Global profiles of the fraudster

The enemy within — profiling the corporate fraudster

KPMG. Make the Difference.

Contents

Introduction

Corporate fraud, often referred to as “white collar” crime, is a persistent and damaging problem that continues to make headlines and impact organizations worldwide. During my time with KPMG forensic services, I have witnessed firsthand the profound effects that fraud can have on companies, their employees, and society at large. The question that remains at the forefront of these efforts is: how can organizations better protect themselves against fraud, make it more difficult to commit, and detect it earlier?

To delve deeper into these critical challenges, KPMG conducted a wide-ranging global survey to uncover the profile of the typical fraudster, understand their methods, and identify the organizational weaknesses they exploit.

As organizations navigate the complexities of corporate fraud, they need to take proactive steps to strengthen their defenses. This includes implementing robust internal controls, promoting an ethical culture, enhancing detection mechanisms and technologies, fostering collaboration and transparency, and adapting to technological changes. At KPMG, we are dedicated to helping clients address these challenges and achieve the best possible outcomes in their fight against fraud.

I invite you to explore the findings of our survey and consider the recommendations provided in this report. Together, we can work towards creating a more secure and trustworthy corporate environment.

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

Who are the fraudsters? What are their methods? And how can organizations better protect themselves?

KPMG’s global fraud survey: Key findings

The typical fraudster is male, **36–55, highly respected,** and long-serving

The most common type of fraud is misappropriation of assets — notably **embezzlement and procurement**

Fraud occurs across a range of departments, including Operations, Finance, the CEO’s office, and Procurement

Weak controls are considered the prime reason for the frauds

The number one detection method is tip-offs via **whistleblowers or informal sources**

Fifty-five percent of frauds involved collaboration — typically with a **group of 2–5 people**

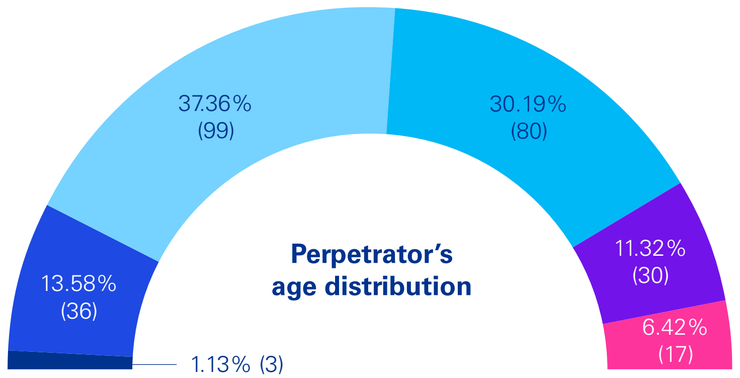
Profile of the fraudsters

"The typical fraudster is often someone you wouldn't suspect — highly respected, long-serving, and seemingly loyal. This highlights the importance of vigilance and robust internal controls."

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

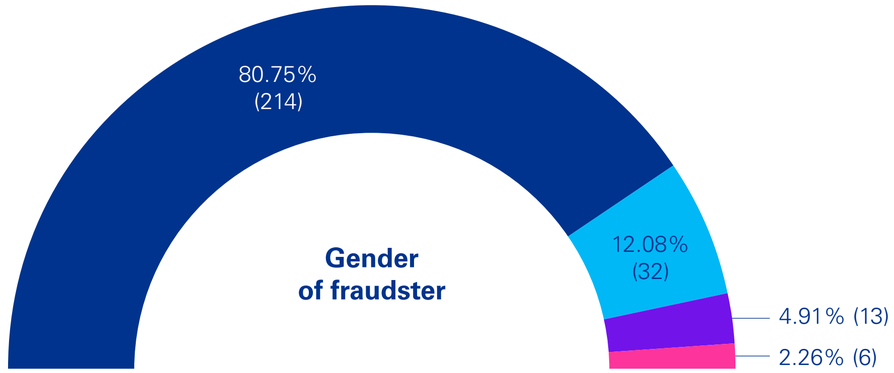
Clearly no two criminals are exactly alike, but our survey reveals some common traits. The typical fraudsters in our survey are males between 36 and 55 years old, and reasonably long-serving, having worked for the victim organization for more than 6 years. Seniority was fairly evenly split between executives (31 percent), management (30 percent) and staff (24 percent). And just over half (51 percent) 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 characterized by a sense of superiority. Interestingly, they didn't show signs of having an obvious grievance against their employer.



