aml/cft journal
journal of anti-money laundering / countering the financing of terrorism

Original paper

Cybersecurity Trends and the Evolution of Fraud in the Banking Sector in the Digital Era

Jum'an[1]*, Muhammad Asyura[2]
[1] Faculty of Islamic Economics and Business, Sultan Muhammad Syafiuddin Sambas Islamic Institute, Indonesia
[2] Politeknik Negeri Sambas, Indonesia

Corresponding author: juman.sambas123@gmail.com

Keywords:
Banking, Cybersecurity, Fraud, Social media

Abstract

The digital transformation of the banking sector has significantly optimized financial service efficiency. However, it has concurrently expanded the risks of cybercrime and fraud. Financial crimes in banking are no longer restricted to internal malfeasance, they increasingly involve external adversaries exploiting both technological vulnerabilities and human behavioral lapses. This study interrogated contemporary cybersecurity trends and the evolution of fraud modalities within the digital banking landscape. Adopting a qualitative Systematic Literature Review (SLR), this research synthesizes relevant scientific literature through the dual lenses of the CIA Triad framework and fraud theories. The findings identify a multifaceted threat landscape, ranging from ransomware and remote-work vulnerabilities to cloud-based incursions, supply chain attacks. It also targeted social engineering, such as phishing and whaling. Notably, the study highlights that social engineering remains the dominant fraud modality, exploiting the 'human element' as the critical vulnerability in security architectures. These results highlight that cybersecurity and fraud are inextricably linked. They require an integrated mitigation strategy that harmonizes technological safeguards, robust business processes, and human capital development to fortify digital banking resilience.

Submitted: 14 August 2024
Accepted: 6 December 2025
Published: 6 December 2025

***To cite this article*:** Jum'an. 2025. *Cybersecurity Trends and the Evolution of Fraud in the Banking Sector in the Digital Era. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 4(1):1-12, https://doi.org/10.59593/amlcft.2025.v4i1.225

Introduction

In today's rapidly evolving regulatory landscape, financial institutions remain at the forefront of efforts to combat increasingly complex and sophisticated financial crimes. The challenges faced by financial institutions entering 2024 demand the adoption of proactive and adaptive approaches to risk management. Financial crimes have progressed from traditional schemes to encompass digital methods, cyber threats, and various forms of fraud. These risks compel financial institutions to re-evaluate their financial systems and prioritize sound banking risk management as well as the integrity of the financial system.

As a vital sector in society, the banking industry is inherently vulnerable to abuses of power and criminal activities, whether committed by internal actors or external parties seeking to

exploit the system for personal gain or illicit purposes. Criminal behavior within banking activities often involves violations of formal regulations, commonly referred to as banking crimes. Consequently, ensuring the security of banking systems is essential for protecting financial information and assets from such threats.[1]

In the current era, where technological development is advancing rapidly, significant changes to social, economic, and cultural dimensions have become inevitable. However, behind these advancements lie various risks, including the spread of viruses, software piracy, and attacks targeting digital services. Cyberattacks, often involving perpetrators and victims across different countries have emerged as a serious form of transnational crime. These developments have likewise created opportunities for individuals or groups to launch attacks on technological systems. Cybercrime represents a new category of criminal offense that has arisen as a direct consequence of the evolution of information technology.[2]

Financial crime is a broad term encompassing any form of criminal conduct connected to financial entities and markets, including banks, fintech companies, lending institutions, and similar organizations. One category of financial crime that has become increasingly prevalent toda and has raised significant concern among industry stakeholders, the government, and the public is the growing trend of sophisticated financial offenses within the modern financial ecosystem.[3]

The banking sector faces a range of challenges in addressing the continually evolving threat of cyberattacks. One of the principal challenges lies in the increasingly sophisticated role of technology, which enables cybercriminals to develop new methods for targeting banking systems. In addition, the lack of awareness regarding the importance of data security, both within banking institutions and among customers, further exacerbates this situation. At the same time, banks must ensure smooth operational processes and uninterrupted services to customers without compromising the protection of sensitive data. In light of these challenges, the banking sector must adopt innovative solutions to strengthen its cybersecurity framework.[4]

In confronting cyberattacks, the banking sector inevitably bears significant consequences. Cyberattacks targeting the financial sector, particularly banking, occur nearly three times more frequently than those in other industries. The motives driving cybercriminals are diverse. Some attackers act out of mere mischief, while others engage in financially motivated crimes, using the proceeds for various purposes ranging from personal gain to funding political activities.

