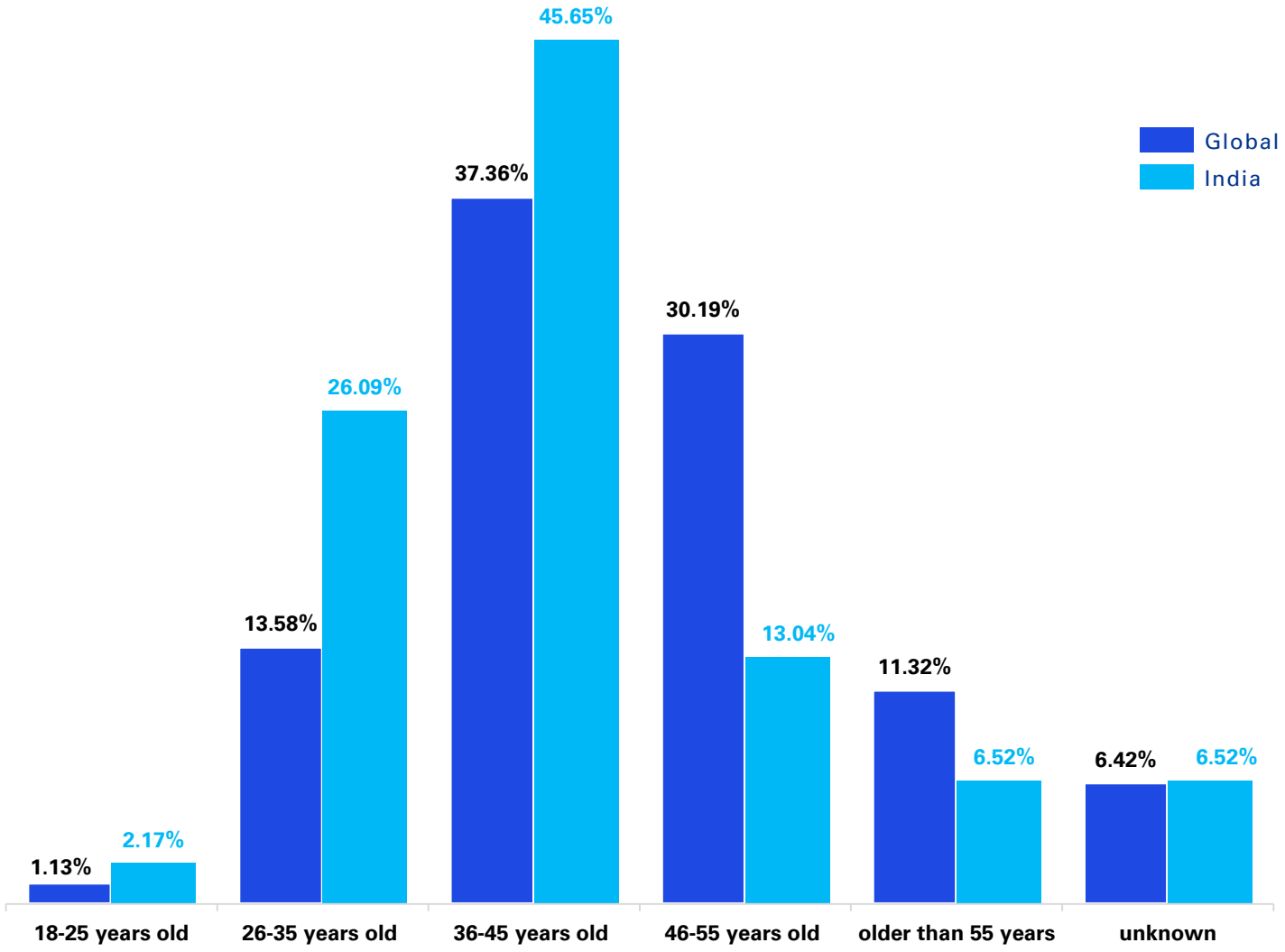
These findings suggest a lack of adequate checks and balances within internal control systems, and a need for stronger oversight and clearly defined limits on authority. No matter how senior or charismatic an individual may be, formal limits and controls should be applied and consistently enforced.

