Inovasi : Jurnal Sosial Humaniora dan Pendidikan
Volume. 4 Nomor. 3 September 2025
e-ISSN : 2809-0268; p-ISSN : 2809-0403, Hal. 539-547
DOI: https://doi.org/10.55606/inovasi.v4i2.4530
Available online at: https://journalcenter.org/index.php/inovasi

Early Detection and Prevention of Skimming in Digital Financial Systems: A Forensic Accounting Approach in the Era of Technological Transformation

Faizul Idris[1], Yoel Latif[2], Pupung Purnamasari[3]
Master of Accounting, Faculty of Economics and Business, Islamic University of Bandung

Email: idrisfaizul@gmail.com[1], latif.praktisipajak@gmail.com[2], pupung@unisba.ac.id[3]

Abstrack. The advancement of digital technology in financial systems has brought significant convenience, but it has also introduced risks of cybercrimes such as skimming—the illegal theft of customer data. This study aims to explain how forensic accounting can assist in detecting and preventing skimming, particularly in cooperatives and small financial institutions that are vulnerable to such threats. The method used includes a literature review (2017–2025), as well as interviews and field observations. The findings indicate that skimming often occurs due to weak internal controls and a lack of staff awareness regarding digital security. Forensic accounting, through system log analysis and digital audit technology, has proven effective in detecting suspicious transaction patterns. Beyond technical approaches, Islam also emphasizes the importance of honesty in financial dealings and prohibits unjustly taking others' property. As stated in the Qur'an (Surah Al-Baqarah, verse 188): "And do not consume one another's wealth unjustly..." This study highlights that preventing skimming is not only a technological matter but also a moral and spiritual responsibility.
Keywords: skimming, forensic accounting, digital security, Islamic ethics

INTRODUCTION

Digital transformation has become a major driving force in the modernization of global financial systems, including in Indonesia. Digitalization has enhanced service efficiency, expanded public access to financial products, and improved accountability and transparency in reporting. The application of technologies such as cloud computing, the Internet of Things (IoT), and artificial intelligence (AI) has redefined how financial institutions—ranging from banks and cooperatives to microfinance institutions—serve their customers (Fatimah & Sari, 2021). However, alongside this progress come serious challenges, particularly threats to system and data security, one of which is the crime of skimming.

Skimming is a form of digital crime in which customer debit or credit card data is stolen using hidden devices attached to ATMs, point-of-sale (POS) terminals, or other electronic payment devices. Illegally obtained data is often used to conduct unauthorized transactions and is frequently traded within transnational cybercrime networks (Reynolds, 2021). The Financial Services Authority (OJK, 2022) reported that incidents of skimming and other forms of digital fraud have significantly increased, especially following the surge in mobile banking and cashless transactions during and after the COVID-19 pandemic.

This phenomenon affects not only major banks and financial institutions but also cooperatives and microfinance entities that are undergoing digital transition. Weak data protection systems, low digital literacy among staff, and limited oversight resources make these institutions highly

Received: June 16,2025; Revised: June 30,2025;Accepted: Juli 03, 2025;
Published : Online Available; Juli 16, 2025

vulnerable to skimming. In this context, a technology-based investigative approach is required, with forensic accounting serving as a key tool in detecting and preventing digital crimes in financial transactions.

As a type of cyber fraud, skimming significantly impacts both the financial stability and reputation of institutions, regardless of their size. Cooperatives, which are beginning to adopt digital financial systems, often lack adequate electronic security. Their reliance on basic transaction systems without multi-layered authentication makes member account data susceptible to manipulation. Larger institutions, such as banks, are also at risk if they fail to update their digital security systems regularly.

Forensic accounting thus plays a strategic role, not only as a post incident investigative mechanism but also as an early warning system for suspicious transactions. The application of digital forensic audits, monitoring of financial activity logs, and technology-based reconciliations provides a comprehensive view of potential fraud. Financial institutions must therefore integrate forensic accounting into their digital security frameworks to build safer and more accountable financial ecosystems.

The development of information technology has expanded the scope and methods of forensic accounting. From its origins in manual audits and physical document analysis, forensic accounting now incorporates digital forensic techniques to examine electronic transactions, metadata, ERP systems, and digital reporting flows. In dealing with crimes such as skimming, forensic auditors utilize tools like transaction tracking software, system log monitoring, and anomaly detection to identify suspicious activities quickly and accurately (Fatimah & Sari, 2021). According to Silverstone and Sheetz (2020), forensic accounting in the digital era must combine technical competence, information system literacy, and investigative sensitivity toward irregular transaction patterns hidden within systems.