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

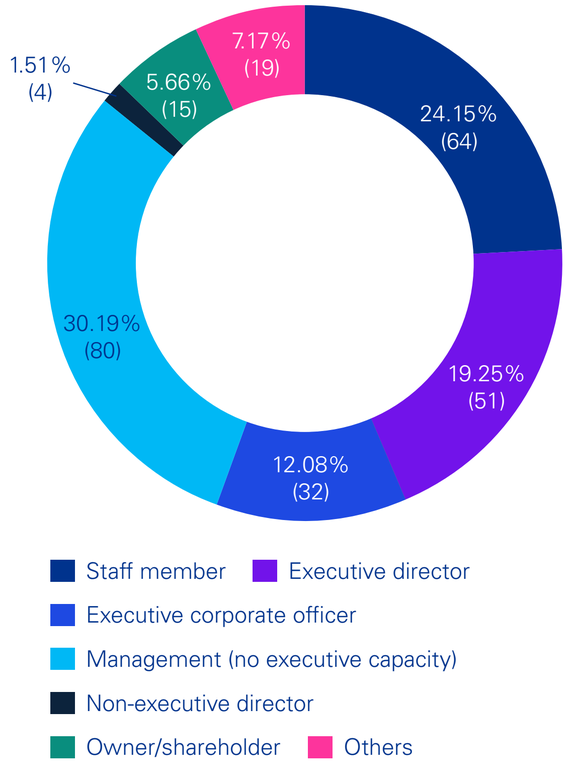
Source: Global profiles of the fraudster, 2025



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

Source: Global profiles of the fraudster, 2025

Neither did they appear to be struggling in their personal or professional lives. A relatively small proportion carried out the fraud to overcome a personal financial difficulty, or to enhance or protect their corporate reputation by hiding losses or meeting targets. The predominant motivation behind the crime was simple financial gain and greed, followed by opportunism.

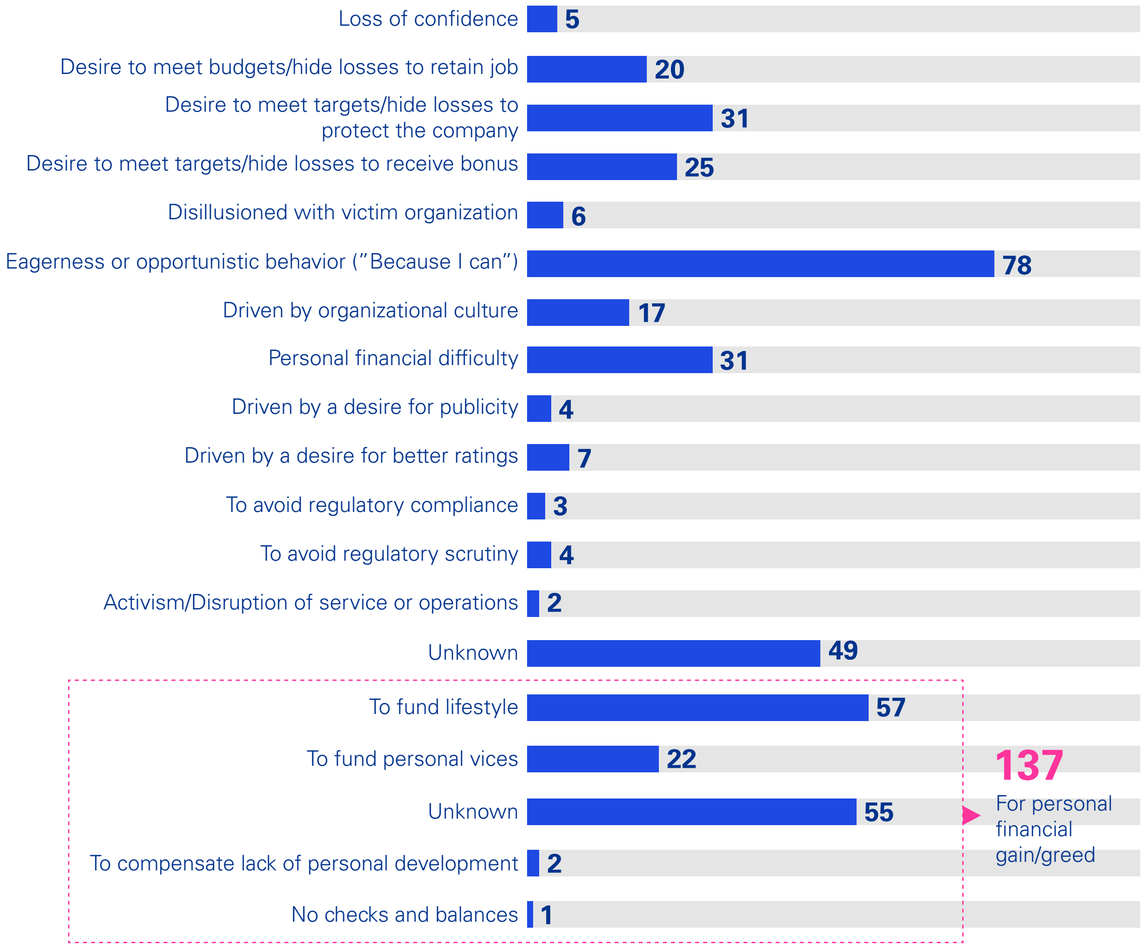


Source: Global profiles of the fraudster, 2025

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

Motivation of the perpetrator

What was the overriding motivation for the perpetrator?