Given the shift to remote work have introduced new challenges but have not significantly driven increased fraud. However, given the rapid evolution in technology-led fraud, organisations should adapt their controls to this new working environment.

Perpetrator's age

A breakdown of the age groups of individuals who committed the fraud, providing insights into how age may correlate with fraudulent behavior.



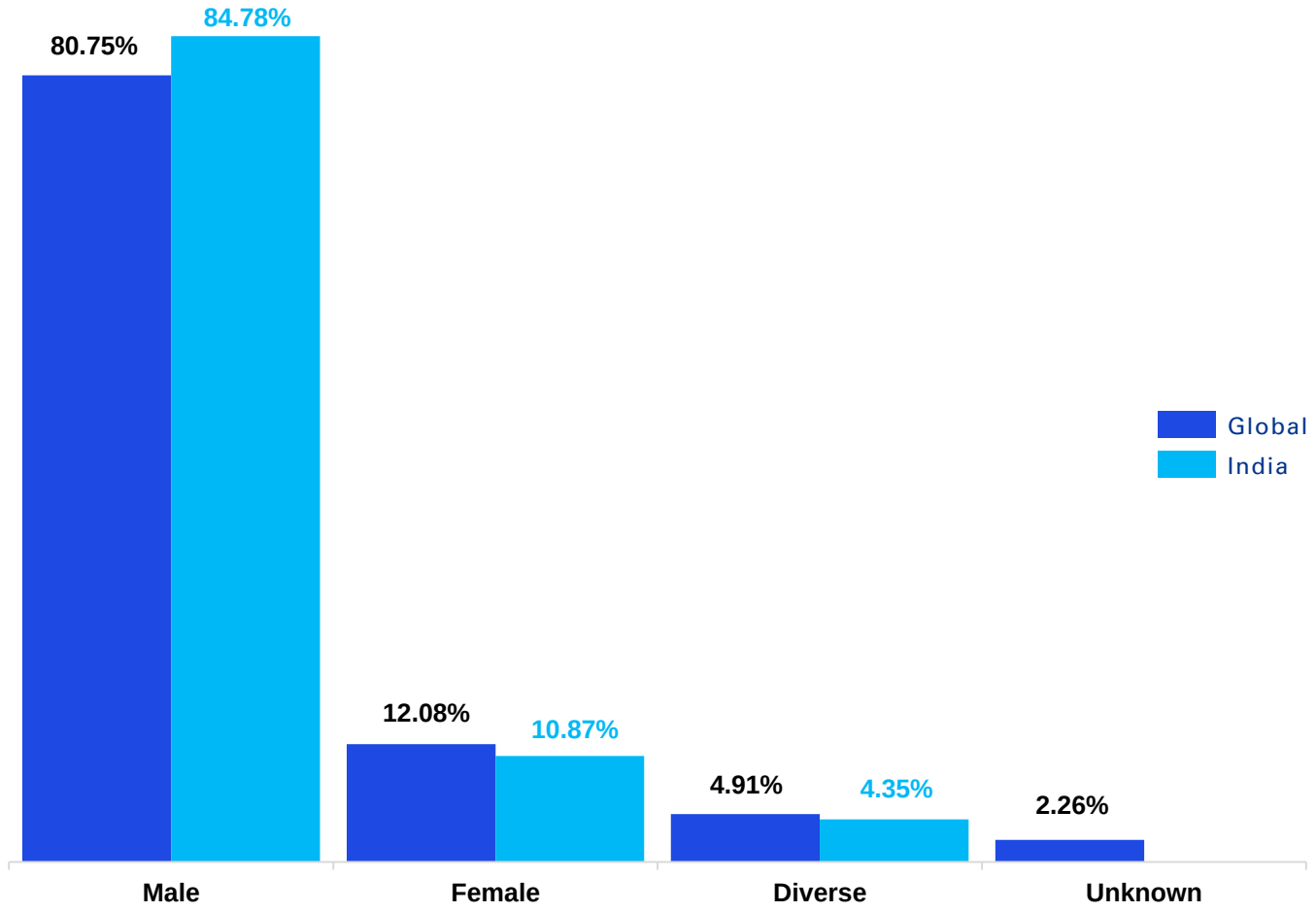


Perpetrator's gender

An exploration of the gender distribution of perpetrators, identifying whether the fraud was more prevalent among male or female individuals.

