EXPLOITING TRUST: THE FRAUD LIFECYCLE OF INTERNAL THREAT ACTORS

UNIVERSAL JOURNAL OF 21ST CENTURY
Women's Entrepreneurschip, Leadership, Technology & Publishing

Dr. Connie Y. Bell
Senior Vice President,
Security Risk, Global Incident Response & Fraud Analytics
Professor and Chair, University of Phoenix

KEYWORDS

Insider Fraud, Occupational Fraud, Fraud Lifecycle, Consumer Data Exploitation, Privilege Escalation, Obfuscation Techniques, Fraud Detection, Governance and Ethics, Fraud Triangle, Fraud Diamond, Fraud Polygon, Insider Threat, Behavioral Analytics, Whistleblower Protections, Data Privacy (GDPR, CCPA), Zero Trust Architecture, Organizational Culture, Segregation of Duties, Reputational Risk

ABSTRACT

Insider-driven fraud remains a significant and often underappreciated threat to organizations, particularly those managing consumer data and financial operations. Unlike external attackers who must breach defenses, insiders take advantage of their legitimate access to manipulate systems targeting processes such as refunds, credits, and account management. This article traces the lifecycle of internal fraud actors across key phases: reconnaissance, privilege escalation, lateral movement, obfuscation, execution, and evasion. It examines how these stages contribute to data exploitation, privacy breaches, and financial

misconduct. Drawing from fraud theory and governance research, the study emphasizes the urgent need for robust internal controls, zero-trust architecture, and ethically grounded leadership. It concludes with practical guidance for organizational leaders and suggests avenues for further research into mitigating insider risk.

INTRODUCTION: INSIDER FRAUD IN THE AGE OF CONSUMER DATA

Insider fraud is becoming an increasingly complex challenge in the digital age, as employees leverage authorized access to perpetrate fraud against consumers and the organizations they serve. These acts often take the form of unauthorized refunds, credit adjustments, or the misuse of consumer data for personal advantage. According to the Association of Certified Fraud Examiners (ACFE, 2024), occupational fraud leads to billions of dollars in global losses annually, with the median time to detection surpassing 12 months. This significant delay indicates that fraud embedded in everyday customer interactions can often go unnoticed for extended periods. Supporting this concern, PwC's (2022) Global Economic Crime and Fraud Survey identifies insider-enabled fraud as one of the most difficult types to prevent, primarily due to its dependence on employee trust and deep familiarity with internal systems and processes.

To explain the motivations and mechanisms behind such internal misconduct, scholars have long turned to classic fraud theories. Cressey's (1953) Fraud Triangle, for example, frames fraud through the lenses of opportunity, pressure, and rationalization. Building on this model, Wolfe and Hermanson's (2004) Fraud Diamond introduces the concept of capability, while Roffia and Poffo's (2025) Fraud Polygon further incorporates organizational culture and contextual factors. These theoretical frameworks offer valuable insights into the enabling conditions of insider fraud, particularly in environments where employees interact directly with consumer data and financial systems. Collectively, they underscore how individual motivations intersect with structural vulnerabilities to create openings for internal exploitation.

THEORETICAL FRAMEWORK

Theoretical frameworks offer critical tools for interpreting insider fraud, grounding behavioral patterns in established academic models. Cressey's (1953) Fraud Triangle remains foundational, suggesting that fraud occurs when opportunity, pressure, and rationalization converge. In the context of consumer data exploitation, opportunity often arises from excessive or poorly managed access rights, pressure stems from personal or financial stressors, and rationalization may take the form of common justifications like "everyone does it" or "the company won't notice." These elements provide a structured way to understand why otherwise trusted employees might cross ethical boundaries.

Expanding on this, Wolfe and Hermanson's (2004) Fraud Diamond introduces a fourth component, capability, highlighting the importance of technical skill and procedural knowledge in facilitating fraud. Employees typically have both the access and the expertise needed to navigate internal systems without raising suspicion. This makes insider fraud particularly difficult to detect and disrupt, as perpetrators can embed their schemes within normal consumer-facing processes, evading basic oversight mechanisms.