Source: Global profiles of the fraudster, 2025

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

Years of service

3.40% (9)

18.49% (49)

13.21% (35)

64.91% (172)

- Less than 1 year
- 1 to 4 years
- 4 to 6 years
- More than 6 years

Source: Global profiles of the fraudster, 2025

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

The nature of the fraud — and where it happened

"Misappropriation of assets remains the most common type of fraud, emphasizing the need for stringent asset management and procurement controls."

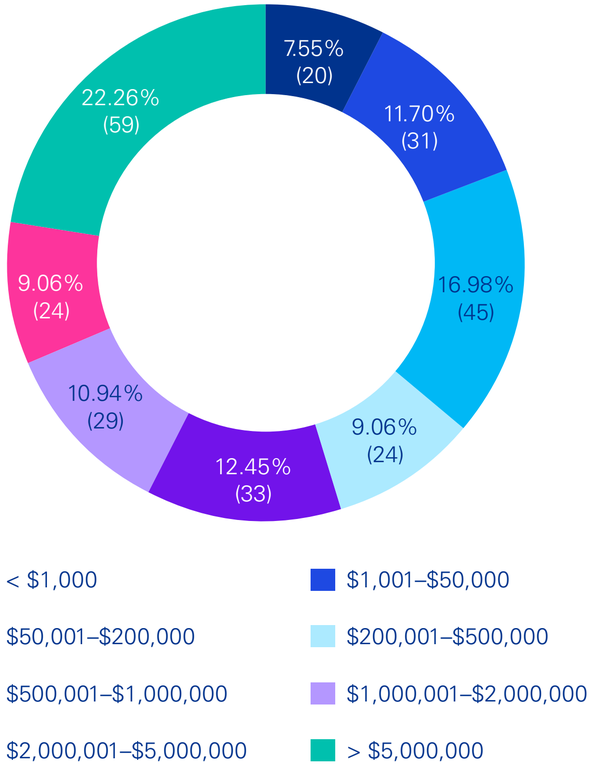
Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

With a few exceptions, most of the frauds studied (78 percent) were below US$200,000. Ten percent ranged from US$200,000 to US$1 million, and 8 percent were between US$1 million and US$5 million. The remaining frauds were all more than US$5 million. Just 13 percent involved cross-border crime, but these tended to be higher-value fraud — almost half incurring damages of US$5 million or more.

The single most common type of fraud in our survey was misappropriation of assets, representing 52 percent of all the reported cases, followed by falsified documentation (29 percent) — which may also enable misappropriation. Other frauds include theft of assets (24 percent).

Half (50 percent) of all the misappropriation cases were embezzlement — where individuals in trusted positions unlawfully use assets entrusted to them for personal gain — and 38 percent were procurement fraud. In the latter, the fraudster may collude with a vendor to create falsely high prices, and in return receive a portion of the increased revenues.