The global survey underscores **male dominance among perpetrators at 80.75 per cent**, while **female offenders remain significantly lower at 12.08 per cent**. Additionally, **diverse individuals account for 4.91 per cent**, with **2.26 per cent unidentified**, reflecting a clear gender disparity in reported offenses.

India exhibits **similar trends to global patterns**, with **male perpetrators dominating at 84.78 per cent**, while **female offenders remain significantly lower at 10.87 per cent**, and **diverse individuals account for 4.35 per cent**.

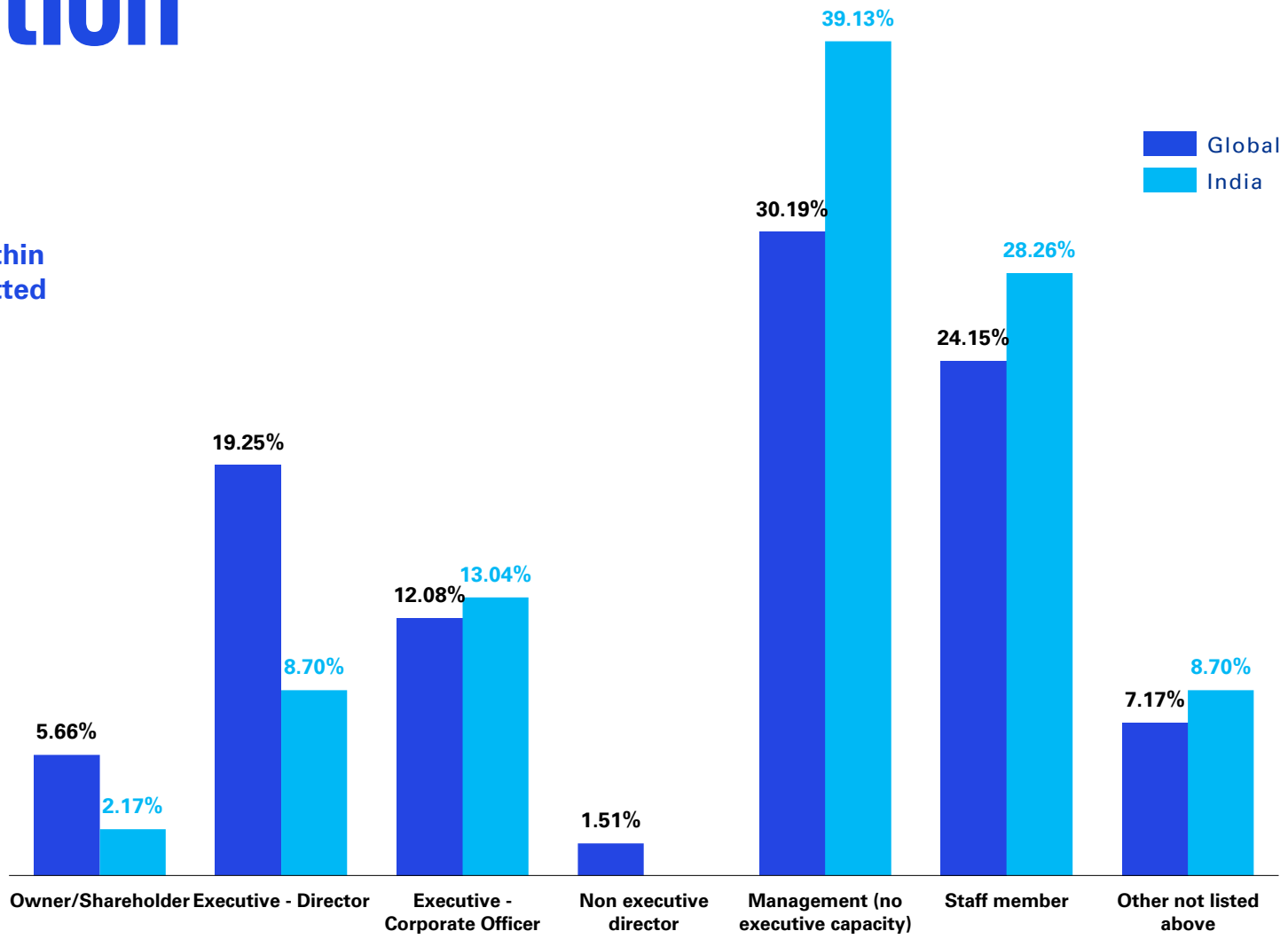


Perpetrator's position and seniority

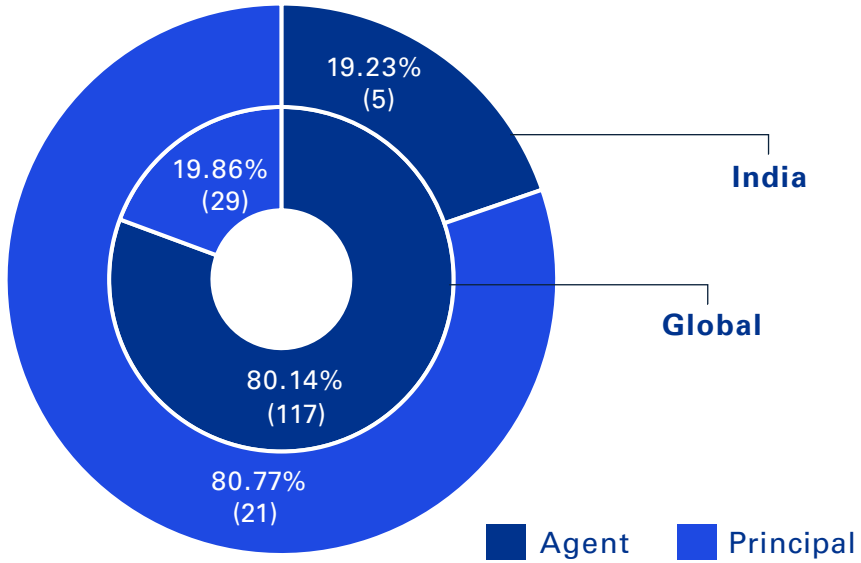
