Fraud Barometer 2025 of the Netherlands



KPMG The Netherlands

—

October 2026

KPMG. Make the Difference.

From conviction patterns to targeted action

What the 2025 Fraud Barometer insights mean for fraud, integrity and compliance priorities in 2026

The KPMG Fraud Barometer provides a unique perspective on white-collar crime in the Netherlands by analyzing media-reported cases that resulted in a Dutch court ruling or settlement in 2025. Fraudulent reporting and misappropriation account for the largest share of convictions, while perpetrators range from external individuals and employees to organized criminal groups. The findings demonstrate that financial crime affects a broad range of stakeholders, including businesses, government institutions and society as a whole.

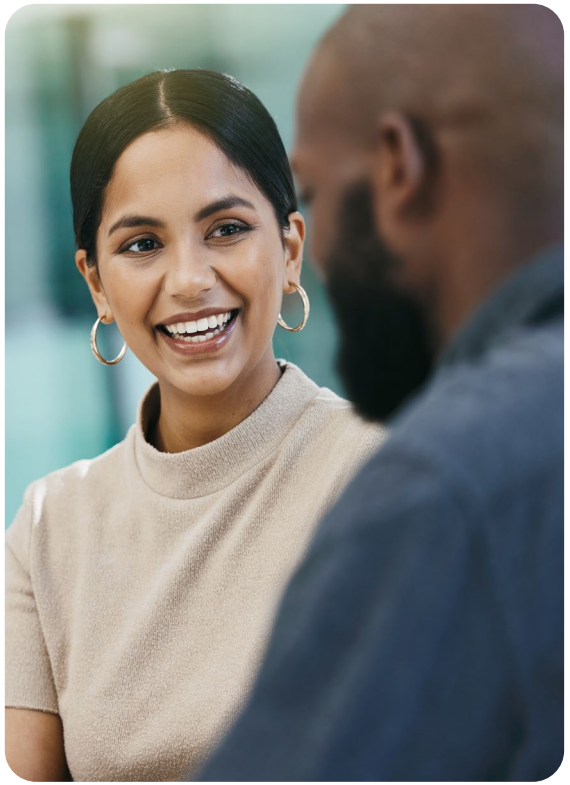
The insider challenge

While external individuals account for the largest share of convicted perpetrators, the findings reveal that a significant proportion of cases involve employees and individuals operating from positions of trust. This highlights that organizations are not only exposed to threats from outside actors, but also risks emerging from within their own operations.

Employees often have access to sensitive information, systems and financial resources, creating opportunities to commit or facilitate misconduct. As a result, organizations should complement external fraud prevention measures with controls that address insider risks, including segregation of duties, monitoring activities and effective oversight. At the same time, fostering a strong culture of integrity and encouraging employees to speak up when concerns arise can help organizations identify and address risks at an early stage.

A connected response

The diversity of offenses, perpetrators and victim groups demonstrates that financial crime risks rarely exist in isolation.



Fraud, integrity violations and money laundering risks often overlap, while the same individuals, networks or control weaknesses can give rise to multiple forms of misconduct. Treating these risks as separate challenges may leave organizations vulnerable to blind spots and fragmented responses.

A more integrated approach can help organizations build greater resilience. By aligning governance, risk management, internal controls, investigations and speak-up mechanisms, organizations can develop a more complete view of their risk landscape. This not only strengthens oversight but also enables earlier detection of emerging threats and more coordinated responses across the organization.

Looking forward

As organizations continue to digitalize their operations and adopt AI-enabled technologies, fraud schemes are likely to evolve alongside them, creating new challenges for prevention and detection efforts. At the same time, advances in data analytics and AI offer powerful opportunities to identify suspicious behavior earlier, strengthen fraud detection and enhance investigative effectiveness.



Leonie Stolk
Partner
Head of Forensic NL

“Financial crime rarely stays within a single risk domain.

Given the complexity of today’s risk landscape, leaders must move beyond managing fraud, integrity, and compliance risks in isolation and adopt an integrated approach to risk management.

Looking ahead, AI will not only create new risks and opportunities, but also reshape how organizations prevent, detect, and respond to financial crime.”

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Fraud Barometer 2025

Key insights

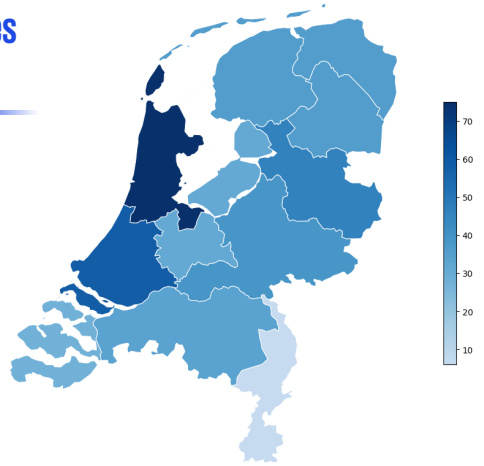
The white-collar crime landscape of the Netherlands in 2025

The KPMG Forensic Fraud Barometer only covers white-collar crimes that have resulted in convictions by Dutch courts in 2025

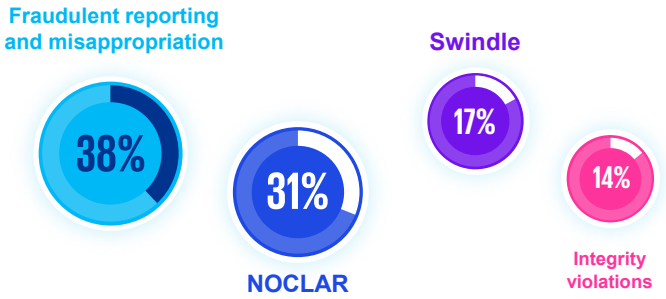
38%

of district court cases originate from the provinces of North and South Holland, representing the largest regional concentration of convicted cases.

Convicted cases by region



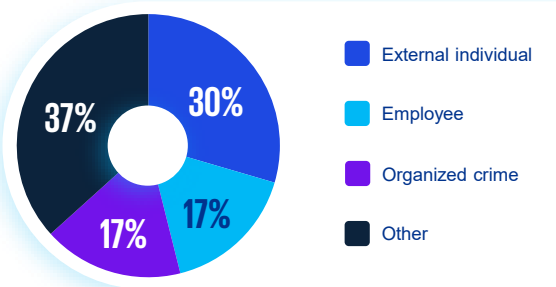
Distribution of convictions across domains



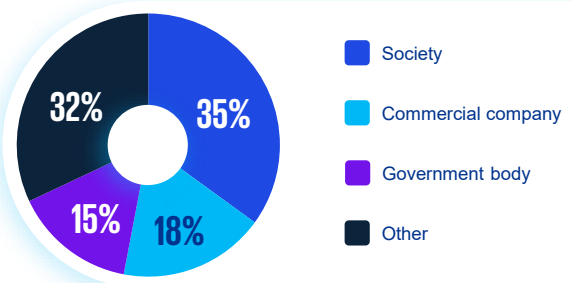
Most prevalent offense types among convictions



External individuals, employees and organized crime account for 64% of convicted individuals



Society, commercial companies and government bodies represent 68% of identified victims



n=447 | Due to rounding differences, percentages may not always add up to 100%. This applies to all subsequent charts and figures throughout this report.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Contents

01	The diversity of white-collar crime	05
02	A closer look at ‘fraudulent reporting and misappropriation’	09
03	A closer look at ‘NOCLAR’	11
04	A closer look at ‘swindle’	13
05	A closer look at ‘integrity violations’	15
06	From insights to action	17



© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The diversity of white-collar crime

Using Dutch media as its primary source, the Fraud Barometer provides a perspective on white-collar crime in the Netherlands. The Fraud Barometer exclusively covers cases that resulted in a formal court ruling or settlement issued by a Dutch court in 2025. By analyzing cases reported in the media, it offers a unique view of how financial and integrity-related crime manifests itself in practice and how they are addressed within the Dutch legal system.