Recent work by Roffia and Poffo (2025) further refines this understanding with the Fraud Polygon, which incorporates organizational culture and structural vulnerabilities. This framework emphasizes that insider fraud is not purely the result of individual choice; it is shaped by weak governance, poor internal controls, and permissive ethical climates. In cases involving consumer privacy violations or refund manipulation, for example, insufficient oversight and a lack of whistleblower protections can allow fraudulent behavior to persist unchecked (needs citation).

Complementing these fraud-specific models, insider threat frameworks from the CERT Insider Threat Center and corporate governance research (Johari et al., 2022; Deloitte, 2023) stress the importance of ethics and organizational resilience. These perspectives frame insider fraud as more than just a

financial or technical issue. It is fundamentally a governance problem. Addressing governance requires not only advanced monitoring tools but also strong ethical leadership, clear accountability structures, and a culture that discourages misconduct from the top down. Together, these theoretical lenses lay the groundwork for analyzing the insider fraud lifecycle detailed in the following sections.

THE LIFECYCLE OF FRAUD-CENTRIC INSIDER THREATS

RECONNAISSANCE AND DISCOVERY

Insider fraud often begins with a phase of reconnaissance, during which employees observe and test internal systems to uncover vulnerabilities. For example, call center agents may experiment with refund protocols to identify loopholes or seek out consumer accounts that receive minimal oversight. Research indicates that environments lacking proper segregation of duties and robust access controls are especially susceptible to such activity (Colwill, 2009). Armed with process familiarity and access to consumer data, insiders can craft highly targeted schemes that exploit specific organizational weaknesses.

ESCALATION OF PRIVILEGES

When initial access proves insufficient for executing fraud, insiders may escalate their privileges through various strategies. These can include collusion with supervisors, exploiting technical misconfigurations, or requesting elevated roles under false pretenses. Gaining higher-level access enables fraud actors to override controls, approve unauthorized refunds, or retrieve sensitive customer information. Such escalation reveals how deeply insider fraud relies on trust within the organization, enabling actors to manipulate systems from within (Hu et al., 2020).

LATERAL MOVEMENT

After securing elevated access, insiders often extend their reach through lateral movement across interconnected platforms. For instance, a fraudster who begins in a billing environment might later gain access to loyalty programs or vendor accounts. This cross-system infiltration amplifies the scope of fraud and allows malicious activity to blend in with legitimate operations. According to CrowdStrike (2023), lateral movement is especially effective for concealment, as actions mimic standard user behavior, making them difficult to distinguish from routine tasks.

OBFUSCATION AND PERSISTENCE

To keep fraudulent schemes running over time, insiders typically deploy obfuscation techniques designed to mislead monitoring systems and auditors. Common strategies include falsifying audit logs, creating fictitious consumer profiles, and distributing unauthorized credits across numerous transactions to avoid detection. The ACFE (2024) finds that such schemes often remain active for more than a year, largely due to ineffective oversight and monitoring mechanisms. Fraudsters also embed recurring approvals or automate processes to simulate legitimate workflows, which further delays discovery and complicates remediation efforts.

EXECUTION OF OBJECTIVES

The execution phase marks the realization of insider fraud schemes, typically through unauthorized actions such as issuing refunds, applying illegitimate credits, or misusing consumers' personally identifiable information (PII). These activities can lead to direct financial loss, regulatory repercussions under laws like the GDPR and CCPA, and significant reputational harm (Johari et al., 2022). Beyond financial and legal consequences, the exploitation of consumer trust fundamentally undermines an organization's credibility and its social license to operate.

EVASION AND EXIT

In the final stage, insiders attempt to cover their tracks through evasion strategies, including erasing digital evidence, submitting resignation, or embedding persistent access mechanisms for future exploitation. Often, fraudulent activity is only discovered well after the perpetrator's departure, usually triggered by consumer complaints or uncovered during forensic investigations (Kroll, 2023). This delayed recognition reflects the broader challenge of distinguishing insider fraud from routine customer service behaviors, particularly in high-volume, consumer-facing environments (needs citation). As a result, organizations may face prolonged periods of exposure

before identifying the breach and initiating remediation.