Cyberthreats cannot be ignored in today's digital era, where the financial industry is increasingly interconnected. It is therefore essential to recognize the methods employed in cybercrime and the strategies needed to mitigate them in order to protect personal and business interests from such threats. As key actors within the financial industry, banks must maintain heightened vigilance toward cyber risks, especially as fraud involving social engineering has become increasingly widespread in parallel with the growing use of social media.

Cybersecurity refers to the full set of protective measures implemented to minimize disruptions to the availability, integrity, and confidentiality of information. Data confidentiality

[1] Nida Rafa Arofah and Yeni Priatnasari, "Internet Banking dan Cyber Crime: Sebuah Studi Kasus di Perbankan Nasional," *Jurnal Pendidikan Akuntansi Indonesia* 18, no. 2 (2020): 107–19, https://doi.org/10.21831/jpai.v18i2.35872.

[2] Ervina Chintia et al., "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya," *JIEET (Journal of Information Engineering and Educational Technology)* 2, no. 2 (2018): 65–69, https://doi.org/10.26740/jieet.v2n2.p65-69.

[3] Anisyah Nur Radiyah and Abshoril Fithry, "Kejahatan Keuangan pada Tindak Pidana Money Laundering dalam Menghilangkan Jejak Kejahatan," *Prosiding SNAPP: Sosial Humaniora, Pertanian, Kesehatan dan Teknologi* 2, no. 1 (2023): 39–45, https://doi.org/10.24929/snapp.v2i1.3179.

[4] Eka Febriantika Nur Afifah, Diny Widya Evriyanti Simatangkir, and Nafiza Salsabila Faliha, "Keamanan Siber dalam Perbankan serta Tantangan dan Solusi Di Era Digital," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 33–42, https://doi.org/10.61722/jmia.v2i1.3119.

pertains to authorized access to information, meaning that only individuals with legitimate permission may view or use it. Any attempt to obtain access by stealing information is considered an act that compromises data confidentiality.[5]