A classification of the perpetrator's position and seniority within the organisation, highlighting whether the fraud was committed by lower-level staff or higher-level executives.

The global survey highlights management (no executive capacity) involvement in **30.19 per cent of cases**, nearly **one-third of incidents. Staff members account for 24.15 per cent (one-fourth), while executive directors are implicated in 19.25 per cent (one-fifth).**

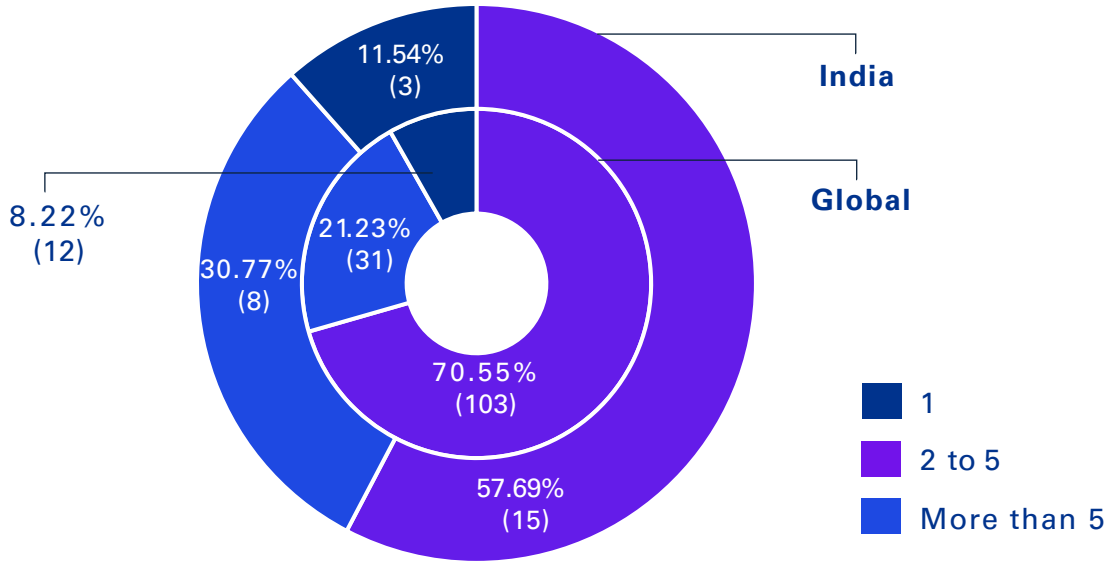
India exhibits **nearly similar trends to global patterns,** with **management (no executive capacity) involved in 39.13 per cent of cases.** Additionally, **staff members are implicated in slightly more than one-fourth of incidents.**