The Fraud Barometer covers a broad spectrum of financial and integrity-related offenses, reflecting the types of misconduct we frequently encounter in our work. These include crimes such as embezzlement, money laundering, and financial statement fraud. We also included non-financial types of misconduct, such as workplace misconduct, conflicts of interest, and abuse of power, reflecting the diverse fraud risks and convictions observed in the Netherlands.

In 2025, KPMG Global published the *Global Profile of the Fraudster**, offering valuable insights into the profile of the typical defrauder. The Fraud Barometer adds on these insights by exploring the fraud landscape in the Netherlands, providing a complementary perspective on the types of fraud committed and the stakeholders involved.

Welcome to the Dutch Fraud Barometer 2025. The Fraud Barometer is an initiative of KPMG Forensic, a division of KPMG Advisory N.V. (hereafter referred to as 'KPMG').

In this publication, you will discover key insights into the fraud landscape in the Netherlands in 2025, including the prevalence of different fraud types, perpetrator and victim groups, and sentencing outcomes. In total, 31 distinct subtypes of integrity- and fraud-related crimes were identified within scope. Given the diversity of these offenses, they were grouped into four key domains:

Fraudulent reporting and misappropriation

Cases involving the misuse of entrusted assets, resources, or information for financial gain. This category includes offenses such as embezzlement, document falsification, tax fraud, and the manipulation of financial or administrative records.

Swindle

Cases involving deception or manipulation to obtain money, assets or other benefits from victims. This category includes a wide range of scam -related offenses, such as fraud through false pretenses, investment scams, online fraud, and cyber-enabled deception.

NOCLAR (Non-Compliance with Laws and Regulations)

Cases involving violations of legal or regulatory requirements, including money laundering, sanctions violations, bribery, corruption, and other compliance-related offenses. These cases often involve the concealment of illicit proceeds or failures to comply with statutory obligations.

Integrity violations

Cases involving conduct that undermines ethical standards, professional responsibilities, or organizational integrity. Examples include abuse of power, conflicts of interest, breaches of confidentiality, workplace misconduct, and other forms of inappropriate behavior.

The report provides an overview of current risks and patterns across these domains, with Chapters 2 to 5 offering a deeper analysis of each domain. In doing so, it sheds light on evolving risks and vulnerabilities faced by organizations, public institutions, and individuals. These insights can help stakeholders better understand how fraud is perpetrated, under which circumstances they face exposure to key risks, and what preventive measures may be needed.

If you would like to learn more about how this research was conducted, please feel free to contact us.

KPMG

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

* For more details, see the Global profiles of the fraudster

The diversity of white-collar crime

Distribution of convictions

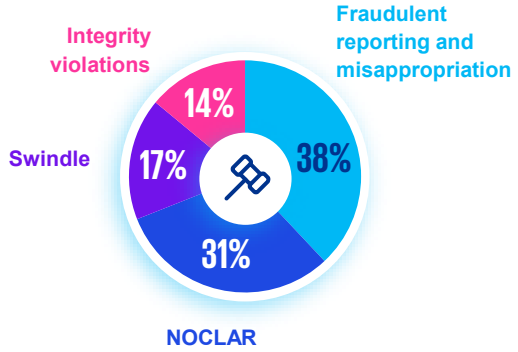
In total, 447 unique cases were identified in Dutch media, with each convicted individual considered a separate case. Consequently, a crime involving two convicted individuals is treated as two cases.

The distribution of convictions shows that **fraudulent reporting and misappropriation**-related offenses (38%) and **NOCLAR** schemes (31%) are the most frequently convicted white-collar crimes. While the former includes offenses such as document falsification and embezzlement, the latter covers crimes such as money laundering and other compliance violations. The prevalence of these offenses points to the continued importance of strong financial controls, effective transaction monitoring, and robust compliance frameworks.

At the same time, **swindle**-related offenses, including scams and cyber fraud, illustrate the need for effective cybersecurity, customer protection measures, and awareness of externally driven threats.

Integrity violations (e.g., abuse of power, inappropriate conduct) appear less frequently in court cases. Based on our experience, integrity violations are often handled internally rather than through legal proceedings. Preventing integrity-related incidents requires a strong organizational culture, clear governance, and effective speak-up mechanisms, which also help mitigate risks arising from internal actors.

Distribution of convictions across domains in the Netherlands



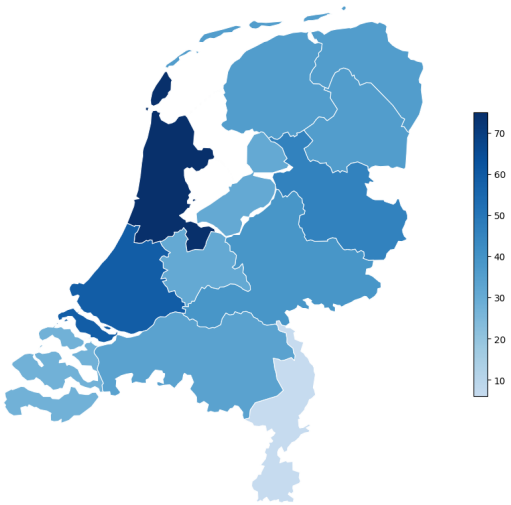
Geographical insights

Overall, the presence of all four domains highlights the importance for an integrated approach that combines financial, compliance, and integrity measures to effectively manage white-collar crime risks.

Based on the court location, we analyzed the geographical distribution of convictions*. **North Holland** and **South Holland** account for 38% of the total district court cases, reflecting the higher populated density and higher economic activity in these provinces. Within these provinces, the distribution of convictions across domains closely resembles the national picture.

In contrast, in the provinces of **Gelderland** and **Overijssel**, together accounting for 24% of convicted cases by district courts, the proportion of swindle-related schemes (24%) is significantly higher, while its share of NOCLAR convictions (23%) is lower.

Geographical distribution of convicted cases in the Netherlands



* The geographical distribution reflects only those cases convicted by Dutch district courts. It excludes cases handled by higher judicial instances, such as courts of appeal and the Supreme Court, as well as decisions originating from disciplinary bodies.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Perpetrators and victims

White-collar crime spans a wide range of perpetrators and an equally diverse victim base.

In terms of perpetrators, **external individuals** account for 30% of cases, positioning them as a key driver of white-collar crime. Nearly half of these cases are linked to money laundering (45%) and typically do not combine multiple convictions in scope. This may suggest that these individuals operate in more isolated roles, with potential links to organized crime networks that are not fully visible in this barometer or reflected in court rulings. They mostly target **society** or **commercial companies**.