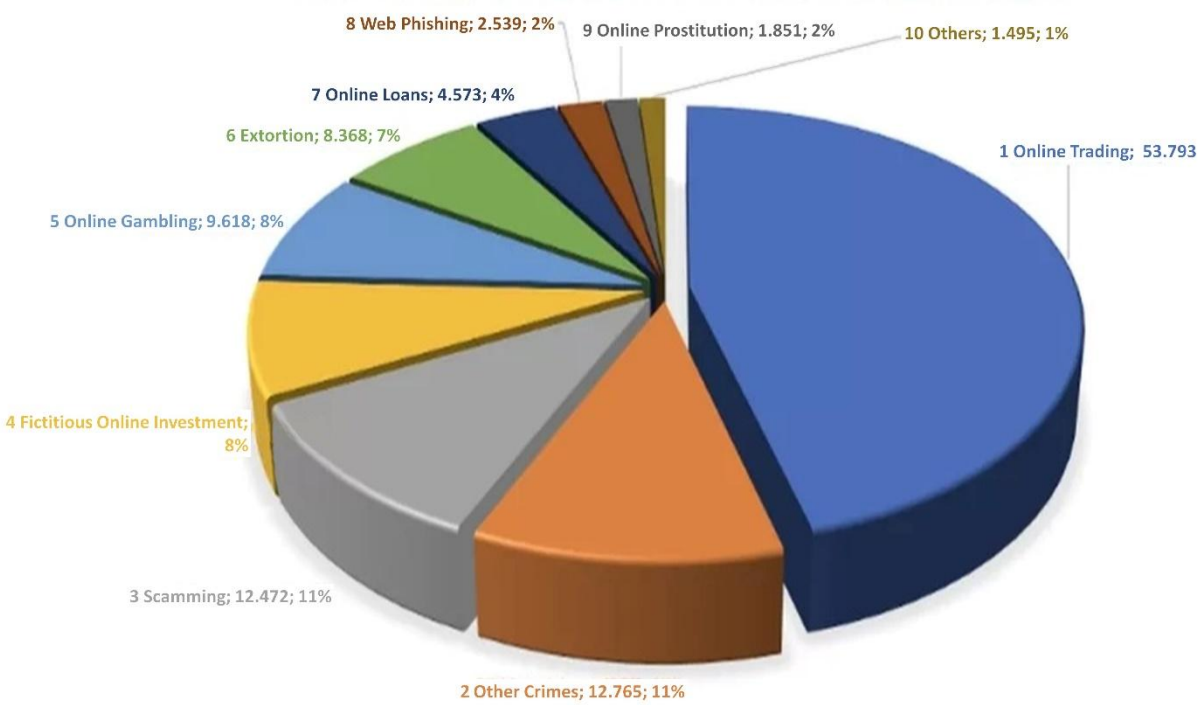

Figure 1. Cybercrime Statistics in Indonesia for 2023
Source: BSNN (2023)

Figure 1 illustrates that the most frequently reported activity, and the primary arena for cybercrime is online trading, which ranks first with 53,793 incidents, accounting for 45.87% of all reports. This is followed by scamming, ranking second with 12,472 incidents or 10.63%. Fictitious online investment schemes, often disguised as freelance job opportunities that lure job seekers and subsequently deceive victims into transferring money with the promise of large profits, rank third with 9,618 reports or 8.36%. Next is online gambling, with 8,364 incidents or 7.13% of total reports. Meanwhile, cases involving extortion by debt collectors account for 4,573 incidents or 3.90%.[6]

As fraud threats and financial crimes targeting the banking sector continue to escalate rapidly driven by digital advancements, banking institutions must be prepared to deliver a comprehensive response. Such responses must reinforce strong security measures encompassing personnel, business processes, and technology. A public report issued by GBG (GB Group plc) in collaboration with Chartis Risk indicates that Indonesia ranks highest globally in money mule activity (fraudulent transfer schemes) and identity theft, accounting for 67% of cases. The GBG and Chartis Risk report underscores that fraud cases continue to evolve

[5] Nikola Schmidt, "Critical Comments on Current Research Agenda in Cyber Security," *Obrana a Strategie* 14, no. 1 (2014): 29–38.

[6] Wahyu Subyanto, "Statistik Kejahatan Siber Indonesia 2023, Jual Beli Online Terbanyak Penipuan," nextren.grid.id, last modified November 27, 2023, https://nextren.grid.id/read/013955948/statistik-kejahatan-siber-indonesia-2023-jual-beli-online-terbanyak-penipuan?page=all.

and transform. Indonesia has become a major target due to its expanding digital product market and high level of financial inclusion, which is projected to reach 90% by 2024.[7]

Fraud refers to an act, omission, concealment, or misleading representation that deceives another person and results in harm or loss to the victim.[8] The Association of Certified Fraud Examiners (ACFE) defines fraud as a deceptive act or misrepresentation committed by an individual or entity with the knowledge that such misconduct may result in an improper benefit to themselves or to another party.[9]

In the business and information technology environment, fraud constitutes a serious and pervasive issue. One of the most widely used frameworks for understanding the occurrence of fraud is the Fraud Triangle, introduced by Donald Cressey (1973). This theory explains that fraud arises when three key factors coexist: pressure, or the motivation compelling an individual to commit fraud; opportunity, or the circumstances that enable the misconduct to occur without easy detection; and rationalization, which allows the individual to justify or legitimize their unethical actions.[10]

With the continuous evolution of information technology, protecting data and systems has become increasingly essential. The concept of information security is commonly represented by the CIA Triad, which consists of confidentiality, integrity, and availability.[11] Confidentiality ensures that information is accessible only to authorized parties; integrity guarantees that data remain accurate, consistent, and unaltered; and availability ensures that information and systems are accessible when needed. These three principles serve as the foundation for developing security policies, procedures, and technologies within organizations across various sectors.