Understanding the collaborators



An investigation into whether the fraud collaborator acted as a principal (main actor) or an agent (a subordinate or intermediary), shedding light on the nature of the collaboration.



An examination of how many individuals were involved in the fraudulent act, ranging from a single collaborator to groups of more than five individuals, providing insight into the scale of the fraud.

In India, **57 per cent of the fraudsters colluded with others in commission of the fraudulent act**. Meanwhile, in global context, this figure stands at 55 per cent.

For majority of the fraudulent acts committed within India and at global level, it can be observed that around **2 to 5 individuals** were involved as collaborators.

Stark difference is noted between the global survey and the India specific observations in the nature of collaboration. 81 per cent of the collaborators acted as the principal (main actor) in the India, whereas 80 per cent of the collaborators acted as an agent (subordinate or intermediary) in the global survey.

Understanding the collaborators

Fraud is rarely a solo act, it often involves collaboration, whether between colleagues or within a hierarchy. When we compare how these collaborations play out in India compared to the global scene, some notable differences come to light. Globally, around 55 per cent of fraud cases involve more than one person, while in India, the number is slightly higher at 57 per cent. This indicates that while collaboration in fraud is common in both, it's a bit less frequent in the Indian context.

Diving deeper into the breakdown of the roles people play, the global data reveals that about 70.55 per cent of those involved acted as masterminds, the main decision-makers while under 29.45 per cent acted as middleman or facilitators. In India, however, there is more balanced distribution, with 57.66 per cent acting as main decision makers and 42.34 per cent as agents. This indicates that in India, fraud tends to involve more people at the operational-level, rather than being directed solely from the top.