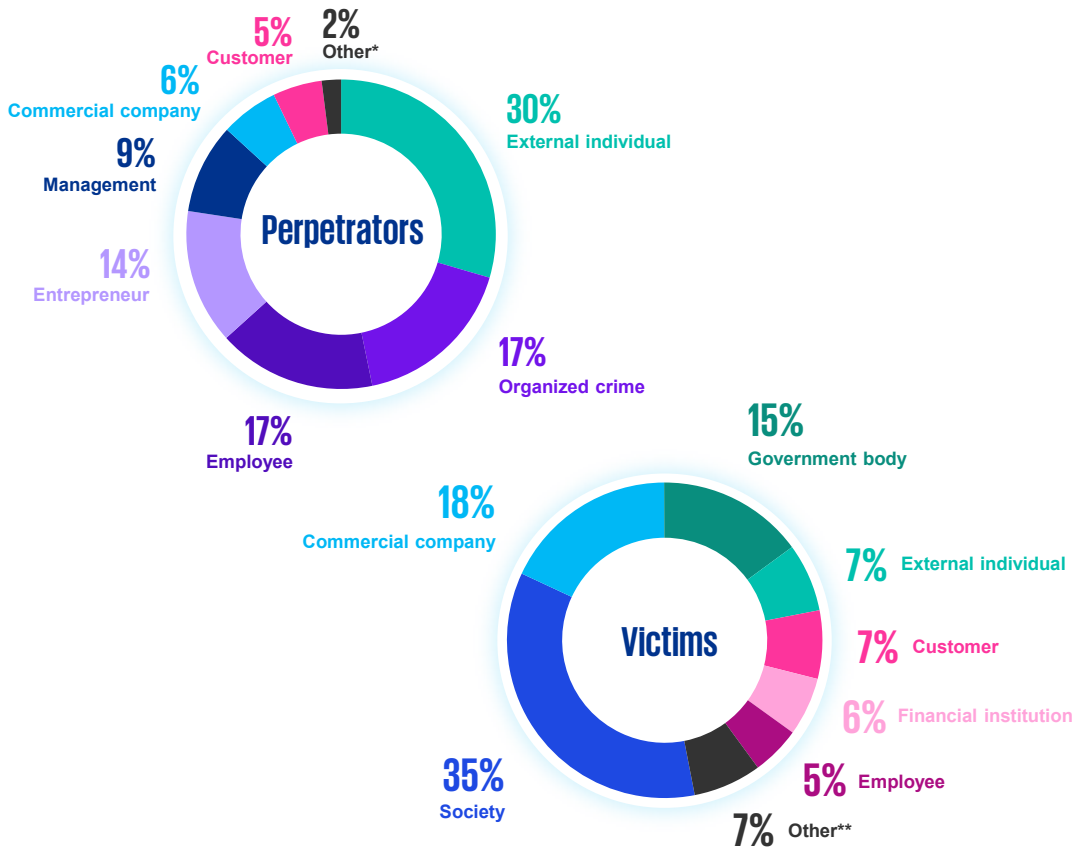
Organized crime represents 17% of offenders. This illustrates that a considerable portion of white-collar crime is not incidental, but rather structured and professionally coordinated. In practice, these perpetrators often tried to conceal the origins of funds derived from drugs or none fraud related crimes outside the scope of the barometer. In cases involving organized crime, **society** is typically identified as the primary victim, reflecting the broad and indirect impact of these offenses on the financial system and public trust.

Employees also account for 17% of perpetrators, highlighting that fraud risk is not only external, but also driven by insider risk within organizations. Employees are most commonly linked to embezzlement (25%), typically targeting their own organization (e.g., **commercial** and **non-commercial companies** and **government bodies**) and, in a small number of cases, its **customers**. A strong control environment with elements such as segregation of duties, and ongoing awareness initiatives therefore remains fundamental to reducing insider risk.

Entrepreneurs are the driver behind 14% of the cases. They are most frequently convicted for document falsification (28%) and, to a lesser degree, for money laundering, scams and tax fraud. **Government bodies** are the primary victims of these offenses, highlighting the exposure of public institutions to financial reporting and tax violations.

In line with KPMG's *Global Profile of the Fraudster**, these insights demonstrate that organizations face fraud risks from both internal and external actors. Managing these risks requires effective controls, continuous monitoring across different roles and access levels, and remaining attentive to the structured and coordinated nature of certain fraud schemes.

Distribution of perpetrators and victims of white-collar crime



* 'Other' includes the following perpetrator types: financial institution (0.9%), government body (0.7%), and non-commercial organization (0.4%).
** 'Other' includes the following victim types: entrepreneur (2.9%), non-commercial organization (2.6%), and management (1.2%).

* For more details, see the Global profiles of the fraudster

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Sentencing

The sentencing patterns reinforce the seriousness with which financial and integrity-related offenses are treated.

Financial sanctions, comprising fines, compensations and confiscations, continue to represent a significant component in these cases. The total value of these financial measures differs notably across offense types, both in absolute terms and relative to the number of cases. While the amounts include efforts to recover or compensate crime-related losses, they exclude unrecovered losses and non-monetary confiscated assets and should therefore not be interpreted as a direct reflection of the total underlying losses.

Fraudulent reporting and misappropriation cases account for the largest share of total financial sanctions, reaching approximately EUR 210 million. This aligns with this domain representing the largest proportion of cases (38%). While the total amount is partly driven by the high volume of cases, the financial impact per case also remains significant compared to several other offense domains. The combination of high case volumes and substantial financial sanctions demonstrates that traditional fraud schemes continue to pose a significant risk to organizations.

Swindle cases, while representing a smaller share of total cases (17%), show a relatively high aggregate financial impact of approximately EUR 109 million. This suggests that individual swindle cases often involve substantial financial damage, which can result in significant losses per incident. External fraud risks, including scams, impersonation, and computer fraud, therefore remain a material concern for organizations.

In contrast, **NOCLAR** cases account for 31% of all cases but result in a significantly lower total value of financial sanctions, at approximately EUR 32 million*. This indicates that, despite their frequency, financial compensations in these cases remain relatively limited. At the same time, money laundering cases are more frequently associated with (higher) prison sentences (48%), reflecting the severity with which these offenses are addressed through non-financial sanctions. Organizations subject to Anti Money Laundering (AML) regulations continue to face significant regulatory and enforcement risks, as non-compliance may not only lead to financial penalties but also severe legal consequences for individuals involved. This places continued emphasis on effective client due diligence, transaction monitoring and a timely escalation of suspicious activities.

Integrity violations, representing 14% of cases, show the lowest aggregate financial sanctions at approximately EUR 22 million. This may be attributable to the nature of these cases, as they do not always translate into large quantifiable financial damages. However, for organizations, integrity breaches often carry significant reputational impacts that can trigger regulatory scrutiny as well as high internal investigation or remediation costs. Organizations therefore benefit from fostering a strong ethical culture supported by clear policies and accessible reporting channels.

Overall, the data shows that both the frequency of cases and the type and magnitude of sanctions differ significantly by offense domain. Organizations face varying levels of financial, regulatory, legal, and reputational risks across these offense domains, making a risk-based approach to fraud and compliance essential.

* The values are restricted to Dutch court cases and do not include international fines. The values reflect only those amounts reported in the media articles in scope and may therefore not capture all financial sanctions imposed.

