INSIDE THE MIND OF THE MODERN FRAUDSTER: A TEN-YEAR COMPARATIVE ANALYSIS (2014–2024)

Oleksandr Mihus[1], Mykhailo Laptiev[2]

[1]Student, WSHIU Academy of Applied Sciences, Poznan, Poland; Junior Researcher, Scientific Center of Innovative Research, Pussi, Estonia, e-mail: alexmihus@icloud.com, ORCID: https://orcid.org/0009-0007-7856-8199

[2]Ph.D. (Economics), Associate Professor, Associate Professor of the Department of Financial and Economic Security Management, KROK University, Kyiv, Ukraine, e-mail: michael.laptev@krok.edu.ua, ORCID: https://orcid.org/0000-0002-3537-6345

Citation:
Mihus, O., & Laptiev, M. (2025). Inside the Mind of the Modern Fraudster: a Ten-Year Comparative Analysis (2014–2024). *Public Administration and Law Review*, (1(21), 75–86. https://doi.org/10.36690/2674-5216-2025-1-75-86

Received: March 18, 2025
Approved: March 29, 2025
Published: March 31, 2025

Abstract. *Understanding the mindset and operational patterns of occupational fraudsters has become increasingly critical for modern organizations. Over the last decade, the landscape of occupational fraud has shifted in response to dynamic changes in workplace structure, digital communication, and employee roles. This study investigates the evolving profile of the occupational fraudster from 2014 to 2024, focusing on how demographic patterns, behavioral signals, organizational positioning, and detection channels have transformed. The topic is timely and relevant given the mounting complexity of internal threats that intersect with digital environments and new modes of employment. The primary objective of this research is to uncover how fraudster traits and fraud execution mechanisms have changed over a ten-year period and to determine what these shifts suggest about vulnerabilities within contemporary organizations. To achieve this, the study applies a longitudinal comparative approach using standardized data collected from thousands of occupational fraud cases. The analysis draws on a consistent framework of variables including age, gender, education, employment tenure, hierarchical position, behavioral indicators, collusion, and the methods by which frauds were detected. Both quantitative trends and qualitative behaviors were reviewed and interpreted thematically. The methodology integrates comparative metrics with interpretive analysis to construct a multidimensional understanding of the modern fraudster's evolution. The results reveal several significant patterns. While the demographic profile of fraudsters—predominantly male, mid-career, and educated—has remained largely stable, their placement within organizations has shifted. There has been a marked increase in employee-level frauds, particularly from departments such as operations, sales, and accounting. At the same time, executive-level fraud, though less frequent, continues to cause the most severe financial damage. Behavioral red flags remain widespread but underutilized in prevention, and frauds involving long-tenured employees or multiple collaborators prove significantly more costly. Detection methods have also modernized: digital whistleblowing tools, particularly web and email-based platforms, have overtaken traditional phone hotlines. These findings collectively point to a fraud risk environment that is more diffuse, digitally enabled, and embedded across all organizational levels. As organizations transition further into a digital-first, hybrid-working future, fraud prevention strategies must prioritize behavioral insight, adaptive internal controls, and culture-driven vigilance.*

Keywords: *occupational fraud; fraudster profile; internal fraud; whistleblowing; behavioral red flags; collusion; fraud detection; digital reporting systems; organizational risk; longitudinal fraud analysis.*

JEL Classification: D74, F52, H56, G32

Formulas: 0; fig.: 1; table: 6; bibl.: 12

Introduction. Occupational fraud remains one of the most significant financial threats to modern organizations, affecting both public and private sectors across the globe. As defined by the Association of Certified Fraud Examiners (ACFE), occupational fraud involves the misuse of one's position within an organization to achieve personal financial gain. Since 1996, the ACFE's biennial *Report to the Nations* has served as a foundational data source for understanding fraud schemes, the profiles of perpetrators, and the impact on organizations. While much attention has been paid to fraud prevention technologies and compliance strategies, comparatively less focus has been directed toward the evolving psychological, professional, and behavioral characteristics of fraudsters themselves. Between 2014 and 2024, the ACFE has documented over 20,000 occupational fraud cases, offering an invaluable dataset to examine the shifting profile of the modern fraudster. This study aims to synthesize this ten-year span of research, tracing demographic consistency, changes in organizational position, behavioral patterns, and shifts in detection mechanisms. Understanding how fraudster characteristics have evolved over time is essential to designing proactive, psychologically attuned prevention strategies that address not only fraud risk—but fraudsters themselves.