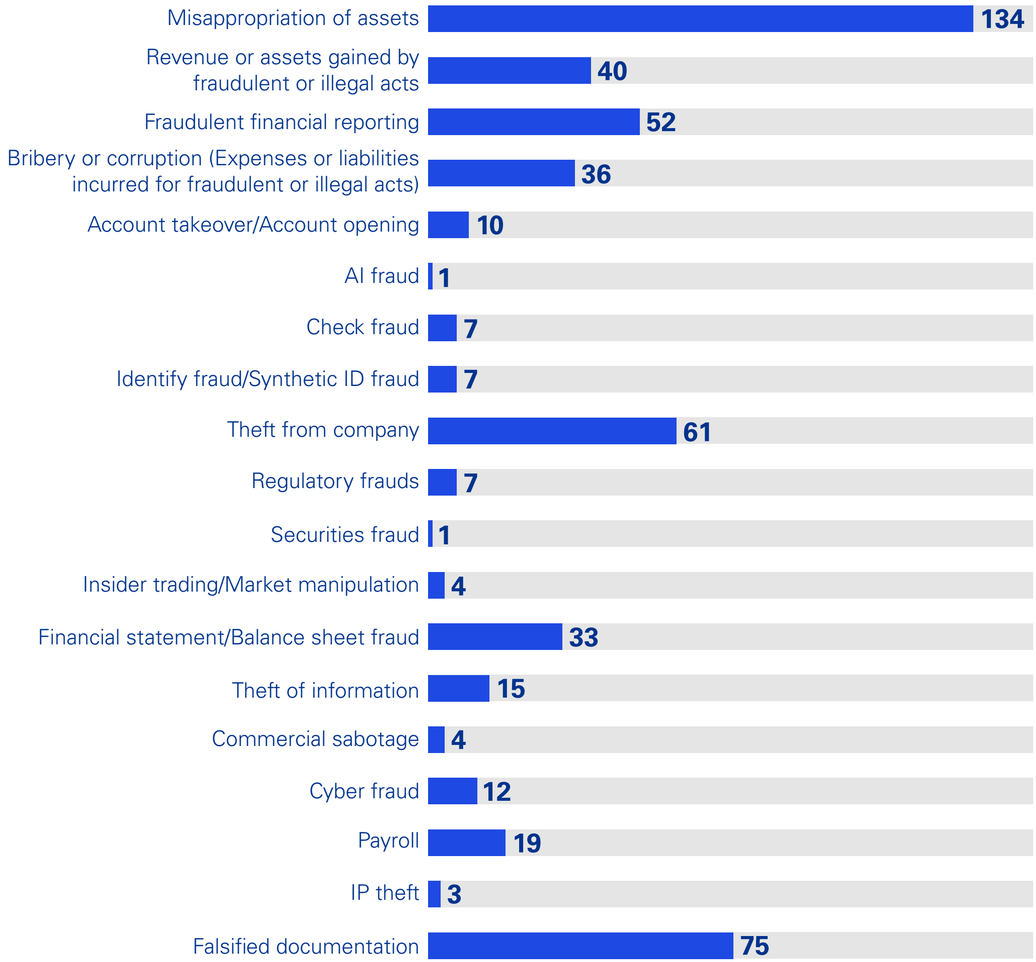
Just **13 percent** involved cross-border crime, but these tended to be higher-value fraud — almost half incurring damages of **US$5 million** or more.



Source: Global profiles of the fraudster, 2025

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.

What kind of fraud was committed?

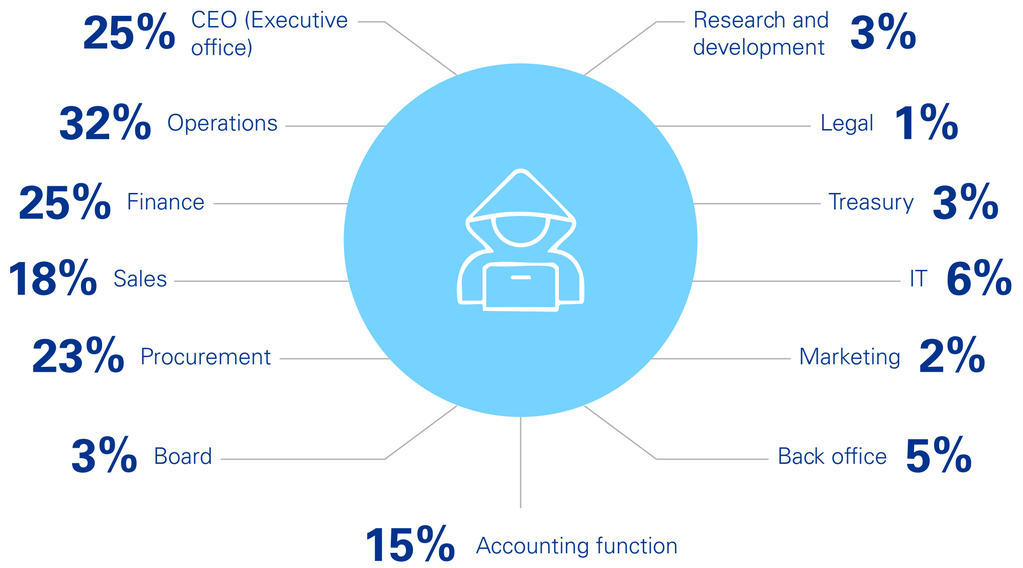


Source: Global profiles of the fraudster, 2025

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

One-fifth (20 percent) of the fraud cases involved fraudulent financial reporting. And a significant proportion (56 percent) of these involved improper revenue recognition, where financial statements used fictitious or premature revenue recognition to enhance earnings.

Frauds occurred across a range of departments, most notably Operations (32 percent), Finance (25 percent), the CEO's office (25 percent) and Procurement (23 percent). Although 34 percent of all misappropriation incidences happened within the CEO's department, this did not necessarily mean that the CEO or executive management themselves were the perpetrators. Within this part of the organization, opportunities for fraud are potentially greater, due to the higher authority.