In the context of digital crime, organizations face risks that may result in significant losses. The digital crime risk model emphasizes the importance of understanding three key components: threat, vulnerability, and impact. A threat refers to any factor capable of harming an information system; vulnerability is a weakness that enables a threat to materialize; while impact describes the losses incurred when a threat is realized.[12] Risk itself represents a combination of the likelihood of a threat occurring and the magnitude of the impact it generates. Understanding this model enables organizations to conduct effective risk assessments and design appropriate controls to prevent or mitigate digital crime.

A substantial body of research on cybersecurity and banking fraud in the digital era, both globally and locally has strengthened insights into digital crime mechanisms and mitigation strategies.

Naam (2013) conducted research specifically on defending against malware attacks by identifying malware pathways and classifications. The aim of the study was to propose solutions to malware attacks by analyzing how malware operates and determining steps to mitigate the

[7] Imam Suhartadi, "Survei GBG: RI Duduki Peringkat Teratas Kasus Money Mule dan Pencurian Identitas," Investor.Id, last modified August 5, 2024, https://investor.id/business/369245/survei-gbg-ri-duduki-peringkat-teratas-kasus-money-mule-dan-pencurian-identitas.

[8] Daniel T. H. Manurung and Andhika Ligar Hardika, "Analysis of Factors that Influence Financial Statement Fraud in the Perspective Fraud Diamond: Empirical Study on Banking Companies Listed on the Indonesia Stock Exchange Year 2012 to 2014," *International Conference on Accounting Studies (ICAS) 2015* (2015): 280–86, https://doi.org/10.13140/RG.2.1.2058.8563.

[9] Ernst and Young, *Detecting Financial Statement Fraud: What Every Manager Needs to Know* (London: E & Y LLP, 2009).

[10] Donald R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement* (Montclair, NJ: Patterson Smith, 1973).

[11] M. E. Whitman and H. J. Mattord, *The CIA Triad: Confidentiality, Integrity, and Availability*, 4th ed. (Waltham, MA: Elsevier/Morgan Kaufmann, 2017).

[12] Gary Stoneburner, Alice Goguen, and Alexis Feringa, "Risk Management Guide for Information Technology Systems," *NIST Special Publication* 800, no. 30 (2002): 800–830.

effects of malware infection on computer systems.[13] Faridi (2018) investigated cybercrime within the banking sector. The goal of this research was to identify various types of banking crimes and formulate preventive and corrective measures to combat criminal activities in banking.[14] Meliana and Hartono (2019) carried out an exploratory study on banking fraud in Indonesia. Their research aimed to examine in depth the motivations behind banking crime offenders in Indonesia.[15] Setiawan and Wahyudi (2023) explored fraud prevention in cybercrime affecting the banking sector. Their study sought to explain the realities of cybercrime cases in internet banking in Indonesia and to provide preventive alternatives to minimize cybercrime in online banking.[16] The study by Alodhiani (2023), titled A Systematic Literature Review on Financial Technology (Fintech) and Cybersecurity, aimed to identify cyber threats within the financial sector as well as security measures that financial institutions can adopt.[17] Research conducted by Nur Afifah, Simatangkir, and Faliha (2023) affirms that malware, phishing, and Distributed Denial of Service (DDoS) attacks constitute significant and ongoing threats to digital banking in Indonesia.[18]

Syahraeni et al. (2024) examined fraud cases in Sharia banking through an analysis of internal fraud and its implications for customer trust. The study aimed to identify the factors contributing to fraud and to evaluate the effectiveness of internal control systems and anti-fraud policies implemented by the institution.[19] Balaka et al. (2024) conducted research on customer data theft in the banking sector, identifying it as a serious threat in the digital era. Their study aimed to analyze the modus operandi of cybercrime related to the theft of customer data in the banking industry, as well as preventive measures taken to combat cyber-based data theft.[20] Azzahra et al. (2024) performed a literature study on cybercrime threats and cybersecurity implementation within the banking sector. The research sought to identify major cyber threats, evaluate existing security measures within banks, and recommend strategies to enhance cybersecurity capabilities.[21] Munajat and Yusuf (2024) investigated the role of information technology in preventing and uncovering economic crimes, focusing specifically on digital financial offenses. Their study reviewed the role of technologies such as artificial intelligence (AI), big data analytics, and blockchain in detecting suspicious activities within the financial sector.[22]

[13] Jufriadif Naam, "Metoda Pertahan Diri Program Virus," *Jurnal PROCESSOR* 8, no. 2 (2013): 36.