Literature Review. Occupational fraud, defined as the use of one's occupation for personal enrichment through the deliberate misuse of the employing organization's assets (Association of Certified Fraud Examiners [ACFE], 2024), remains one of the most pervasive and costly forms of white-collar crime globally. Over the past decade, extensive studies have been conducted to better understand the traits, behaviors, and environments that contribute to fraud perpetration. The ACFE's biennial *Report to the Nations* provides a robust data-driven foundation for understanding occupational fraud trends, synthesizing over 20,000 real-world cases across multiple industries and geographies. This literature review draws upon findings from ACFE reports published between 2014 and 2024 to trace the evolving profile of occupational fraudsters, with attention to demographic trends, behavioral indicators, organizational dynamics, and detection methods.

From 2014 to 2024, the core demographic characteristics of occupational fraudsters remained remarkably consistent. The majority of fraudsters were male (approximately 70% across all years), between the ages of 36 and 45, and held at least a bachelor's degree (ACFE, 2014, 2016, 2018, 2020, 2022, 2024). These patterns challenge traditional assumptions that fraud is more prevalent among lower-level or less-educated employees. Instead, they highlight that individuals with education and institutional trust are often those best positioned to exploit systemic vulnerabilities (Button, Johnston, & Frimpong, 2007). Importantly, fewer than 6% of fraudsters had prior fraud convictions, a finding consistent across all ten years, suggesting that many perpetrators are first-time offenders acting within trusted roles.

While the demographic profile has remained static, the organizational positions held by fraudsters have shown gradual evolution. In earlier reports, frauds were more often committed by executives and managers, with these individuals causing significantly higher losses per case due to greater access and authority (ACFE, 2014, 2016). However, by 2024, employees at the non-managerial level were responsible for

over 50% of fraud incidents, indicating a broadening of fraud risk across all hierarchical levels (ACFE, 2024). High-risk departments such as operations, accounting, and sales have consistently been implicated in a majority of fraud cases. The decentralization of access in modern workplaces, particularly through digitization and remote work, may explain this shift in perpetrator roles (Peltier-Rivest & Lanoue, 2015).

A consistent and critical feature of occupational fraudsters is the presence of behavioral red flags. Over 80% of fraudsters across all reports displayed at least one red flag prior to detection, most commonly living beyond their means, experiencing financial difficulty, exhibiting control issues, or being unusually secretive (ACFE, 2014–2024). These findings align with the Fraud Triangle theory introduced by Cressey (1953), which posits that fraud is driven by a combination of pressure, opportunity, and rationalization. Despite the predictability of these signs, many organizations fail to act on them, suggesting a gap between awareness and enforcement. Recent studies underscore the importance of behavioral analytics and proactive monitoring as part of internal controls (Murphy & Dacin, 2011).

Fraudsters with longer tenure pose an outsized risk to organizations. The ACFE (2024) reported that individuals with over 10 years at an organization caused median losses five times greater than those employed for less than a year. This trend has remained consistent throughout the decade and is explained by increased system familiarity and organizational trust, which can lead to reduced scrutiny. Additionally, collusion significantly elevates the financial impact of fraud. Cases involving three or more perpetrators result in median losses four times higher than those involving a single individual (ACFE, 2020, 2024). These findings underscore the necessity of separation of duties and continuous risk assessments within organizational structures (Wells, 2017).

Tip-offs have consistently been the most effective method of detecting fraud, accounting for over 40% of case detections annually (ACFE, 2014–2024). Most tips originate from employees, but there has been a noticeable increase in tips from external parties such as vendors and customers, particularly in recent years. Notably, the mechanisms through which tips are delivered have shifted dramatically—from telephone hotlines in earlier reports to email and web-based forms by 2024 (ACFE, 2024). This change reflects a broader digital transformation in communication and reporting culture. Studies on whistleblowing efficacy highlight the importance of anonymous, accessible channels for fostering a culture of transparency and accountability (Kaptein, 2011).