Financial sanctions



© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A closer look at 'fraudulent reporting and misappropriation'

Fraudulent reporting and misappropriation convictions

We identified 186 unique cases with a conviction in the domain fraudulent reporting and misappropriation.

This domain covers a broad range of convictions, from document falsification and tax fraud to insolvency and benefits fraud. These crimes rarely occur in isolation. In 42% of cases, perpetrators were convicted of a combination of white-collar crimes. Most of these combinations span multiple domains, such as document falsification from the Fraudulent reporting and misappropriation domain paired with scams from the Swindle domain. The high proportion of multi-offense convictions suggests that white-collar crime is often perpetrated through interconnected schemes.

Document falsification is the clearest example of this interconnectedness. Representing 44% of the convictions, it is not only the most common offense but also often appears to play an enabling role in broader fraud schemes. The most common combinations link document falsification with scams, money laundering and embezzlement, illustrating how forged contracts, financial statements, and other documents may be used to both deceive stakeholders and to conceal illicit proceeds.

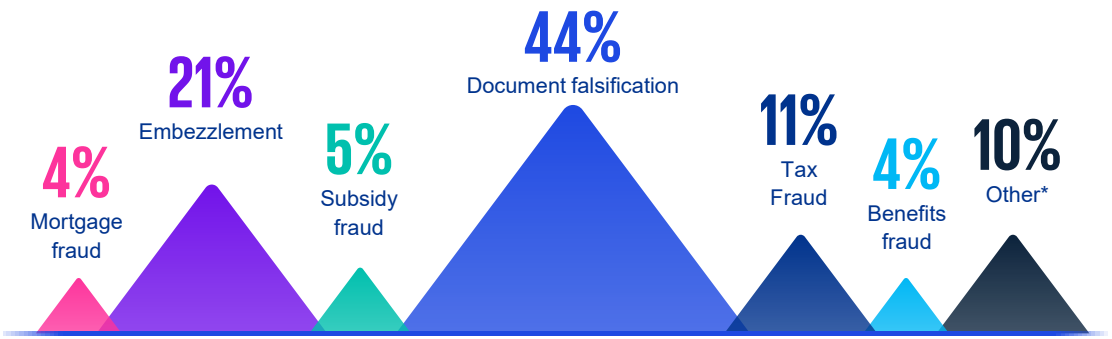
Continuous developments in AI are making forged documents increasingly difficult to detect, further emphasizing not only the need for effective controls and approval workflows, but also for the use of AI-enabled detection measures to identify increasingly sophisticated threats.

Embezzlement (21%), the second most prevalent conviction, also frequently appears alongside other offenses, particularly document falsification. Embezzlement is primarily an insider risk, often arising where someone has trusted access to funds or assets. Insufficient segregation of duties and limited oversight may create conditions in which embezzlement is more likely to occur.

In contrast, **tax fraud** (11%) is more commonly observed as a stand-alone offense. Tax fraud can give perpetrators an unfair competitive advantage, reduce public revenues and undermine trust in the economic system. It may arise where tax positions, transactions, or reporting are insufficiently challenged or reviewed.

These findings demonstrate the importance of looking beyond individual incidents and considering how different risks can interact and compound one another. If these risks are not adequately addressed, they may result in regulatory breaches, reputational damage, significant financial losses and weakened public and stakeholder trust. The findings also reinforce the value of integrated fraud risk management, as weaknesses in one area can create opportunities for broader and more complex schemes.

Distribution of fraudulent reporting and misappropriation convictions



* 'Other' includes the following subtypes: expense claim fraud (3.0%), insolvency fraud (3.0%), insurance fraud (2.2%), financial statement fraud (1.3%), and investment fraud (0.9%).

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The perpetrators

Across the 186 cases, the analysis shows that fraud can be committed by a diverse range of actors, and that the perpetrator profile shapes both the nature of the offense and the victim.

Entrepreneurs, which account for 25% of perpetrators, are most often linked to document falsification and tax fraud, targeting government bodies, commercial organizations and clients. This highlights that risks can arise both within organizations and through external business relationships, reinforcing the importance of effective controls over documentation and financial reporting, particularly where individuals have significant autonomy.

Employees (20%) and **management** (12%) are most frequently involved in embezzlement and document falsification. These offenses occur across government bodies, commercial and non-commercial companies, showing how trusted access, authority and process knowledge can be misused for personal gain.

Organized crime (12%) and **external individuals** (9%) are primarily associated with document falsification and tax fraud, often victimizing commercial companies and government bodies, demonstrating that fraud risks can also originate outside the organization. This underlines the value of robust due diligence and monitoring of third-party interactions.

The victims

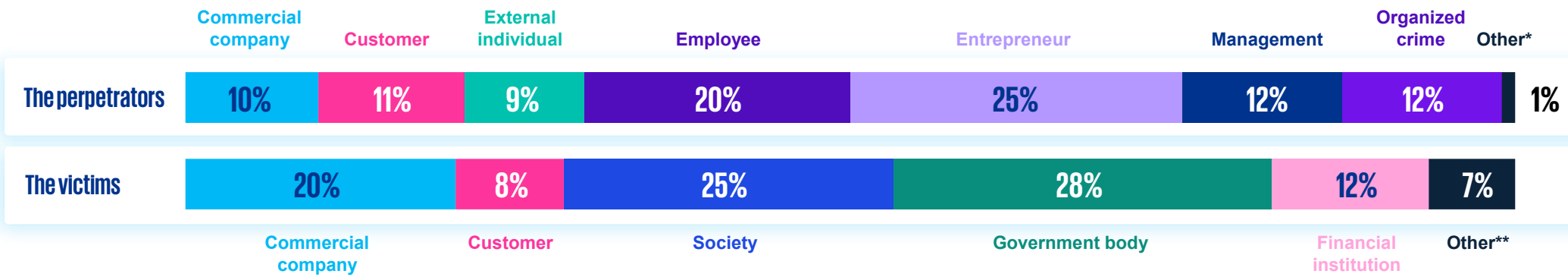
From a perspective focusing on the victims, government bodies are the dominant type, alongside society, commercial companies and financial institutions. Notably, 25% of cases involve more than one victim type.

Government bodies represent 28% of victims and are often exposed to tax, subsidy and benefits fraud. These offenses also affect society indirectly: tax fraud limits public inflows, while subsidy and benefits fraud increase outflows beyond what should be paid. Ultimately, wider society is left with fewer resources for public priorities.

Commercial companies form 20% of victims and are mainly targeted by internal perpetrators, such as employees and management, particularly through embezzlement and document falsification. This underscores the importance of addressing insider risk, where access, authority, and familiarity with organizational processes can create opportunities for misconduct.

Financial institutions amount to 12% of victims and are notably targeted by different perpetrator types, including their own clients through mortgage fraud and document falsification, underscoring the ongoing need for customer due diligence and document verification.

Distribution of perpetrators and victims in the fraudulent reporting and misappropriation domain



* 'Other' includes the following perpetrator types: financial institution (0.5%), and non-commercial organization (0.5%).