KEY DISTINCTIONS FROM EXTERNAL FRAUD ACTORS

Although both internal and external fraud actors seek financial benefit, insiders possess critical advantages that make their schemes more difficult to detect. Unlike external attackers who must bypass security perimeters, insiders operate with authorized credentials and benefit from the inherent trust placed in employees. Their deep familiarity with internal workflows and customer-facing processes allows them to design fraud strategies that seamlessly blend with routine operations. While external threats often trigger alerts through unusual login patterns or unauthorized system access, insider fraud frequently goes unnoticed, disguised as standard consumer service activity (PwC, 2022). These fundamental differences underscore the need for fraud detection systems specifically tailored to insider behaviors rather than generalized threat models.

RECOMMENDATIONS FOR LEADERS

Organizational leaders play a pivotal role in reducing the risk of insider fraud by embedding robust governance into both culture and systems. First, enforcing segregation of duties and role-based access controls limits the ability of individuals to exploit systems unchecked. Second, the deployment of continuous monitoring and behavioral analytics can flag unusual refund or credit activity before it escalates. Third, fostering a speak-up culture is essential, this includes establishing secure whistleblower channels and clearly communicating protections for those who report concerns (Deloitte, 2023). Lastly, leaders should reframe insider fraud as a consumer trust issue, integrating fraud mitigation strategies with environmental, social, and governance (ESG) commitments to protect long-term reputational capital (needs citation).

RECOMMENDATIONS FOR FUTURE RESEARCH

There are several promising directions for future inquiry into insider fraud. Research should examine how global variations in consumer privacy regulations intersect with organizational fraud and governance frameworks. Additionally, scholars could assess the efficacy of AI and machine learning tools in identifying fraud patterns that are otherwise hidden within legitimate transactions. Comparative industry studies may also shed light on how sector-specific factors, such as consumer interaction volume or levels of regulatory scrutiny, affect vulnerability to insider schemes. Finally, longitudinal research is needed to evaluate whether interventions like ethics training and restorative governance practices meaningfully reduce fraud recurrence over time (needs citation).

CONCLUSION

The insider fraud lifecycle reveals how trusted access, operational knowledge, and internal process manipulation can be weaponized to breach consumer trust. Unlike external threats, insider actors operate within the bounds of legitimate roles, embedding fraud into everyday activities, which significantly complicates detection and response. Recognizing these dynamics enables organizations to adopt more targeted governance strategies that not only strengthen fraud controls but also align with consumer protection and privacy imperatives. Ultimately, mitigating insider fraud requires a holistic approach, combining technical defenses with ethical leadership, cultural reinforcement, and an evolving research base that supports continuous improvement in prevention.

Acknowledgement

The author acknowledges using Open AI's ChatGPT (GPT-5) language model to assist in research synthesis and editorial refinement. While the author maintained full control over content development and scholarly positioning, the AI tool enhanced clarity, coherence, and academic rigor.

REFERENCES

ACFE. (2024). *Occupational fraud: A report to the nations*. Association of Certified Fraud Examiners. https://www.acfe.com

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report, 14*(4), 186–196. https://doi.org/10.1016/j.istr.2010.04.004

CrowdStrike. (2023). *What is lateral movement?* https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/

Cressey, D. R. (1953). *Other people's money: A study in the social psychology of embezzlement*. Free Press.

Deloitte. (2023). *The future of fraud risk management: Shaping proactive, ethical governance*. Deloitte Insights. https://www2.deloitte.com

Hu, Q., Xu, Z., Dinev, T., & Ling, H. (2020). Does deterrence work in reducing information security policy abuse by employees? *Communications of the ACM, 63*(3), 80–87. https://doi.org/10.1145/3365020

Johari, R. J., Rosnidah, I., Talib, N. A., & Helmi, I. M. (2022). Role of code of ethics in building a fraud-resilient organization: The case of the developing economy. *Governance & Regulation, 11*(2), 32–40. https://doi.org/10.22495/jgrv11i2art3

Kroll. (2023). *The intrusion lifecycle and insider threats.* https://www.kroll.com/en/publications/cyber/kroll-intrusion-lifecycle

PwC. (2022). *Global economic crime and fraud survey 2022*. PricewaterhouseCoopers. https://www.pwc.com/fraudsurvey

Roffia, P., & Poffo, M. (2025). Revisiting the fraud triangle in corporate frauds: Towards a polygon of elements. *Journal of Risk and Financial Management*, *18*(3), Article 156. https://doi.org/10.3390/jrfm18030156

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal*, *74*(12), 38–42