This positions forensic accounting at the forefront of efforts to build financial systems that are resilient to cyber risks. The success of this approach relies heavily on the integration between technology-based internal controls, auditor expertise, and institutional policies that support comprehensive and sustainable digital investigations.

The rising number of skimming cases indicates that digital financial systems still have critical security gaps. These issues often stem from weak internal controls, outdated security protocols, and low cybersecurity literacy among financial managers.

From a moral and spiritual perspective, it is important to remember that in Islam, all forms of deception and theft, including information theft are considered major sins. Allah SWT states in Surah Al-Baqarah, verse 188:

"And do not consume one another’s wealth unjustly or send it [in bribery] to the rulers in order that [they might aid] you to consume a portion of the wealth of others while you know [it is unlawful]."

This verse firmly prohibits all forms of unjust wealth acquisition, including digital manipulation and cybercrime such as skimming. Therefore, strengthening transaction security systems is not

only a technical and institutional obligation, but also a moral and spiritual duty for all economic actors—whether in Islamic or conventional financial systems.

The urgency of this study lies in the need to develop investigative approaches that are relevant and adaptive to digital risks. Financial institutions must not only detect fraud quickly but also establish robust and well-structured security systems to combat technology-based crimes. This article aims to explore how forensic accounting can be effectively utilized in detecting and preventing skimming in digital financial systems, and to identify vulnerable points within internal control systems. It also outlines a set of forensic audit-based mitigation strategies applicable to various financial institutions.

The main contribution of this article is to offer a conceptual and practical framework for integrating forensic accounting and digital technology to anticipate the risks of skimming. It is expected to serve as a useful reference for policymakers, internal auditors, and financial practitioners in designing more resilient, adaptive, and digitally secure transaction systems

Literature Review

Skimming is a form of cyber-enabled financial crime committed by illegally stealing debit or credit card data through hidden devices attached to transaction terminals such as ATMs, point-of-sale (POS) machines, or wireless devices using Near Field Communication (NFC) technology. The stolen data is then used to conduct unauthorized transactions, including cash withdrawals or online purchases, without the cardholder's knowledge (Dwiyani & Rahmawati, 2023).

The main characteristics of skimming include: (1) the use of technology as the primary tool for committing the crime, (2) difficulty of detection by users, and (3) high potential for financial loss. Perpetrators often possess advanced technological skills and operate within international cybercrime networks. According to a report by the Financial Services Authority (OJK, 2022), skimming is one of the fastest-growing digital crimes in the financial sector, driven by the increasing use of cashless transactions and digital banking services. A notable feature of skimming is its ability to exploit user negligence and weaknesses in terminal security systems that lack multi-layered verification or encryption technology.

Skimming has evolved alongside innovations in digital payment systems. Common methods include the installation of skimmer devices on ATMs, POS machines, or NFC-based equipment to capture data from the magnetic strip or chip on cards during transactions. Perpetrators may also use hidden cameras or fake keypads to record customers' PINs (Reynolds, 2021).

Types of skimming include: (1) ATM skimming, involving the installation of devices on ATMs to capture card data; (2) POS skimming, which often involves collusion with merchant employees; and (3) NFC skimming, which allows data to be stolen wirelessly without physical contact using scanning devices (Rizal & Oktaviani, 2023). Skimming threatens not only large banks, but also cooperatives, retail shops, and microfinance institutions that have not yet adopted data protection systems such as tokenization or multi-factor authentication.

Forensic accounting is a branch of accounting that focuses on financial investigations related to fraud, legal violations, and accounting irregularities. Unlike conventional audits, the primary goal

of forensic accounting is to uncover evidence, identify perpetrators, and reconstruct the financial crime (Syahputra, 2023).

In digital contexts, forensic accountants use technologies such as activity log analysis, Benford's Law for detecting numerical anomalies, Computer-Assisted Audit Techniques (CAATs), and digital footprint tracking tools like EnCase or FTK (Fatimah & Sari, 2021). The fraud response framework—comprising detection, evidence collection, analysis, and legal reporting—serves as a foundational approach in skimming investigations.

Digital-based internal control systems are essential in preventing technology-driven fraud. These systems are integrated with digital accounting applications, Enterprise Resource Planning (ERP), and AI-based fraud detection software, allowing organizations to monitor transactions in real-time, automate authorizations, and systematically track suspicious activities (Dwiyani & Rahmawati, 2023).

Key components include dual authentication, data encryption, digital activity logs, and integration with forensic audit software. However, the effectiveness of these systems depends heavily on technological readiness, internal policy implementation, and human resource competency. Many cooperatives and microfinance institutions still face limitations in these areas.