The decade-long data from the ACFE paints a complex yet coherent picture of the modern occupational fraudster. While the demographic and behavioral profiles have remained largely stable, important changes have occurred in the levels at which fraud is committed, the organizational factors enabling it, and the ways in which it is detected. These trends suggest that while the motivations for fraud may be enduring, the contexts and opportunities are increasingly shaped by organizational structure, technology, and cultural dynamics. Future research should explore how hybrid work, AI-driven controls, and ethical leadership influence the next generation of fraud risk.

For now, organizations must balance trust with vigilance, implementing data-driven strategies that anticipate—not just react to—the evolving fraud landscape.

Aims. The primary aim of this study is to analyze how the portrait of occupational fraudsters has changed over a ten-year period, based on data from the ACFE's *Report to the Nations* from 2014 to 2024. Specifically, this research seeks to:

- identify patterns and consistencies in fraudster demographics, including gender, age, education, and prior criminal background;
- examine the shifts in organizational roles from which fraud is most frequently committed and assess departmental risk areas;
- assess the financial impact of fraud across different hierarchical levels within organizations;
- explore the prevalence and type of behavioral red flags displayed by fraudsters prior to detection;
- investigate the relationship between employee tenure, collusion, and the magnitude of fraud losses;
- evaluate the evolution of fraud detection mechanisms, particularly whistleblower reporting methods, in a digitalized work environment.

By meeting these objectives, the study contributes to a more nuanced understanding of occupational fraud and offers actionable insights for corporate governance, internal auditors, and fraud investigators.

Methodology. This research employs a longitudinal comparative analysis using secondary data extracted from six editions of the ACFE's *Report to the Nations* (2014, 2016, 2018, 2020, 2022, and 2024). Each report synthesizes thousands of real occupational fraud cases submitted by Certified Fraud Examiners (CFEs) across more than 130 countries. The reports standardize key variables, including the demographic profile of perpetrators, position within the organization, detection methods, behavioral red flags, and financial loss. Quantitative data were systematically tabulated across each edition to identify trends, fluctuations, and stable characteristics. Variables such as gender, age range, education level, tenure, presence of collusion, and reporting channel were compared longitudinally. Additionally, qualitative interpretation was employed to analyze behavioral and organizational context. Where applicable, findings were contextualized within fraud theories such as the Fraud Triangle (Cressey, 1953) and contemporary frameworks in behavioral economics and organizational ethics. The methodology is interpretive in nature but grounded in consistent empirical datasets, enabling both statistical comparison and thematic exploration of evolving fraudster traits.

Results. Our research was conducted in the following areas:

- demographics of fraudsters;
- roles within organizations;
- financial impact by position;
- behavioral red flags;
- tenure and collusion;
- detection and whistleblowing.

Demographics of fraudsters: a decade of consistency and subtle shifts. Over the last ten years, the core demographic profile of occupational fraudsters has remained surprisingly stable. Across all the reports from 2014 to 2024, the majority of perpetrators were male, consistently making up around 70% of fraud cases.

Table 1. The key points of fraudster's demographics

Year	Gender	Most Common Age Range	Most Common Education Level	Prior Fraud Conviction
2014	66% Male	36–45	Bachelor's Degree	<5%
2016	69% Male	36–45	Bachelor's Degree	4%
2018	69% Male	36–45	Bachelor's Degree	4%
2020	72% Male	36–50	Bachelor's Degree	5%
2022	71% Male	36–45	Bachelor's Degree	6%
2024	70% Male	36–45	Bachelor's Degree	6%

Source: estimated by the authors

The most common age bracket for fraudsters remained 36 to 45 years old, which suggests that mid-career professionals—those who have gained trust, responsibility, and access within an organization—are the most likely to commit fraud. This aligns with the idea that opportunity, a key leg of the Fraud Triangle, increases with seniority and tenure. In terms of education, most fraudsters held at least a bachelor's degree, which challenges any stereotype that fraud is typically committed by underqualified or low-level workers. Interestingly, despite the massive financial consequences of their actions, very few perpetrators had prior fraud convictions—only about 4–6% over the years. This pattern reveals that most fraudsters are first-time offenders, likely exploiting trust placed in them over time. The implication here is sobering: organizations must be vigilant even with long-standing, educated employees who have clean records, as prior misconduct is not a reliable predictor. Trust, access, and rationalization appear to be much more significant drivers of fraud than prior criminal behavior.