** 'Other' includes the following victim types: external individual (3.3%), and non-commercial organization (3.3%).

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A closer look at 'NOCLAR'

NOCLAR convictions

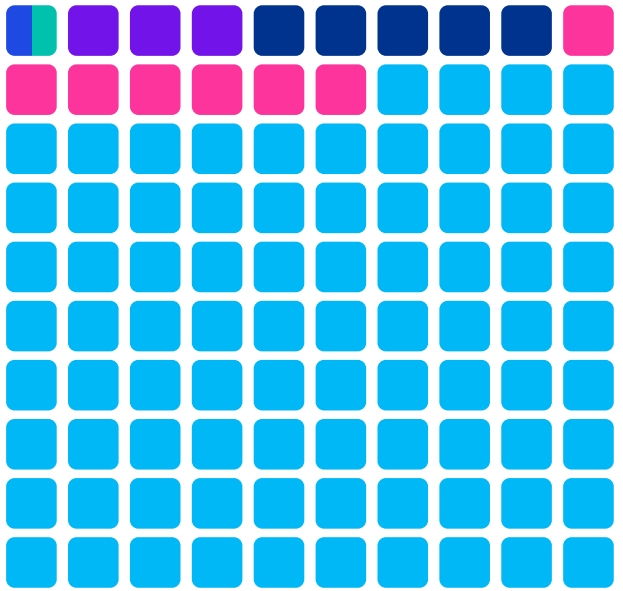
A total of 181 unique cases were identified as involving a primary conviction in the NOCLAR domain, with money laundering being the dominant offense (155 convictions).

In just over a quarter of its cases, **money laundering** appears alongside other white-collar crimes, most commonly document falsification and scams. This points to its role as the concealment layer within broader schemes, with document falsification helping to create apparent legitimacy and scam-related conduct generating illicit proceeds. Although most money laundering convictions are stand-alone within the scope of this report, case narratives show that money laundering often relates to predicate offenses outside the scope of this barometer, such as drug trafficking. Money laundering is also strongly associated with prison sentences, with the longest sentence reaching ten years. For financial institutions, strong customer due diligence, transaction monitoring, and escalation procedures for unusual activity remain key safeguards against the misuse of financial services. Failure to detect such activity may result in substantial regulatory, financial, and reputational consequences.

By contrast, **other compliance violations** (7%) are almost exclusively isolated offenses. While the other NOCLAR categories focus on underlying offenses, this category relates to failures to meet regulatory obligations. Examples include shortcomings in AML controls, fraud detection, oversight, and governance. In roughly half of these cases, companies are identified as the perpetrators, making fines a common outcome, while cases involving individual accountability more often led to prison sentences. Effective policies, oversight and regulatory adherence remain important safeguards against these violations.

Bribery (5%) and **corruption** (3%) occur less frequently but are rarely isolated. They are often linked with document falsification and computer fraud and abuse, and typically, they involve multiple perpetrators. This suggests that organizations should look beyond isolated incidents and consider how third-party relationships, internal influence, and misuse of systems can play key roles.

Distribution of NOCLAR convictions



- 0.5% Sanctions
- 0.5% Terrorism financing
- 3% Corruption
- 5% Bribery
- 7% Other compliance violations
- 84% Money laundering

Finally, the dataset contains a limited number of sanctions and **terrorism financing** cases. While limited in number, these cases show that both risks remain relevant and should continue to form part of AML, sanctions, and screening frameworks, as they can have far-reaching consequences.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The perpetrators

Within this domain, external individuals and organized crime together account for 71% of convicted cases. At the same time, insider risk remains significant, with entrepreneurs, employees and management together driving 24% of cases.

External individuals (40%) and **organized crime** (31%) are almost exclusively linked to money laundering cases. This suggests that while money laundering is often associated with structured criminal networks, a significant portion is carried out independently. This may point to lower-threshold entry into money laundering activities, in which individuals act as facilitators or intermediaries (e.g., money mules or small-scale actors), while more complex, coordinated schemes are driven by organized groups.

Entrepreneurs (11%) are also mainly associated with money laundering, which may indicate involvement as strawmen to conceal illicit financial flows. Their involvement in bribery and other compliance violations, victimizing mostly commercial companies and society, highlight the need for careful due diligence in business relationships, and effective compliance oversight.

Employees (7%) and **management** (6%) appear less frequently in this domain, but when involved, they are more often associated with bribery and corruption. This suggests that access, authority, and influence within organizations can play an important role in enabling these offenses, which most commonly affect commercial companies.

The victims

Society (64%) is the primary victim group, driven by the prominence of money laundering and its broader impact on financial integrity, market stability and public trust.

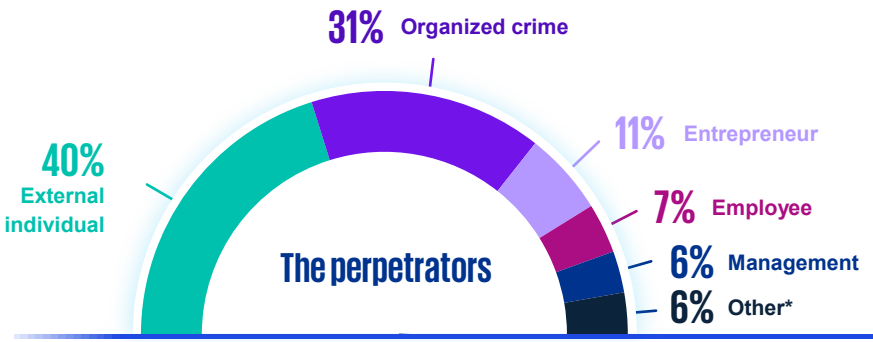
External individuals (9%) are also affected by money laundering schemes, often through underlying scams. This highlights the value to view suspicious transactions not only through an AML lens but also in combination with scam detection and customer protection.

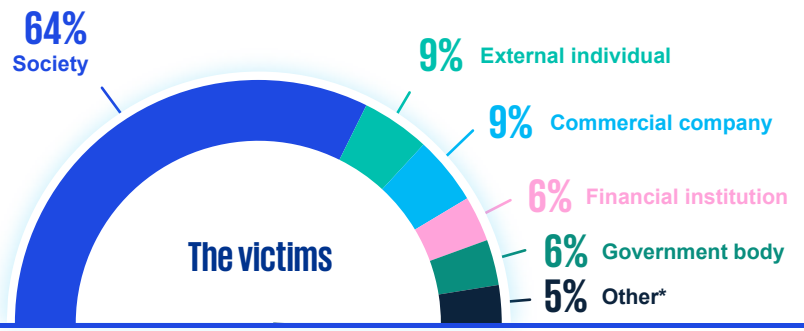
Financial institutions (6%) are mainly affected by more structured schemes, combining money laundering with offenses such as document falsification, scams, or mortgage fraud. Often driven by organized crime and entrepreneurs, these cases reinforce the importance of customer due diligence and transaction monitoring.

Commercial companies (9%) are the main victim group in bribery and corruption cases. Driven by a mix of organized crime, employees, and management, it shows how internal influence may be manipulated for personal or criminal gain, potentially damaging business integrity and trust in the organization.

Government bodies (6%) are mainly affected by money laundering schemes linked to offenses such as tax fraud, subsidy fraud, and embezzlement. The risk exposure in this domain is not limited to one single perpetrator profile but can arise through both internal misuse and external abuse of public systems or funds.