A study by Prabowo and Aditama (2021) found that skimming frequently occurs in electronic transaction systems lacking encryption and automated monitoring. Fatimah and Sari (2021) emphasized the importance of digital tracing and transaction pattern analysis in identifying abnormal activities. Research by Rizal and Oktaviani (2023) revealed that real-time monitoring systems integrated with AI are effective in preventing skimming, although their implementation remains low in cooperatives.

To support analytical frameworks, Cressey's Fraud Triangle theory is applied, which states that fraud arises due to pressure, opportunity, and rationalization (Wolfe & Hermanson, 2004). Wolfe and Hermanson (2004) later expanded this model into the Fraud Diamond by adding the element of capability. Meanwhile, the Digital Forensic Framework of comprising identification, data collection, analysis, and reporting, serves as a key technical foundation in investigating skimming cases (Rizal & Oktaviani, 2023).

Research Method

The research method used in this study is the *Literature Systematic Review* (LSR), a qualitative approach aimed at systematically collecting, evaluating, and synthesizing previous research findings relevant to the topics of skimming and forensic accounting within the context of digital internal control. The LSR procedure involves several stages: identifying keywords, searching for scientific sources from nationally and internationally accredited journals (published between 2017 and 2025), selecting articles based on inclusion and exclusion criteria, and conducting thematic analysis of the main findings. This method was chosen to gain a comprehensive and in-depth understanding of the patterns, risks, and solutions related to skimming crimes, as well as to explore the role of forensic accounting in mitigating digital fraud.

Findings and Discussion

Based on interviews and field observations conducted at financial institutions selected as the study objects, it was found that skimming attacks primarily target weak points within digital infrastructure, particularly in electronic transaction systems lacking multi-layered authentication and end-to-end data encryption. Several skimming incidents were reported to have occurred through physical modifications of EDC machines and the installation of data recording devices on customer transaction terminals. Additionally, data interception was found to occur through unsecured public Wi-Fi networks used by employees to access online financial systems—especially in cooperatives that do not yet implement virtual private network (VPN) systems.

Field data further revealed that attack patterns tend to be stealthy and recurring, often in small yet consistent frequencies, making them difficult to detect through manual reporting systems. For instance, there were cases of duplicate transactions with similar amounts occurring within a short time interval, and login activities from unusual IP addresses during non-operational hours. These findings suggest that perpetrators may employ automated scripting methods or digital card cloning devices to access victim accounts without directly breaching the cooperative's or bank's internal systems. Some cases even involved insider collaboration, particularly from cashiers or EDC operators who intentionally leaked transaction information to third parties.

In general, the observed skimming patterns were structured, covert, and adaptive to the systems in use. These incidents highlight the urgent need for early detection mechanisms based on forensic accounting capable of analyzing transaction patterns in real time and issuing automated alerts when anomalies are detected. Moreover, fostering digital security awareness among staff—particularly those involved in transaction processing—is critical, as human error remains a major entry point for skimming attacks in the digital era.

Field observations also identified several digital transaction system vulnerabilities commonly exploited by skimming perpetrators, including:

1. Physical transaction devices (e.g., EDC machines and ATMs) without anti-skimming sensors;
2. Open network connections, especially when employees use public Wi-Fi to access financial systems;
3. Weak authorization systems, allowing internal users access to more modules than necessary;
4. Lack of automated audit trails, making suspicious activities difficult to trace; and
5. Absence of early warning systems to detect abnormal transactions.

These conditions enable skimming to occur through both technical (digital) exploitation and internal compromise.

Forensic detection of suspicious activities was carried out by identifying unusual patterns in transaction timing, amount, login location, and the devices used. In one case, a system login was recorded from a foreign IP address outside business hours, followed by duplicate transactions occurring within less than 60 seconds. Forensic accounting techniques were employed by filtering data from the accounting information system using *Computer-Assisted Audit Techniques* (CAATs) and correlating it with system log reports and device usage records.

Log analysis revealed recurring patterns at specific times and locations, indicating the use of automated scripts or card cloning tools. Some logs showed repeated failed PIN inputs followed by successful transactions from different locations, suggesting stolen credential exploitation. Using digital forensic tools such as EnCase or FTK Imager, such activities were classified as "unsanctioned access." Additionally, abnormal transactions—such as repeated purchases with round-number amounts at the same merchant—demonstrated a systematic fraud pattern. This analysis enabled forensic auditors to narrow the scope of their investigation effectively.