Roles within organizations: from executive corridors to frontline desks. One of the more notable shifts from 2014 to 2024 has been the changing roles of perpetrators within their organizations. In earlier years, particularly 2014 and 2016, a significant share of occupational fraud was committed by managers and executives, who held the authority to override controls or manipulate financial records.

Table 2. The key roles of fraudsters in organizations

Year	Executives	Managers	Employees	Top Risk Departments
2014	19%	36%	42%	Accounting, Operations, Sales
2022	23%	36%	41%	Operations, Accounting, Sales, Executive Mgmt
2024	20%	30%	50%	Operations, Sales, Accounting, Customer Service

Source: estimated by the authors

Executives, though involved in fewer cases, caused the greatest financial losses—often several times more than those committed by lower-level employees. Over time, however, there has been a steady rise in the proportion of fraud committed by regular employees. By 2024, nearly half of all occupational fraud cases involved frontline staff,

indicating a decentralization of fraud risk. This trend may be due in part to broader access to financial systems and decentralized processes, especially in companies embracing digital transformation and remote work. Departments like operations, sales, accounting, and customer service consistently appear as high-risk areas. These units often involve frequent transactions, customer interaction, and physical or digital asset access, making them ideal environments for small but consistent misappropriations. The shift underscores that fraud is no longer a risk isolated to top leadership—vulnerabilities now exist across every level of an organization.

Financial impact by position: fewer execs, bigger scandals. While fraud at the employee level has become more frequent over the years, financial data from the reports consistently show that executive-level fraud remains the most devastating in terms of monetary loss.

Table 3. Financial impact by fraudster's role

Role	2014 Median Loss	2020	2022	2024
Executives	$500,000	$600,000	$337,000	$459,000
Managers	$130,000	$150,000	$125,000	Not Specified
Employees	$75,000	$60,000	$50,000	$60,000

Source: estimated by the authors

In 2014, the median loss for executive fraud was about $500,000, and by 2024 it had increased to approximately $459,000—even after some fluctuations in between. This is often because executives have the ability to manipulate larger financial systems, bypass internal controls, and influence subordinates, making detection more difficult. In contrast, employee-level fraud, though increasing in volume, tends to involve smaller sums—usually under $100,000. This suggests that while employees are the most frequent offenders, executives still represent the biggest single threat in terms of financial consequences. Managerial fraud tends to sit somewhere in the middle, both in frequency and median losses. Organizations should therefore tailor their fraud prevention strategies accordingly—focusing not only on deterring large-scale fraud at the top but also on monitoring the accumulation of smaller schemes at the operational level. The data implies that while fraud may be democratizing in frequency, the severity of the impact still depends heavily on the fraudster's level of access and authority.

Behavioral Red Flags: Warning Signs Hiding in Plain Sight. One of the most consistent findings across all the ACFE reports is the prevalence of behavioral red flags displayed by fraudsters before they are caught. Around 80–85% of fraudsters exhibit at least one such warning sign, often well in advance of the fraud being discovered.