[14] Muhammad Khairul Faridi, "Kejahatan Siber dalam Bidang Perbankan," *Cyber Security dan Forensik Digital* 1, no. 2 (2018): 57–61, https://doi.org/10.14421/csecurity.2018.1.2.1373.

[15] Meliana Meliana and Trie Rundi Hartono, "Fraud Perbankan Indonesia: Studi Eksplorasi," *Prosiding Seminar Nasional Pakar* 1, no. 1 (2019): 2521–27, https://doi.org/10.25105/pakar.v0i0.4335.

[16] Nanang Setiawan and Imam Wahyudi, "Pencegahan Fraud pada Kejahatan Siber Perbankan," *Kabillah : Journal of Social Community* 8, no. 1 (2023): 508–18, https://doi.org/10.35127/kabillah.v8i1.280.

[17] Ahmed Abdulrhman B. Alodhiani, "Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review." *Arab Journal for Humanities and Social Sciences*, no. 20 (2023), https://doi.org/10.59735/arabjhs.vi20.55.

[18] Afifah, Simatangkir, and Faliha, "Keamanan Siber dalam Perbankan Serta Tantangan dan Solusi di Era Digital."

[19] Syahraeni Syahraeni, Nur Hikmah, and Sitti Nikmah Marzuki, "Kasus Penipuan di Perbankan Syariah: Analisis Fraud Internal dan Implikasinya terhadap Kepercayaan Nasabah," *Lan Tabur: Jurnal Ekonomi Syariah* 6, no. 1 (2024): 122–40, https://doi.org/10.53515/lantabur.2024.6.1.122-140.

[20] Kemal Idris Balaka, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany, "Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital," *Yustitiabelen* 10, no. 2 (2024): 105–30, https://doi.org/10.36563/yustitiabelen.v10i2.1167.

[21] Nasywa Shafa Azzahra et al., "Tinjauan Literatur Tentang Ancaman Cybercrime dan Implementasi Keamanan Siber di Industri Perbankan," *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis* 2, no. 7 (2024): 692–700.

[22] Andi Ahmad Munajat and Hudi Yusuf, "Peran Teknologi Informasi dalam Pencegahan dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi tentang Kejahatan Keuangan Berbasis Digital," *Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): 4853–65.

A systematic study by Waliullah et al. (2025) demonstrated that cyber threats such as phishing, malware, and ransomware are key factors influencing the adoption and growth of digital banking services.[23] The study emphasizes the importance of implementing security technologies such as multi-factor authentication (MFA) and biometrics. Similarly, George et al. (2025), through a review of 118 related studies, found that the use of machine learning, particularly supervised and deep learning approaches, has become increasingly effective in detecting emerging fraud patterns, although real-time implementation remains a significant challenge.[24]

Several previous studies reveal a research gap that forms the foundation of this study, namely, the separation of focus between cybersecurity research and financial fraud research. Earlier studies generally highlight only one of these aspects, either cybersecurity or financial fraud, without integrating the two systematically within the banking context. There is also a lack of research examining the trends and evolution of digital fraud schemes in the era of modern banking. Most existing studies still discuss traditional fraud cases or conventional security systems and have not yet adapted to the increasingly complex and automated attack patterns of today. Furthermore, previous research often lacks empirical and multidimensional approaches. Many studies remain conceptual or purely literature-based, and do not explore the interrelationship between security technologies, offender behaviors, and the effectiveness of cybersecurity defenses in the banking sector. To date, there is no conceptual model or analytical framework that connects cybersecurity, fraud behavior, and customer trust. Accordingly, this study differs significantly from prior research because it not only examines cybersecurity and fraud as separate elements but integrates both dimensions within a single, interconnected analytical framework. It also provides updated analyses of crime trends and evolving fraud patterns in alignment with the digital transformation of the banking sector, and offers both theoretical and practical contributions, enhancing understanding of digital fraud behavior as well as strategies for strengthening cybersecurity in the banking industry.