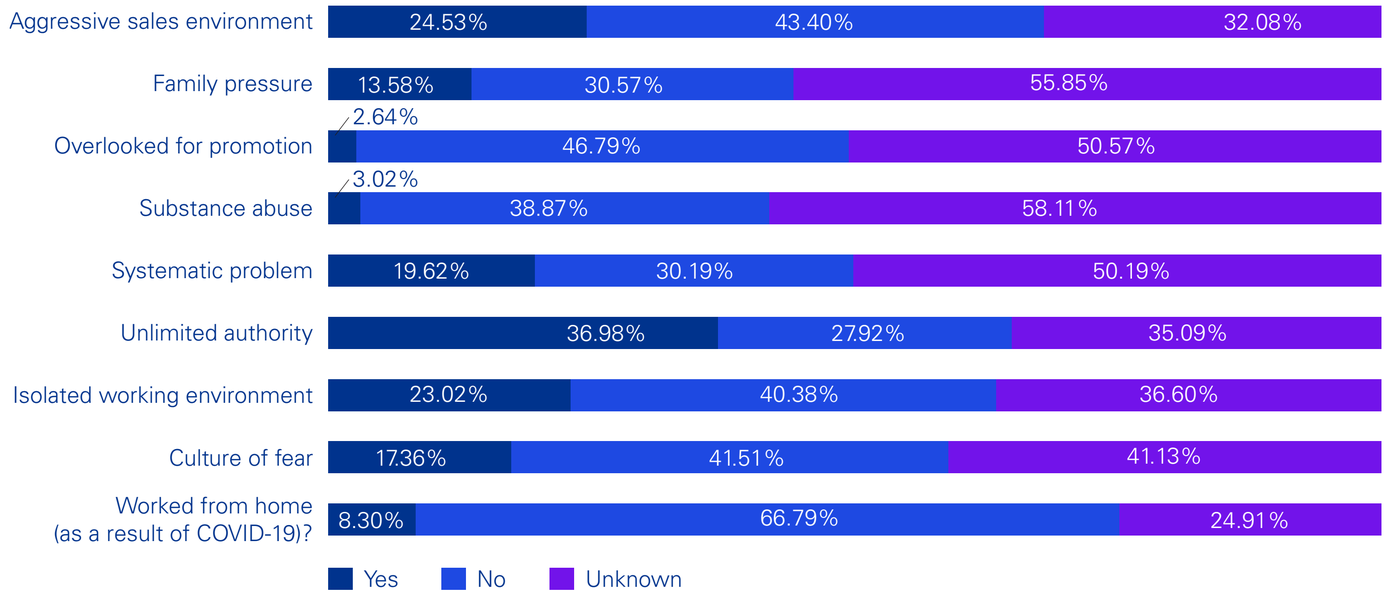
Source: Global profiles of the fraudster, 2025

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

Exposing systemic vulnerabilities

"Weak controls are a significant enabler of fraud. Organizations should prioritize strengthening their internal control systems to mitigate risks."

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany



Source: Global profiles of the fraudster, 2025

A review of the various environmental factors that shaped the perpetrator's context, such as aggressive work culture, family pressure, substance abuse, or a culture of fear, which may have contributed to fraudulent actions.

Internal controls are a key element in preventing and spotting fraud. In three-quarters (76 percent) of the cases studied, weak controls were considered the prime reason for the fraud. This represents a significant increase over our previous fraudster survey, where 61 percent cited poor controls as the cause. Indeed, 51 percent of the victim organizations had no anti-fraud controls in place when the fraud was committed. For those organizations that did have controls, the most common preventative controls were code of conduct (81 percent), internal audit (64 percent) and whistleblowing (60 percent).

Given the relative lack of effective defenses, it's little surprise that the number one method of detection was tip-offs (45 percent), either via a formal whistleblowing hotline or an anonymous, informal source. This demonstrates the importance of encouraging an ethical, "speak-up" corporate culture, along with prompt and effective handling of the incoming information. However, the fact that so many frauds remain undetected by preventive controls indicates a need for enhanced internal monitoring systems, to achieve earlier detection and minimize the damage caused.

Interestingly, "unlimited authority" was the top environmental factor associated with fraudsters. In half (49 percent) of such cases, the value of the fraud exceeded US$1 million. The greater the fraud value, the more likely the fraudster was to have unlimited authority. Twenty-nine percent of all frauds over US$5 million were associated with unlimited authority whereas for frauds between US$1–2 million, and US$2–5 million, unlimited authority played a role in 9 percent and 11 percent of cases respectively.

Conversely, only a small proportion of perpetrators with limited authority (12 percent) incurred damages over US$1 million. 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.