Table 4. Behavioral Red Flags

Year	% of Fraudsters with Red Flags	Most Common Red Flags
2014	~80%	Living beyond means, Financial difficulties
2018	85%	Same
2022	85%	Same
2024	84%	Living beyond means (42%), Financial pressure, Control issues

Source: estimated by the authors

The most common red flags include living beyond one's means, experiencing financial difficulties, exhibiting control issues, or displaying unusual levels of defensiveness or secrecy. Despite this consistency, organizations often overlook or dismiss these signs, either due to a lack of training, organizational culture, or fear of accusing a colleague without definitive proof. Over the decade, the list of common behavioral indicators has remained largely unchanged, reinforcing their value as predictive tools. However, their effectiveness depends entirely on whether employees are educated to recognize and act on them. The consistent appearance of these red flags shows that fraud is rarely impulsive—it often comes with emotional and behavioral baggage that surfaces beforehand. A robust fraud prevention program, therefore, should incorporate behavioral training for managers and HR professionals to help spot and respond to these early warning signs. In the end, recognizing red flags is not just about suspicion—it's about awareness, communication, and culture.

Tenure and Collusion: The Hidden Multipliers of Fraud Risk. Two often overlooked dimensions in occupational fraud are the impact of the fraudster's tenure and the presence of collusion. The data across the decade makes it clear: the longer someone has worked at an organization, the more damaging their fraud tends to be. Fraudsters with over 10 years of tenure often cause median losses 4–5 times greater than those who have been employed for less than a year. This is likely because long-tenured employees understand internal systems deeply, and they are often trusted implicitly, which reduces the scrutiny they receive. Meanwhile, collusion—where two or more individuals commit fraud together—amplifies the damage dramatically.

Table 5. Tenure and collusion to defraud

Perpetrators	2024 Median Loss
Solo	$75,000
3+ Collaborators	$329,000

Source: estimated by the authors

In 2024, frauds involving three or more people resulted in median losses over $300,000, compared to just $75,000 for solo perpetrators. Collusion also makes detection much harder, as checks and balances are neutralized from within. These findings emphasize the importance of rotating duties, implementing checks even for high-trust employees, and creating safe, anonymous reporting mechanisms that encourage whistleblowing from those who may observe collaborative misconduct. Tenure and teamwork, though often celebrated in business culture, can become powerful tools for fraud if left unmonitored.

Detection and Whistleblowing: The Digital Evolution of Tips. The way occupational fraud is detected has evolved significantly in the last decade, particularly with the rise of digital whistleblowing tools. Tips have remained the leading method of detection, responsible for over 40% of all cases in every report. However, the channel through which tips are submitted has changed dramatically. In 2014, telephone hotlines were the most common tool for whistleblowers.

Table 6. Changes in fraud detection

Year	% Detected by Tip	Most Common Tip Sources	Key Reporting Channels
2014	40%	Employees	Telephone hotline
2018	46%	Employees (50%), External (30%)	Hotline, Email, Web
2022	42%	Employees	Web and Email surpassed phone
2024	43%	Employees (52%), Vendors (11%)	Web (40%), Email (30%), Phone (27%)

Source: estimated by the authors

By 2024, email and web-based forms had overtaken the telephone, reflecting shifts in communication preferences, generational changes, and the rise of remote work. Most tips still come from employees, but there's a growing percentage from vendors, customers, and competitors—emphasizing the need for open, external reporting channels. The presence of a hotline is also strongly correlated with lower losses and faster detection. Organizations with a formal, well-publicized reporting mechanism detect fraud more quickly and at a significantly lower cost. As fraud schemes adapt to a digital world, so too must detection efforts. Training staff on how to use these tools, and fostering a culture of transparency and zero tolerance, will be critical to staying ahead of increasingly sophisticated fraud tactics.

Predictions for the Future Fraudster (2025–2035) are presented by Figure 1.