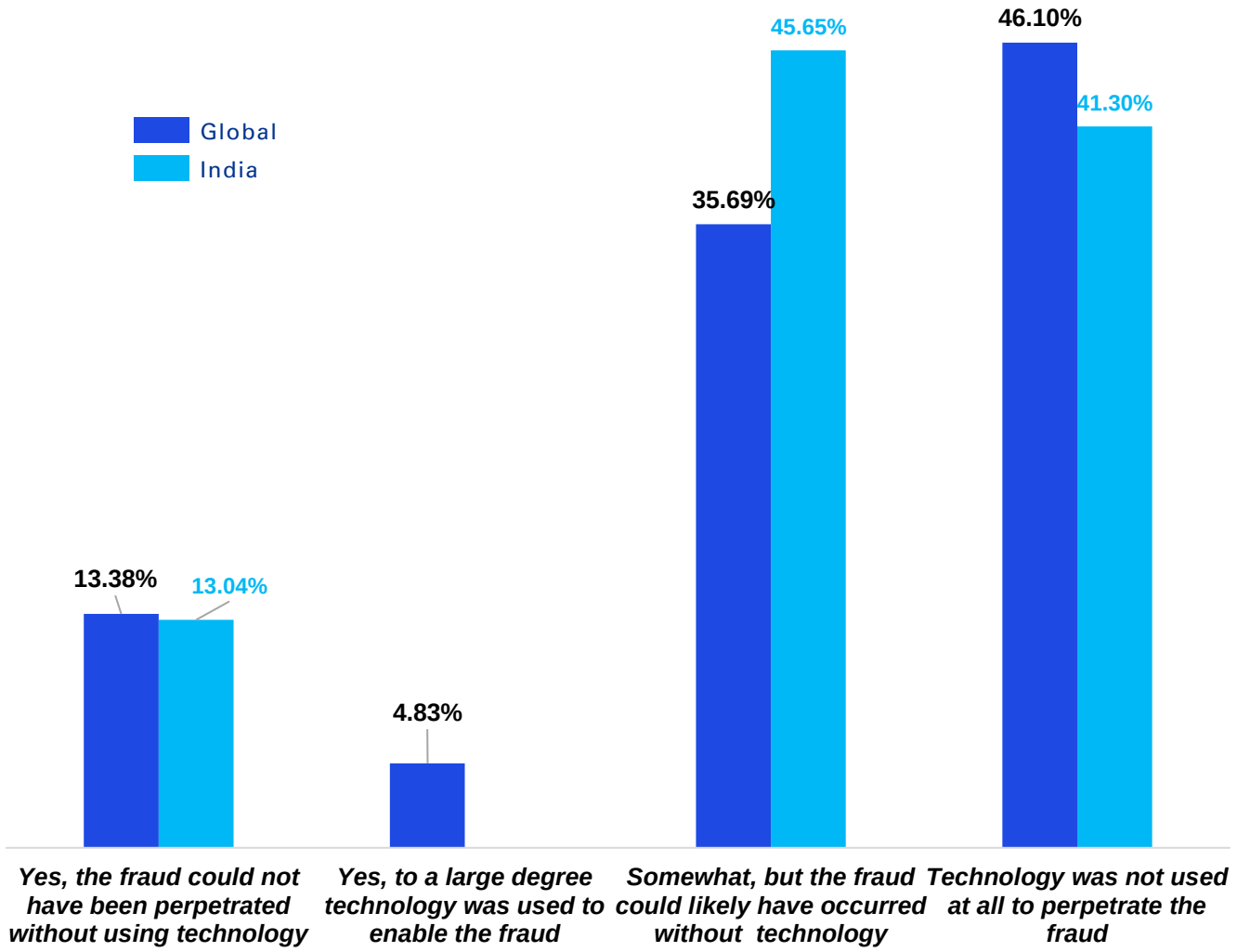
These insights have practical implications for organisations. In India, organisations might need to strengthen control at the operational layer, while globally more supervision is required at the leadership and governance level. Tailored strategies can help companies to stay ahead of the evolving fraud risks.

Did technology play a role in facilitating the fraud?

A look at how technology played a role in facilitating the fraud, whether through digital platforms, AI, cybersecurity lapses, or other technological means.

Insights from global survey and India highlights that **only a small portion (13 per cent) of the cases of fraud were such where technology was an integral factor**, without which the perpetrator would not have been able to commit the fraudulent act.

In majority of the cases considered technology was either not used at all or played only a limited role in facilitating the fraudulent acts.



Did technology play a role in facilitating the fraud?

The nature of fraud is evolving, with cyber threats becoming more sophisticated. Globally, only a very small proportion (5 per cent) of the frauds were defined as "cyber", centered around phishing, CEO fraud or business email compromise, hacking and malware/ransomware. The main aim is to steal data, disrupt services, or extort money. These crimes are usually carried out by technically skilled individuals or groups.

Artificial intelligence and cryptocurrency are emerging tools in fraud. While their current use is limited, they are expected to play a larger role in future scams. Deepfakes, for instance, may be used to impersonate senior figures and authorise fake transactions.

In India, the role of technology in fraud appears less prominent. Just 13.04 per cent of respondents believe fraud could not have occurred without it. A significant 41.30 per cent said technology had no impact at all, despite the prevalence of technology, many frauds are still committed using traditional methods. This suggests that, while technology can aid in detection, fundamental controls remain essential.

Interestingly, the average age of tech-enabled fraudsters is rising, reflecting the greater confidence of all generations in using technology. The majority of these frauds were carried out by staff members, rather than management. However, for those frauds where technology was used, but not considered essential, the perpetrators were more likely to be more senior, management-level employees.

Despite the rise of digital tools, strong internal controls remain essential. Fraud detection is still largely driven by data analytics, management reviews, and employee vigilance. Organisations must continue to invest in both technology and awareness to stay ahead of evolving threats.