Distribution of perpetrators and victims in the NOCLAR domain





* 'Other' includes the following perpetrator types: commercial company (3.3%), customer (1.1%), and financial institution (1.1%).

** 'Other' includes the following victim types: customer (4.3%), non-commercial organization (0.4%), and employee (0.4%).

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A closer look at 'swindle'

Swindle convictions

A total of 102 unique cases were identified as involving a conviction in the swindle domain, covering scams, computer fraud and abuse, cyberfraud and identity fraud.

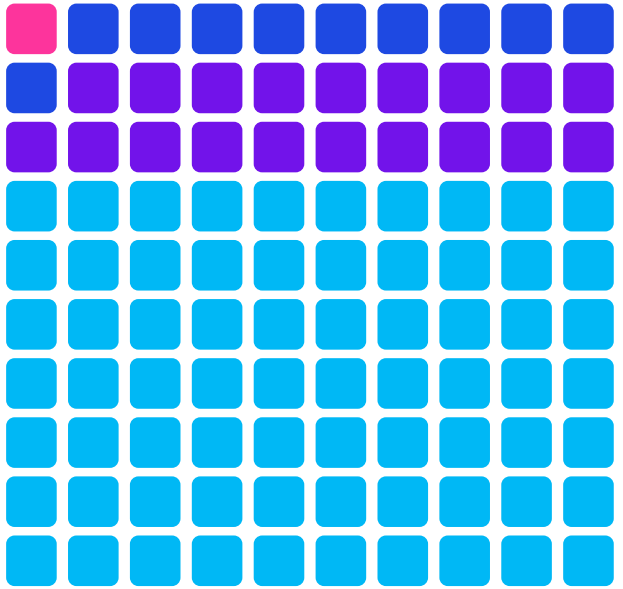
While individual-to-individual swindles occur in practice, they do not fall within the scope of the Fraud Barometer, as it focusses on cases with organizational involvement. As a result, only cases involving at least one party connected to an organization were included.

Scams account for the clear majority of convictions (70%). While nearly half of these cases are stand-alone offenses, scams are frequently combined with document falsification and money laundering, suggesting that organizations should not treat scam risk purely in isolation, but also as a part of broader schemes. Strengthening document verification, transaction monitoring and ongoing scrutiny of unusual activity can help mitigate these risks.

Computer fraud and abuse (19%) covers activities such as hacking, unauthorized access and data leakage. These offenses are rarely isolated and are often linked to other offenses such as cyberfraud, bribery, violations of privacy, or breaches of confidentiality. This illustrates how misuse of digital access can enable broader fraud, integrity, and compliance incidents, suggesting that cyber controls should be aligned with integrity and compliance protocols, rather than be treated as a separate domain. The strong involvement of employees makes this subtype particularly relevant from an insider-risk perspective. Managing these risks requires effective access management, monitoring of unusual user activity, and controls around sensitive systems and data.

Cyberfraud (10%) is predominantly observed as a stand-alone offense and is mainly externally driven. Because cyberfraud affects both organizations and customers, it can potentially disrupt business processes, weaken stakeholder trust and cause substantial financial losses.

Distribution of swindle convictions



- 1% Identity fraud
- 10% Cyberfraud
- 19% Computer fraud and abuse
- 70% Scam

Identity fraud (1%) appears only in combination with computer fraud and abuse, illustrating how it can serve as an entry point into broader digital fraud schemes. Even low-volume risks like identity fraud may have a severe impact when they act as the gateway to broader cyber-enabled crime.

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The perpetrators

An analysis of the perpetrators reveals that external individuals (37%) and organized crime (16%) together drive more than half of the cases, representing the strong presence of external threats. At the same time, employees (17%), entrepreneurs (14%) and management (8%) also account for a significant share, showing that swindle-related risks can arise both outside and within organizations.

External individuals, **organized crime** and **entrepreneurs** are mainly associated with scam and cyberfraud offenses, often affecting commercial companies, customers and financial institutions. This indicates the importance of maintaining resilience against external fraud threats and protecting the integrity of customer and business interactions.

Employees and **management** are the main driver behind computer fraud and abuse, occasionally collaborating with external individuals, showing the key role of insider access in enabling these crimes.

Moreover, in the majority of cases, the perpetrator was not acting alone. In such cases, swindles can be executed through coordinated networks, involving collaboration between multiple different actors.

The victims

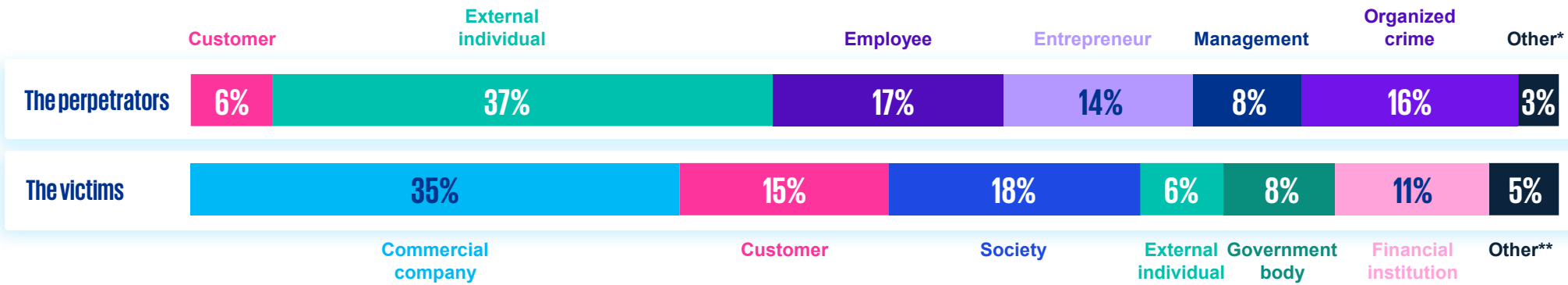
From a victim perspective, swindle offenses affect a wide range of stakeholders. **Commercial companies** emerge as the most frequently affected group (35%), mainly through scam-related offenses driven by external individuals and organized crime. At the same time, insider-enabled risks also emerge through offenses such as computer fraud and abuse, where employees misuse access to systems, data, or processes. Managing these risks requires attention to a combination of fraud, cyber, and insider risk controls.

Customers (15%) are primarily affected by scams orchestrated by entrepreneurs. These cases illustrate how products, services, and client-facing processes may be misused to deceive or exploit customers.

Society (18%) is the second-largest victim group, partly due to the recurring link between scams and money laundering. Still, it shows that the impact extends beyond direct victims, affecting financial integrity and public trust.

While many victims of a swindle are deliberately targeted by offenders, **individuals** (6%) often appear to be harmed as a side effect of broader schemes. As such, swindle-related crimes can create both institutional and personal harm, reinforcing the need for organizations to consider the wider impact of fraud schemes beyond direct losses.

Distribution of perpetrators and victims in the swindle domain



* 'Other' includes the following perpetrator types: commercial company (2.0%), and financial institution (1.0%).

** 'Other' includes the following victim types: non-commercial organization (1.9%), entrepreneur (1.9%), and employee (1.3%).

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

A closer look at 'integrity violations'

Integrity violations

Our dataset contains 73 unique cases surrounding Integrity violations, spanning ten subtypes such as extortion, misconduct, discrimination and conflicts of interest.