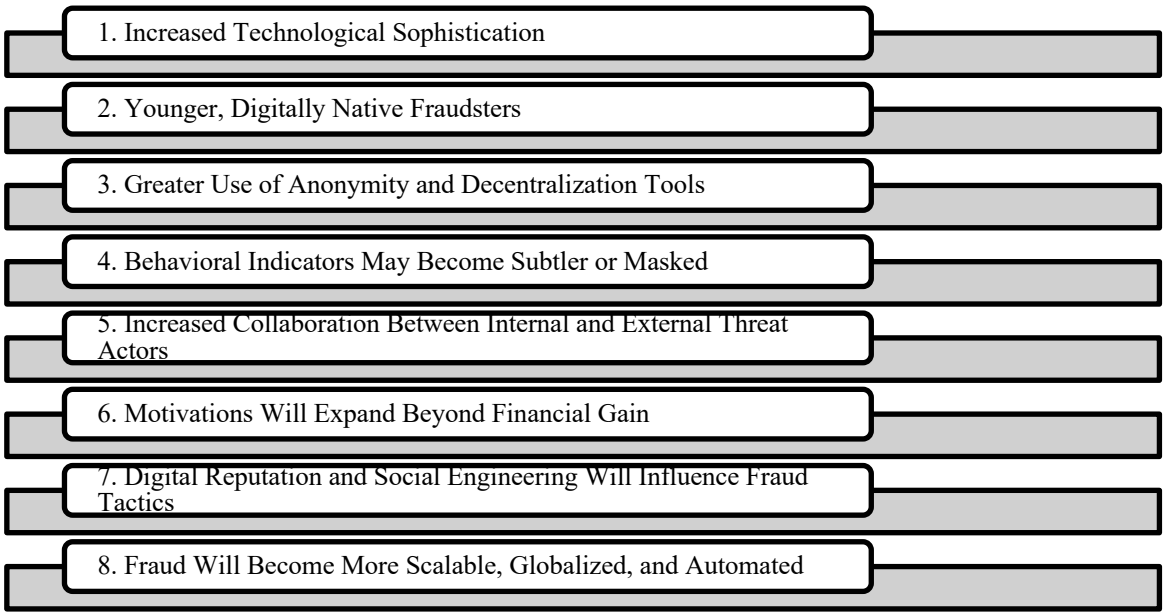

Figure 1. Predictions for the Future Fraudster (2025–2035)

Source: estimated by the authors

1. Increased technological sophistication. As organizations continue integrating artificial intelligence, blockchain, and digital transaction systems, future fraudsters will likely possess greater technological literacy. The average perpetrator may no longer be confined to traditional accounting or operations roles but could emerge from IT, cybersecurity, or data analytics departments. These individuals will exploit system vulnerabilities, automate fraudulent scripts, or manipulate data pipelines, often leaving fewer detectable traces. Cyber-enabled occupational fraud—such as digital asset misappropriation, identity spoofing, or algorithmic manipulation—may surpass traditional check tampering or billing schemes in both frequency and financial impact.

2. Younger, digitally native fraudsters. The fraudster demographic may shift downward in age, with more cases committed by individuals in their 20s and early 30s. As younger, digitally fluent employees enter the workforce with advanced technical skills but potentially limited ethical maturity, they may rationalize digital fraud as a "victimless" crime. This cohort may also be more adept at circumventing outdated fraud controls and less bound by loyalty to organizational norms. Organizations must therefore prepare for a rise in tech-savvy, early-career fraudsters who blend into agile and decentralized digital teams.

3. Greater use of anonymity and decentralization tools. Tools such as encrypted communication platforms, anonymizing software (e.g., VPNs, Tor), and decentralized finance (DeFi) systems will provide fraudsters with more sophisticated means of concealing their identities and laundering funds. Future fraudsters are expected to exploit the opacity of cryptocurrencies and blockchain-based contracts to reroute misappropriated assets beyond traditional traceability. This will demand forensic and investigative teams to build stronger capabilities in digital asset tracking and crypto-compliance enforcement.

4. Behavioral indicators may become subtler or masked. While behavioral red flags will remain relevant, the digital-first environment may make such indicators harder to observe. In remote or hybrid work settings, supervisors and peers will have fewer face-to-face interactions, reducing opportunities to identify changes in demeanor, lifestyle, or stress behavior. Future fraud prevention will need to include digital behavioral analytics, such as irregular login patterns, suspicious file downloads, and unusual communication metadata, as new types of "digital red flags."

5. Increased collaboration between internal and external threat actors. With the growth of insider trading forums, encrypted social networks, and dark web marketplaces, the future may see a rise in collaborative fraud between internal employees and external hackers or fraud rings. This externalization of collusion will complicate detection, as it blends occupational fraud with cybercrime. Organizations will need to monitor both insider activity and external cyber threats holistically, rather than treating them as separate domains.