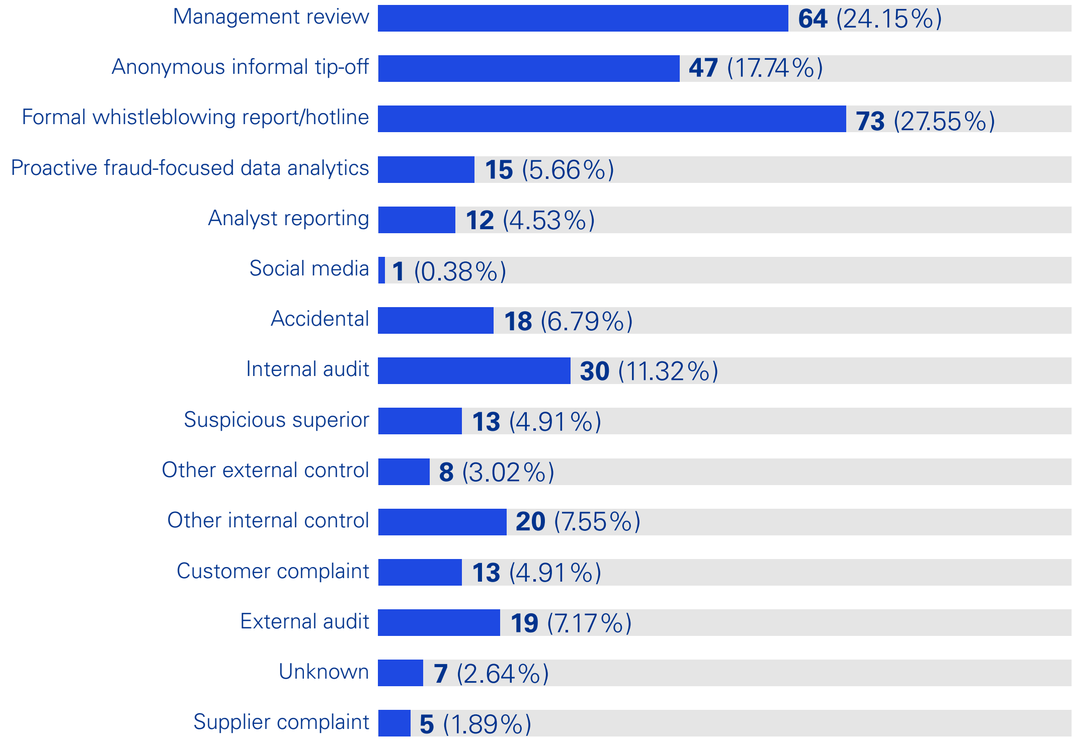
The shift to remote work has had a negligible impact

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

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

Given that fraud and subsequent investigations can happen over a period of years, our survey also looked at the large-scale shift to remote working that accelerated during the COVID-19 pandemic. Remote working "played a part" in just 5 percent of the frauds investigated, and in only 9 percent of cases was the victim organization's lack of control or supervision "compromised somewhat", due to remote working. There are certainly lessons to be learned from the victim organizations, such as falsified e-documents that were not scrutinized sufficiently, fake subcontractors claiming to work remotely, and candidates for new positions interviewed by video without a panel of interviewees.

What means lead to the detection of the fraud?



Source: Global profiles of the fraudster, 2025

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

Unlimited authority

36.98% (98)

27.92% (74)

35.09% (93)

Yes
No
Unknown

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

Understanding the collaborators

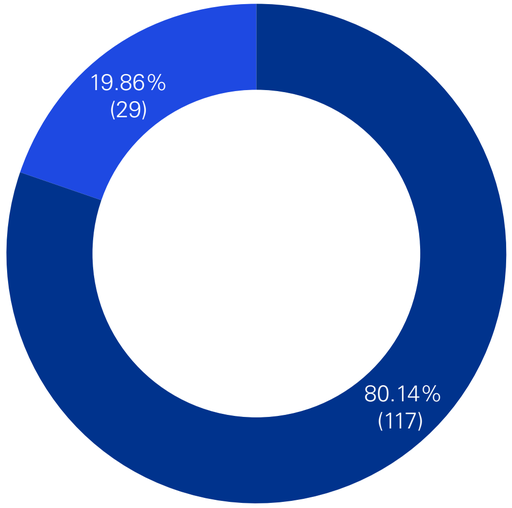
"Collaboration among fraudsters is common, so organizations should foster transparency and closely monitor interactions — particularly with high-risk third parties."

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

Although 55 percent of the fraudsters colluded with others, this proportion has fallen by 7 percent since our previous survey — possibly because technology presents more opportunities to act alone. Fraudsters that colluded with others were more likely to work for a multinational organization, where opportunities to find like-minded individuals are arguably greater, due to the size of the organization. Within the collaboration, the principal actor was invariably the employee rather than an external person(s).