Key takeaways

Our survey results highlight several areas where organisations can reduce their vulnerability to white-collar crime, by considering the following actions:

1

Strengthen internal controls

- Introduce and enforce robust internal controls, including regular audits and monitoring systems
- Establish clear limits on authority and aim to ensure consistent oversight, regardless of an individual's seniority or reputation

2

Promote an ethical culture

- Encourage a "speak-up" culture where employees feel safe to report suspicious activities through formal whistleblowing channels
- Provide regular training on ethical behavior and fraud awareness to all employees

3

Enhance detection mechanisms

- Use advanced data analytics and fraud detection technologies to proactively identify and investigate suspicious activities
- Regularly review and update fraud detection and prevention strategies to address emerging threats and vulnerabilities

4

Foster collaboration and transparency

- Promote transparency and collaboration across departments to help reduce opportunities for collusion
- Conduct thorough background checks, and continuously monitor employees in sensitive positions

5

Know your counterparty

- Undertake due diligence on third parties to understand who you are doing business with
- Periodically check in with higher-risk/higher-spend/spike-in-spend third parties to confirm that they actually exist, and assess their business justification and the legitimacy of the expenditure

6

Adapt to technological changes

- Stay informed about the latest technological advancements and their potential impact on fraud
- Invest in cybersecurity measures and train employees to recognise and respond to cyber threats

How KPMG in India can help

Today's businesses are increasingly vulnerable to fraud and face heightened regulatory and stakeholder expectations over corporate compliance. Acting quickly and decisively to help prevent, detect and respond to fraud and misconduct concerns is essential to help minimise disruption and loss, and to protect the bottom line. Companies need to gain a clear picture of their risks, internal control weaknesses, and policies for monitoring, identifying, reporting, escalating and addressing fraud. When organisations are victims of fraud, it's also vital to carry out thorough investigations and pursue perpetrators effectively.

Some of the world's largest organisations rely on KPMG professionals for global reach, technologies, industry acumen, local insights, and deep experience in navigating board, shareholder, auditor and regulator concerns. To help clients achieve leading investigative outcomes, we draw on our understanding of the regulators' expectations and latest trends.

KPMG's offerings include:

- Internal investigations into a wide spectrum of employee misconduct
- Financial reporting and earnings management fraud, embezzlement and misappropriation
- Regulatory assessments, anti-bribery/corruption reviews and conduct assessments
- Forensic technology services, including evidence collection, e-discovery and forensic data analytics
- Risk and vulnerability assessments, ethics and compliance advisory
- Anti-financial crime, sanctions, AML compliance and usage of Ethical AI
- Third-party due diligence and risk management
- Employee background screening
- Whistle-blowing reporting and helpline solution

About the survey

The survey is based on a questionnaire asking KPMG Forensic around the world for details about the fraudsters. The professionals filled in a detailed questionnaire on each fraudster, after investigating the case at the request of the organisation affected. The investigation frequently involved interviewing the fraudster, helping KPMG to form a detailed picture of the perpetrator and the fraud committed. This report is based on an analysis of 256 fraud cases investigated by KPMG member firms over the past 5 years. As some cases involve more than one fraudster, based on the survey responses, at least 669 fraudsters are covered.

KPMG in India contacts:

Akhilesh Tuteja
Partner and Head
Client and Markets
E: atuteja@kpmg.com

Manoj Kumar Vijai
Office Managing Partner - Mumbai
Head - Risk Advisory
E: mkumar@kpmg.com

Rajosik Banerjee
Deputy Head – Risk Advisory
Head – Financial Risk Management
E: rajosik@kpmg.com

Suveer Khanna
Partner and Head
Forensic Services
E: skhanna@kpmg.com

Maneesha Garg
Partner and Head
Managed Services
E: maneesha@kpmg.com

kpmg.com/in

Access our latest insights on KPMG Insights Edge

Follow us on:

kpmg.com/in/socialmedia

KPMG Assurance and Consulting Services LLP, Lodha Excelus, Apollo Mills Compound, NM Joshi Marg, Mahalaxmi, Mumbai-400 011 Phone: +91 22 3989 6000, Fax: +91 22 3983 6000.