6. Motivations will expand beyond financial gain. Whereas financial pressure remains a classic motivator under the Fraud Triangle model, the coming decade may see fraud driven more by ideological, political, or retaliatory motives, especially in the context of layoffs, ethical disagreements, or social activism. "Hacktivist" behavior and whistleblower-turned-fraudster narratives may blur lines between ethical dissent and criminal intent. Organizational ethics and cultural alignment will play an increasingly important role in mitigating such risks.

7. Digital reputation and social engineering will influence fraud tactics. Future fraudsters may weaponize their digital reputations—using social media profiles, AI-generated credentials, or deepfake technologies—to gain trust, falsify employment histories, or impersonate authority figures. Social engineering attacks that exploit trust within the organization, such as business email compromise (BEC) or CEO fraud, will evolve into more convincing, AI-enhanced forms. Fraud detection will need to

incorporate identity verification, digital credential authentication, and AI-generated content detection.

8. Fraud will become more scalable, globalized, and automated. Automation tools and generative AI may enable fraudsters to conduct wider-reaching fraud schemes with minimal effort. For instance, a single fraudster could deploy bots to generate fake invoices, simulate communication chains, or exploit AI-driven procurement systems. This means that future occupational fraud may not only be more scalable, but also more difficult to trace to a single individual. Cross-border fraud networks may become more common as fraudsters exploit jurisdictional gaps in regulation and enforcement.

In summary, the occupational fraudster of the next decade will be younger, more tech-enabled, more anonymous, and possibly more ideologically motivated. Their methods will reflect the tools and culture of an increasingly digital workplace, requiring fraud prevention strategies to shift from purely procedural controls to intelligent, adaptive systems that combine behavioral insight, data analytics, and ethical leadership. Organizations that wish to stay ahead of the curve must invest not only in fraud detection technologies but also in cultivating a digitally literate, ethically grounded workforce that can recognize and respond to these emerging threats.

Discussion. The findings of this ten-year comparative analysis reveal both persistent patterns and emerging shifts in the profile of occupational fraudsters. One of the most stable traits across all reports is the demographic profile: predominantly male, aged 36–45, and holding at least a bachelor's degree. This consistency challenges any lingering misconceptions that occupational fraud is primarily committed by entry-level or unqualified personnel. Instead, it reinforces that individuals with organizational trust and authority—whether formal or informal—are best positioned to exploit internal vulnerabilities.

However, while demographics have remained steady, the organizational context of fraud has shifted considerably. A notable trend is the increasing proportion of fraud cases committed by non-managerial employees. By 2024, frontline staff accounted for 50% of fraud incidents, a significant rise from a decade earlier. This decentralization may reflect broader organizational changes, including flatter hierarchies, remote work arrangements, and widespread access to financial and operational systems. The shift implies that fraud risk can no longer be contained by focusing solely on executive or managerial oversight; instead, it must be distributed across all organizational levels through pervasive internal controls and risk assessments.

Financial losses, though, still reflect the power dynamics of organizational roles. Executives, despite being involved in fewer cases, consistently cause the largest median losses. Their ability to override controls, manipulate reporting, and collude across departments enables frauds that are both prolonged and expensive. At the same time, the compounding effects of tenure and collusion are evident: long-standing employees and multi-person schemes result in significantly higher losses and more complex detection challenges. These findings stress the need for rotating job duties, monitoring long-tenured staff with privileged access, and enforcing segregation of duties—even among highly trusted employees.

Behavioral red flags also remained prominent across all case studies. Over 80% of fraudsters displayed at least one warning sign prior to detection, typically involving financial pressure or changes in behavior. Yet these indicators were often overlooked or dismissed, revealing a persistent gap between observable signs and organizational action. The effectiveness of fraud prevention programs will increasingly depend on equipping personnel—not just auditors or compliance teams—with training to recognize and escalate concerns tied to behavioral risk.