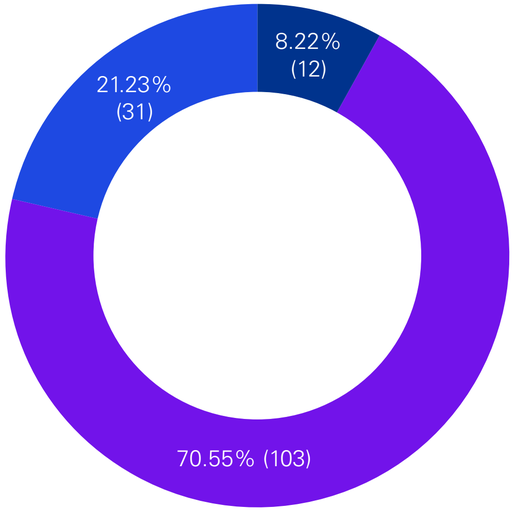
A majority (71 percent) collaborated with a group of between two and five others. And, in most cases, some or all of the collaborators were other employees of the organization, with 39 percent of the collaborations purely internal. Even though most of the principal fraudsters were male, about half (52 percent) of fraud cases where there was collaboration involved females.

When it comes to uncovering the identities of collaborators, the most successful methods were investigating emails, oral evidence from interviews with the fraudsters, and analysis of financial records.



Agent Principal

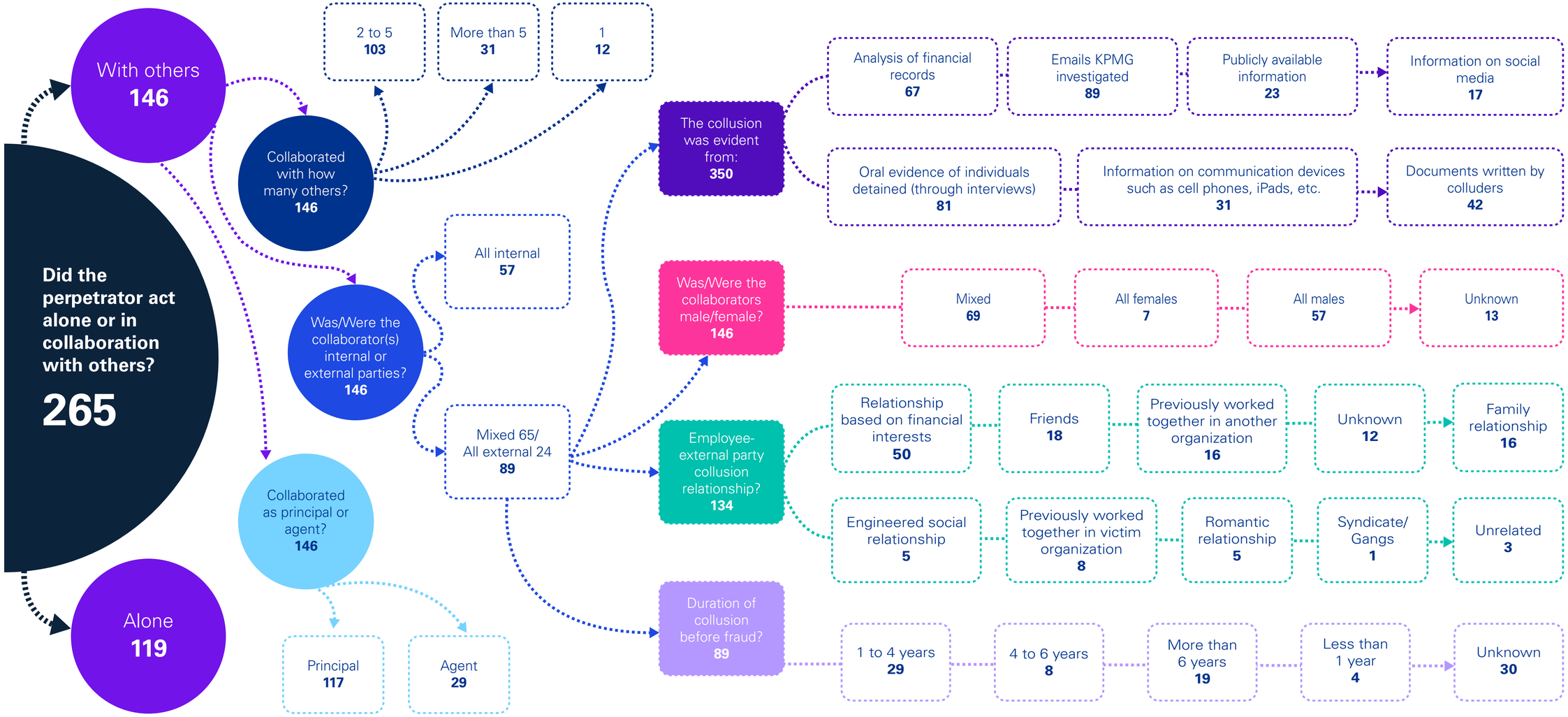
An investigation into whether the fraud collaborator acted as a principal (main actor) or an agent (a subordinate or intermediary), shedding light on the nature of the collaboration.