Unlike other domains, integrity violations are highly diverse, as no single subtype dominates, and most cases occur in isolation rather than alongside other offenses. Where overlaps do occur, it relates almost exclusively to money laundering or swindle.

This dispersion suggests that integrity risks typically arise in specific contexts rather than through one recurring pattern. As a result, organizations may benefit from a broad, well-integrated framework that addresses different types of behavior, rather than narrow controls.

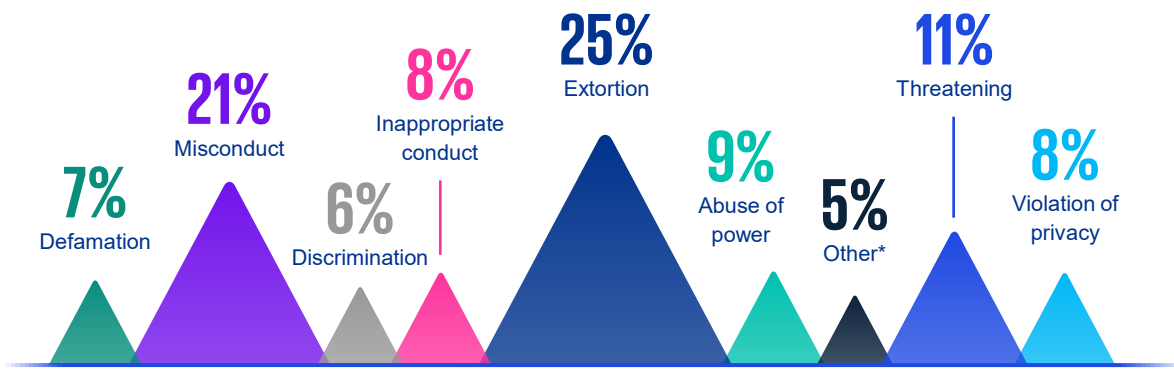
Extortion (25%) is the most frequent conviction and usually appears as a standalone crime. Even when combined with other offenses, no consistent pattern emerges in the combinations observed. When convicted, perpetrators most often receive either prison sentences or community service. The unpredictable and high-impact nature of these cases can make extortion risks, such as coercion or undue pressure, difficult to anticipate, reinforcing the need for strong internal reporting mechanisms and a culture where employees feel safe to speak up.

Misconduct (21%) also shows a stand-alone pattern. In practice, courts often impose financial or employment-related consequences, such as dismissals or suspensions. This may indicate that misconduct frequently occurs within existing working relationships, emphasizing the critical role of internal governance, disciplinary procedures, and clear codes of conduct.

A different dynamic can be seen in **threatening** (11%), which is more often linked to other white-collar crimes. Given the variety of these combinations, threatening behavior often appears to play a facilitating role within broader schemes. As a result, it should not be viewed as an isolated issue, but rather as a potential early warning sign of more complex misconduct.

Overall, integrity violations are diverse and highly context-driven, reflecting a wide range of behaviors across organizations. Therefore, they cannot be effectively managed through isolated or reactive measures. Instead, companies need a proactive, embedded approach that combines strong governance, continuous monitoring, and a culture of transparency and accountability. This is essential not only for early detection, but also to prevent issues from escalating into legal, financial, or reputational harm.

Distribution of integrity violations



* 'Other' includes the following subtypes: breach of confidentiality (2.4%), and conflict of interest (2.4%).

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The perpetrators

In the 73 integrity-related cases, three groups account for the majority of convictions: employees, external individuals, and management (together 85%), reflecting both internal exposure and distinct risk patterns.

Employees are involved in nearly all types of integrity violations, without a clear concentration in any single offense. Their actions are typically related to one type of offense rather than being part of broader schemes involving multiple charges. This suggests that employee-related integrity issues often arise from situational or behavioral factors rather than structural misconduct. For organizations, this reinforces the importance of preventative measures such as awareness, training, and a strong ethical culture to address a wide range of potential risks.

External individuals, in contrast, show a much more targeted pattern. Their involvement is largely concentrated in extortion and threatening, often combined with financially driven offenses such as money laundering. In these cases, companies and their employees are the primary targets and actions tend to be deliberate and goal-oriented in nature. For companies, strong safeguards at key interaction points are an important line of defense, particularly in areas involving financial transactions or external dependencies.

Management-level perpetrators are primarily linked to misconduct, abuse of power, and inappropriate conduct. These offenses typically stem from misuse of authority rather than external motives. They do not only affect the victim but also typically impact the culture within the team and the organization. broader

The victims

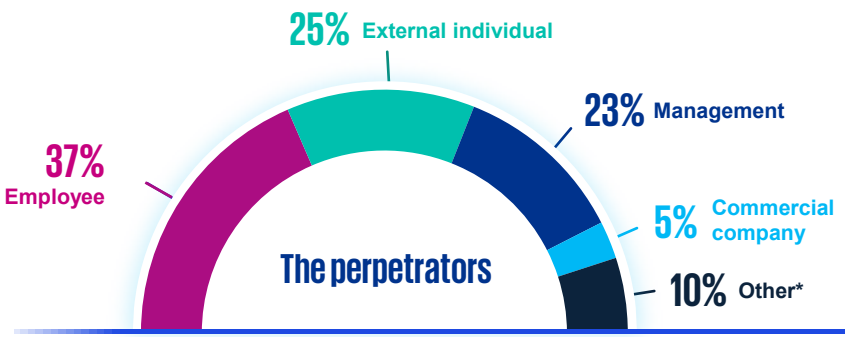
Employees are the most frequent victims in integrity-related cases, followed by commercial organizations, with other parties such as government bodies and non-commercial organizations affected less often.

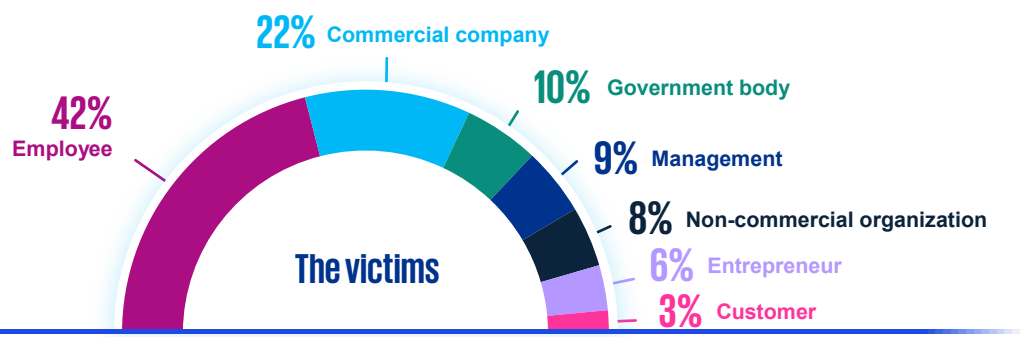
Employees (42%) are typically the sole victim and are exposed to a wide range of offenses, including extortion, abuse of power, and threatening. This highlights their vulnerability within organizational structures, particularly where power imbalances or interpersonal pressure play a role. A safe working environment, supported by accessible reporting channels, clear policies and trusted follow-up procedures, can help organizations address such risks.

Commercial companies (22%), on the other hand, are mainly affected by extortion and misconduct, usually as isolated, financially driven incidents. This shows that strong internal controls and clear processes, particularly in financial and operational areas, are key to mitigating these risks.