Finally, detection mechanisms have experienced a digital transformation. While tips remain the most effective method of uncovering fraud, the mediums through which they are delivered have evolved. By 2024, web-based and email reporting channels had overtaken telephone hotlines, reflecting generational shifts and the prevalence of remote work. This evolution underscores the importance of maintaining accessible, anonymous, and multi-channel whistleblowing systems that encourage both internal and external parties to report suspicious behavior without fear of retaliation.

Together, these patterns suggest that the profile of the fraudster is not simply a static identity—it is shaped by the surrounding technological, cultural, and organizational environment. Fraud schemes today are more embedded, harder to detect, and increasingly tied to systemic failures in trust, oversight, and culture. The need for proactive, psychologically informed, and digitally sophisticated fraud prevention strategies has never been greater.

Conclusion. Over the past decade, the landscape of occupational fraud has undergone both steady and seismic changes. The fraudster remains, in many ways, a familiar figure: educated, mid-career, and acting within the trust of the organization. Yet the nature of their activities, the roles from which they operate, and the systems they exploit have become increasingly complex and diffuse. Fraud has migrated from boardrooms to back offices, from paper trails to digital networks, and from lone actors to covert teams embedded within and beyond the organization.

This study underscores that traditional approaches to fraud prevention—though still vital—must evolve. Demographic indicators alone are insufficient for early detection. Instead, organizations must embed fraud detection into their daily operations, drawing on behavioral insights, technological monitoring, and robust ethical cultures. The growing presence of digital tools for whistleblowing, combined with behavioral analytics and access control systems, offers new avenues for identifying misconduct before it escalates into systemic abuse.

Looking ahead, as fraudsters adopt new technologies and blend occupational fraud with cybercrime, the challenge will be not only to keep pace but to stay ahead. The findings from 2014 to 2024 provide a solid foundation for anticipating the threats of the next decade—threats that will require organizations to become more agile, more vigilant, and more ethically grounded. Ultimately, the fight against occupational fraud is not just about stopping bad actors. It is about understanding the environments in which they thrive and reengineering those environments to prioritize integrity, accountability, and resilience.

Author contributions. The authors contributed equally.

Disclosure statement. The authors do not have any conflict of interest.

References:

1. Association of Certified Fraud Examiners. (2014). *Report to the Nations on Occupational Fraud and Abuse: 2014 Global Fraud Study*. ACFE.
2. Association of Certified Fraud Examiners. (2016). *Report to the Nations on Occupational Fraud and Abuse: 2016 Global Fraud Study*. ACFE.
3. Association of Certified Fraud Examiners. (2018). *Report to the Nations: 2018 Global Study on Occupational Fraud and Abuse*. ACFE.
4. Association of Certified Fraud Examiners. (2020). *Report to the Nations: 2020 Global Study on Occupational Fraud and Abuse*. ACFE.
5. Association of Certified Fraud Examiners. (2022). *Report to the Nations: 2022 Global Study on Occupational Fraud and Abuse*. ACFE.
6. Association of Certified Fraud Examiners. (2024). *Report to the Nations: 2024 Global Study on Occupational Fraud and Abuse*. ACFE.
7. Button, M., Johnston, L., & Frimpong, K. (2007). Fighting fraud: The case for a national fraud strategy. *Criminal Justice Matters, 66*(1), 4–5. https://doi.org/10.1080/09627250708553415
8. Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.
9. Kaptein, M. (2011). From inaction to external whistleblowing: The influence of the ethical culture of organizations on employee responses to observed wrongdoing. *Journal of Business Ethics, 98*(3), 513–530. https://doi.org/10.1007/s10551-010-0591-1
10. Murphy, P. R., & Dacin, M. T. (2011). Psychological pathways to fraud: Understanding and preventing fraud in organizations. *Journal of Business Ethics, 101*(4), 601–618. https://doi.org/10.1007/s10551-011-0741-0
11. Peltier-Rivest, D., & Lanoue, C. (2015). Cutting losses: Insights from fraud victims. *Journal of Financial Crime, 22*(2), 124–136. https://doi.org/10.1108/JFC-01-2014-0007
12. Wells, J. T. (2017). *Corporate fraud handbook: Prevention and detection* (5th ed.). Wiley.