1 2 to 5
More than 5

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.

Source: Global profiles of the fraudster, 2025



Source: Global profiles of the fraudster, 2025

An analysis of how fraud perpetrators collaborated with others, detailing their roles (e.g. principal or agent), the number of collaborators, and the nature of their relationships (internal or external parties).

Cyber fraud

"The rise of AI and cryptocurrency in fraud highlights the evolving nature of threats. Continuous adaptation and vigilance are key to combating these risks."

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

Only a very small proportion (5 percent) of the frauds in our survey were defined as "cyber", centered around phishing, CEO fraud or business email compromise, hacking and malware/ransomware. The main objectives of cyberattacks were acquiring personal data, disrupting services, extortion, and identity theft. Unsurprisingly, the fraudster teams consisted primarily of technical hackers.

Artificial intelligence (AI) is expected to become a bigger factor in cybercrime, not least through the growing use of "deepfakes" to impersonate individuals with authority to sanction transactions. However, due to the recency of AI, a mere handful of all the frauds in the survey involved AI — and it's a similar story with cryptocurrency. However, we expect this picture to change in the future.

Compared to other types of fraud, cyberfraud was more likely to be detected by fraud-focused data analytics, management review and other internal controls. These findings suggest that internal cyber controls may be working relatively efficiently, and that organizational employees are aware of and actively trying to minimize cyberthreats. Alternatively, there may be a significant number of undetected cases of cyber fraud occurring as a result of inadequate controls.

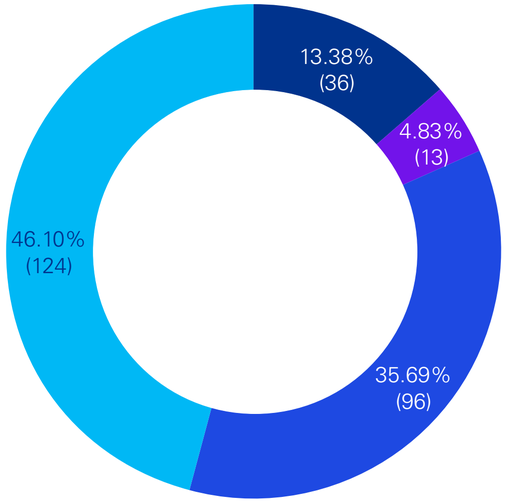
Technology is not yet a critical factor in fraud

"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."

Alexander Geschonneck
Global Forensic Leader
KPMG in Germany

Despite the ubiquitous role of smartphones, laptops and apps in our lives, the frauds investigated in this survey do not appear to have been heavily influenced by technology. Almost half (46 percent) of frauds were perpetrated without any use of technology, and a further 35 percent used technology "somewhat" but could likely have occurred without any use. Compared to the previous KPMG fraudster survey, technology-enabled fraud has not risen. The reasons for these results are unclear, but may be due to the fact that technology is more traceable than traditional, manual methods — and also enables organizations to strengthen their defenses.

Another interesting observation is that the age of those carrying out technology-enabled fraud has, on average, risen since our last survey, 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.



- Yes, the fraud could not have been perpetrated without using technology
- Yes, to a large degree technology was used to enable the fraud
- Somewhat, but the fraud could likely have occurred without technology
- Technology was not used at all to perpetrate the fraud

Source: Global profiles of the fraudster, 2025

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

Key takeaways

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

Strengthen internal controls

1

- 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

Promote an ethical culture

2

- 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

Enhance detection mechanisms

3

- 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

Foster collaboration and transparency

4

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

Know your counterparty

5

- 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

Adapt to technological changes

6

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

How KPMG 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 minimize 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 organizations are victims of fraud, it's also vital to carry out thorough investigations and pursue perpetrators effectively.

Some of the world's largest organizations 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 firms' services include:

- **Internal investigations into a wide spectrum of employee misconduct**
- **Financial reporting and earnings management fraud, embezzlement and misappropriation**
- **Regulatory, anti-bribery and corruption concerns**
- **Forensic technology services, including evidence collection, e-discovery and forensic data analytics**
- **Risk and vulnerability assessments**
- **Anti-financial crime, sanctions, and AML compliance**
- **Ethics and compliance advisory**
- **Third-party risk management**

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 organization 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.

Your contacts in Switzerland

Bob Dillen
Partner,
Head of Forensic

T: +41 58 249 31 11
E: bdillen@kpmg.com

Eric Blot
Partner,
Forensic Western Switzerland

T: +41 58 249 37 24
E: eblot@kpmg.com

KPMG AG
Badenerstrasse 172
PO Box
8036 Zurich

kpmg.ch/forensic

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.