Integrity risks arise both internally and externally, from employee-related incidents to external threats and high-impact management cases. Managing these risks requires a balanced approach that combines strong internal culture and oversight with reliable external controls, enabling organizations to detect issues early and limit their impact.

Distribution of perpetrators and victims in the integrity violations domain





* 'Other' includes the following perpetrator types: government body (4.1%), customer (2.7%), entrepreneur (1.4%), and non-commercial company (1.4%).

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

From insights to action

The findings in this first edition of the KPMG Fraud Barometer highlight the broad, complex, and evolving nature of white-collar crime in the Netherlands. Fraud risks are not confined to a single profile, sector, or modus operandi. Instead, they are multi-faceted, involving both external actors and insiders, and often combining multiple offenses into structured and deliberate schemes. At the same time, the impact extends beyond individual victims, affecting organizations, institutions, and society as a whole.

Key takeaways

As schemes become more complex and technology continues to evolve, organizations need a proactive, integrated, and data-driven approach that combines prevention, detection, and response. Based on these findings, the following actions support organizations in strengthening their resilience to fraud, integrity and financial crime risks:

Managing insider risk

Employees and management are linked to a wide range of offenses, from embezzlement and document falsification to computer fraud and abuse. Managing insider risk requires more than traditional controls alone, combining effective oversight, access management, segregation of duties and data analytics to identify unusual behavior and reduce exposure to emerging risks.

Investigating and responding to misconduct

Many cases involve multiple offenses and perpetrators. Investigative approaches that combine forensic expertise, advanced analytics, technology-assisted evidence review, and AI-supported analysis help organizations establish facts quickly and diligently and respond effectively to potential misconduct.

Promoting a strong integrity culture

Many offenses stem from behavior within organizations. A strong ethical culture, supported by clear policies and governance, training, speak-up mechanisms, leadership commitment, and employee awareness, remains an important safeguard against misconduct and broader integrity risks.

Strengthening defenses against financial crime

More complex and coordinated schemes require organizations to combine effective controls, risk-based due diligence, transaction monitoring, advanced analytics and AI-enabled detection capabilities. Together, these measures can help identify unusual patterns, strengthen resilience against a wide range of fraud and financial crime risks, and support the timely detection and prevention of misconduct, including money laundering and other complex fraud schemes.

KPMG

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

How KPMG can help

The insights presented in this Fraud Barometer build on KPMG Forensic's extensive experience investigating fraud, integrity, and financial crime risks through a combination of data-driven insights, advanced analytics, AI-enabled solutions, and practical expertise.

We support clients with:

- **Fact-finding investigations into a wide spectrum of white-collar crimes, such as embezzlement, misappropriation and scams;**
- **Behavioral investigations into compliance or integrity incidents;**
- **Forensic technology services, leveraging AI capabilities in various types of investigations, including evidence collection, e-discovery and forensic data analytics;**
- **Model validation of AML and sanction compliance programs, and other models that prevent fraud;**
- **Cultural assessments, drafting and auditing company policies and codes of conduct, and various training and communication programs;**
- **Fraud risk management assessments to gain insight into key fraud and misconduct risks; and**
- **Third-party risk management solutions, such as compliance M&A due diligence and distributor reviews for contractual obligations.**

Contact us



Leonie Stolk
Partner, Head of Forensic NL

T +31 206568845
M +31 6 52488308
E stolk.leonie@kpmg.nl



Heleen Hoynck Van Papendrecht
Partner, Forensic Investigations

T +31 206567797
M +31 6 15073765
E hoynckvanpapendrecht.heleen@kpmg.nl



Muel Kaptein
Partner, Forensic I&C

T +31 206567794
M +31 6 51573611
E kaptein.muel@kpmg.nl



Patrick Özer
Partner, Forensic Technology

T +31 206568207
M +31 6 22694146
E ozer.patrick@kpmg.nl

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Appendix

Methodology

© 2026 KPMG Advisory N.V., a Dutch limited liability and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Appendix: Methodology

To identify relevant cases for the Fraud Barometer, KPMG Forensic followed a structured, multi-step methodology designed to achieve consistency and relevance in case selection, classification and analysis. The process consisted of three main phases: defining the scope, identifying relevant media articles and conducting a detailed review and classification of cases.

Defining the scope

KPMG Forensic defined the scope of the Fraud Barometer in line with our forensic expertise and the types of misconduct we frequently encounter in our work. The Fraud Barometer is therefore focused on offenses related to the following areas of financial and integrity-related crime: financial fraud, money laundering, embezzlement, bribery and corruption, cybercrime, integrity violations, NOCLAR, and greenwashing. Furthermore, only cases resulting in a formal court ruling or settlement issued by a Dutch court in 2025 were included. Finally, the Fraud Barometer is focused on cases with organizational involvement. As a result, all included cases involve at least one party connected to an organization, with the exception of money laundering cases due its relevance for the financial services industry.

Identifying relevant media

Potentially relevant articles were identified through structured media searches using carefully developed search terms and filters aligned with the predefined scope of the Fraud Barometer. The searches were performed through LexisNexis, a comprehensive research database that aggregates global media, legal, regulatory, sanctions, and corporate information sources. The Fraud Barometer is exclusively based on Dutch media sources, covering an extensive range of national, regional, and local newspapers, online news platforms, magazines and trade journals. These targeted searches helped narrow down the dataset to articles that were likely to fall within the predefined scope, while remaining sufficiently broad to avoid excluding potentially relevant articles at an early stage.

Classifying the cases

The collected articles from LexisNexis were deduplicated and the remaining set was screened against the predefined inclusion criteria using AI-driven review functionalities, followed by manual checks to verify the results. Articles that did not meet the criteria included, among others, those with convictions outside 2025 or the Netherlands, and cases outside the scope of financial and integrity-related crimes. The articles that fell within the scope of the Fraud Barometer were subsequently transformed into cases, with each convicted individual treated as a separate case. The resulting cases were classified using a standardized taxonomy covering the fraud domain, fraud subtype, perpetrator type, victim type, sentence type, and court location. This structured classification approach enables comparability across cases, facilitates trend analysis, and supports insights into the fraud, integrity and financial crime risks most prevalent in the Netherlands.

Definitions

The following working definitions were applied throughout the development of the Fraud Barometer and the analysis presented in this report:

- **NOCLAR (Non-Compliance with Laws and Regulations):** refers to offenses involving the concealment of illicit funds or non-compliance with applicable legal, regulatory, or professional obligations by individuals or organizations, including failures in governance, oversight, licensing, and reporting.
- **Fraudulent reporting and misappropriation:** refers to offenses involving the falsification or manipulation of information, records or reporting processes, as well as the unauthorized use or appropriation of funds, assets, or organizational resources.
- **Swindle:** refers to offenses that rely primarily on deceiving, manipulating or misleading victims to obtain money, information, access, or other benefits.
- **Integrity violations:** concerns unethical, inappropriate, abusive, or harmful conduct that undermines trust, governance, organizational integrity, workplace culture, or professional relationships.

KPMG

© 2026 KPMG Advisory N.V., a Dutch limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

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



kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

© 2026 KPMG Advisory N.V., a Dutch limited liability and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

Document Classification: KPMG Public