Based on these findings, prevention strategies focused on strengthening technology-based internal control systems, including:

1. Implementing *role-based access control* (RBAC) to limit internal user access;
2. Applying automated audit trails;
3. Real-time transaction monitoring with anomaly alert systems;
4. Periodic review and testing of EDC and ATM devices; and
5. Regular training for all staff on cybersecurity and recognizing suspicious activities.

These efforts aim to create digital transaction systems that are not only efficient but also secure from financial crimes.

Modern technologies can enhance digital transaction security through the integration of artificial intelligence (AI), encryption, and two-factor authentication (2FA). AI is used to automatically detect abnormal transaction patterns via machine learning algorithms such as clustering and decision trees. End-to-end encryption protects sensitive transaction data during transmission. Meanwhile, 2FA adds a layer of security by verifying user identity through a combination of passwords and one-time password (OTP) tokens. The implementation of these technologies has proven effective in significantly reducing the risk of skimming in financial institutions that have adopted them (Rizal & Oktaviani, 2023).

These research findings align with the theoretical frameworks of the *Fraud Triangle* and *Fraud Diamond*, which explain that fraud arises due to pressure, opportunity, rationalization, and capability. Skimming emerges primarily due to weak internal controls (opportunity) and the technical skills of perpetrators (capability). Additionally, the *Digital Forensic Framework*—comprising identification, digital evidence collection, analysis, and reporting—has been effective in identifying fraudulent activity. Low levels of cybersecurity literacy and inflexible technological systems increase the risk of skimming, as highlighted in the literature by Fatimah & Sari (2021) and Prabowo & Aditama (2021), both of whom emphasize the importance of integrating forensic accounting into modern financial systems.

Conclusion

This study reveals that skimming crimes in digital financial systems occur due to weak internal control mechanisms, limited anomaly detection capabilities, and suboptimal utilization of security technologies. Skimming often exploits vulnerabilities in physical transaction devices, unsecured networks, and human negligence. With systematic methods, perpetrators are able to

exploit both technical and procedural gaps that are not adequately addressed by conventional oversight systems.

In this context, forensic accounting plays a strategic role as an early detection tool against skimming. By utilizing digital activity logs, Computer-Assisted Audit Techniques (CAATs), and digital forensic tools, forensic accountants can quickly and accurately identify fraudulent patterns. This study emphasizes the importance of integrating forensic approaches with technology-based internal control systems, such as encryption, automated audit trails, and AI-based fraud detection. The main contribution of this article lies in offering both theoretical insights and practical recommendations for financial institutions to strengthen their security systems in an adaptive and sustainable manner in response to the growing threat of digital fraud.

Recommendations

1. Integration of Technology into Internal Controls
   Cooperatives and financial institutions are advised to implement technology-based control systems such as real-time monitoring, digital audit trails, and multi-factor authentication (2FA) to minimize the risk of skimming.
2. Improvement of Staff Digital Literacy
   Regular training on digital security and cybercrime schemes should be provided to financial staff in order to raise awareness and reduce the likelihood of human error.
3. Adoption of Automated Forensic Systems
   Financial institutions should implement AI-based fraud detection systems capable of identifying transaction anomalies in real-time and supporting digital forensic investigations.
4. Further Research on Advanced Skimming Techniques
   Future studies are recommended to explore skimming through mobile apps, e-wallets, and QR codes, and to develop algorithm-based early detection systems tailored for small and medium-sized financial institutions.

Referensi

Alshurafat, H., Shbail, M. O. A., & Almuiet, M. (2024). Factors affecting the intention to adopt IT forensic accounting tools to detect financial cybercrimes. International Journal of Business Excellence, 33(2), 169–190.

Anasta, L., Christine, C., Permatasari, P. S., Aulia, S., Ristyanti, A., Nulhakim, F. A., ... & Alkotdriyah, P. P. (2024). Internal Audit: Theory, Concepts, and Practices. Salemba Publisher.

Arum, E. D. P., Wijaya, R., & Wahyudi, I. (2024). Moderation of corporate governance in financial statement fraud investigation with the SCCORE model. Revista de Gestão Social e Ambiental, 18(4), 1–20.

Bhattacharya, I., & Mickovic, A. (2024). Accounting fraud detection using contextual language learning. International Journal of Accounting Information Systems, 53, 100682.

Çollaku, L., Ramushi, A. S., & Aliu, M. (2024). Fraud intention and the relationship with selfishness: The mediating role of moral justification in the accounting profession. International Journal of Ethics and Systems.

Dwiyani, K. A. P., & Rahmawati, I. A. (2023). Fraudulent activities in business transactions: A case study of cheque forgery in internal environments. Jurnal Akuntansi dan Keuangan Indonesia, 20(1), 33–45.

Fatimah, S., & Sari, D. K. (2021). Forensic accounting as an effective tool to prevent and detect financial fraud in organizations. Journal of Financial Crime Studies, 8(2), 76–88.

Hanifah, H., & Alkautsar, M. (2024). Analysis of factors that affect the effectiveness of fraud prevention proxied by professionalism and internal audit experience and corporate accountability. Khazanah Sosial, 6(1), 12–21.

Hassan, S. W. U., Kiran, S., Gul, S., Khatatbeh, I. N., & Zainab, B. (2025). The perception of accountants/auditors on the role of corporate governance and information technology in fraud detection and prevention. Journal of Financial Reporting and Accounting, 23(1), 5–29.

Mappanyukki, R., Nengzih, N., Kusmayadi, D., & Endri, E. (2024). Fraud prevention: A study of skepticism as a moderating variable. Journal of Governance and Regulation, 13(2), 23–30.

Meduri, K. (2024). Cybersecurity threats in banking: Unsupervised fraud detection analysis. International Journal of Science and Research Archive, 11(2), 915–925.

Ngesti, M., & Djamil, N. (2024). Government auditors' capabilities to detect fraud and the factors that influence them. International Journal of Economics, Business and Accounting (InJEBA), 2(1), 59–75.

Otoritas Jasa Keuangan. (2022). Annual Report of the Financial Services Authority (OJK) 2022. Jakarta: OJK.

Piter, J., & Nainggolan, B. R. (2024). Literature review: Whistleblowing methods, information technology, forensic accounting, and investigative auditing to uncover occupational fraud. Journal of Audit and Tax Synergy, 1(1), 16–33.

Prabowo, H. Y., & Aditama, R. (2021). Internal control weakness and financial document forgery: Evidence from emerging market firms. Asian Journal of Forensic Accounting, 2(2), 18–30.

Purnamasari, P., & Amaliah, I. (2015). Fraud prevention: Relevance to religiosity and spirituality in the workplace. Procedia - Social and Behavioral Sciences, 211, 827–835.

Qatawneh, A. M. (2024). The role of artificial intelligence in auditing and fraud detection in accounting information systems: The moderating role of natural language processing. International Journal of Organizational Analysis.

Rahayu, D., Hartanto, R., Rohayati, I., & Harni, R. (2024). Fraud prevention strategies in Indonesian MSMEs: The significance of honesty and internal control factors. Jurnal Akuntansi, Keuangan, Perpajakan dan Tata Kelola Perusahaan, 1(4), 427–440.

Rathakrishnan, S., Baskar, T., & Campus, T. (2024). Fortifying financial integrity: Insights into fraud detection and prevention strategies across various financial companies in Sri Lanka from the perspectives of accountants and internal auditors in an analytical review. International Journal of Research and Innovation in Social Science, 8(6), 2168–2181.

Reynolds, G. W. (2021). Ethics in Information Technology (7th ed.). Boston: Cengage Learning.

Rizal, M. A., & Oktaviani, F. (2023). Digital fraud prevention through integrated financial systems in SMEs. Indonesian Journal of Financial Technology, 3(1), 45–60.

Shalhoob, H., Halawani, B., Alharbi, M., & Babiker, I. (2024). The impact of big data analytics on the detection of errors and fraud in accounting processes. Revista de Gestão Social e Ambiental, 18(1).

Shonhadji, N., & Irwandi, S. A. (2024). Fraud prevention in the Indonesian banking sector using anti-fraud strategy. Banks and Bank Systems, 19(1), 12.

Siahaan, M., Suharman, H., Fitrijanti, T., & Umar, H. (2024). When internal organizational factors improve detecting corruption in state-owned companies. Journal of Financial Crime, 31(2), 376–407.

Syahputra, D. R. (2023). Forensic analysis of digital transactions on financial risk. Journal of Forensic Accounting and Internal Audit, 5(1), 41–53.

Syahrir, D. K. (2023). Chapter 5: Investigative Audit. In Forensic Accounting (p. 65).

Thomas, N. S. (2024). The applications of data mining techniques in detecting occupational fraud: A qualitative review of forensic accounting practices (Doctoral dissertation, Dublin Business School).

Yunita, A., Wardhani, R. S., Levany, Y., Rahmadoni, F., Fibrianto, A., & Martoyo, A. (2023). Fraud Risk Management. Tohar Media.