This study is designed to fill the identified research gap by examining cybersecurity trends and the evolution of fraud schemes in the banking sector in the digital era. This issue warrants special attention, as recent years have seen a continued rise in public reports concerning financial crimes experienced by banking customers. The research employs a Systematic Literature Review (SLR) approach to systematically identify, select, and analyze literature related to cybersecurity and fraud schemes within the banking sector. The SLR method was chosen because it enables a transparent, structured, and replicable review process, thereby providing a comprehensive understanding of research trends and the evolution of digital crime patterns. The research process begins with formulating the study's objectives and research questions, which focus on identifying the types of fraud most frequently occurring in digital banking and examining key information security aspects, including confidentiality, integrity, and availability. The findings of this study are expected to provide a strong scientific foundation for the development of information security policies, fraud risk mitigation strategies, and data protection systems within the banking industry. Moreover, this study is intended to serve as a reference for future research in the fields of cybersecurity and digital crime.

[23] Md Waliullah et al., "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review," *American Journal of Advanced Technology and Engineering Solutions* 1, no. 1 (2025): 226–57, https://doi.org/10.63125/fh49gz18.

[24] Md Zahin Hossain George, Md Khorshed Alam, and Md Tarek Hasan, "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review REVIEW," *ASRC Procedia: Global Perspectives in Science and Scholarship* 3, no. 1 (2023): 37–61, https://doi.org/10.63125/913ksy63.

Discussion

Cybersecurity Trends in the Banking Sector

Digitalization has become a widespread phenomenon affecting various sectors of life, including the banking industry. While banking digitalization offers significant convenience, it also introduces risks that must be carefully managed, one of the most critical being cybersecurity. Cybersecurity in the banking sector demands heightened attention, especially given the increasing frequency of cyberattacks targeting national banks.

According to the International Organization for Standardization, cybersecurity refers to measures taken to protect computer systems from digital attacks or unauthorized access.[25] Several key elements constitute cybersecurity, including application security, information security, cloud security, network security, disaster recovery and business continuity planning, operational security, and end-user education. These elements are essential for ensuring comprehensive cybersecurity protection, particularly as exposure to digital threats continues to rise and the nature of these threats grows increasingly diverse. Therefore, safeguarding systems even against the smallest risks is crucial for maintaining the resilience and security of banking operations.[26]

Cybersecurity plays a critical role in preventing attacks aimed at disabling or disrupting system operations or devices. The increasing sophistication of cyber threats, along with the rising frequency of cyber incidents, requires banks to maintain heightened vigilance and develop strong capabilities to anticipate, respond to, and manage emerging threats. Poorly handled cyber incidents can disrupt banking business processes and produce widespread consequences. Moreover, inadequate cybersecurity measures may result in a loss of public trust and can generate significant reputational risk for the institution.

According to the National Cyber Security Center (NCSC), several cybersecurity trends that the banking sector must pay close attention to are as follows:[27]

1. *Ransomware*

   In recent years, ransomware has become a major global issue for organizations worldwide. This type of malware constitutes a form of cybercrime in which files are encrypted and users are locked out of their systems, while the perpetrators demand payment in exchange for restoring access. Organizations affected by ransomware often experience prolonged operational paralysis, especially those lacking adequate data backup systems.

2. *Persistent Risks Arising from Remote Work*

   As the pandemic entered its fourth year, reliance on remote work and cloud-based software systems became widespread. This shift means that the banking sector is now exposed to a greater number of cybersecurity vulnerabilities compared to other industries. Employees do not always access data through systems and networks controlled by the organization, thereby increasing exposure to potential threats. As a result, comprehensive vigilance and enhanced security measures are essential.

3. *Cloud-Based Cyberattacks*

   With the increasing volume of software systems and data stored in cloud environments, cybercriminals are taking advantage of these platforms. As a result, cloud-based attacks have become one of the most common cyber threats faced by the banking sector. Banks must

[25] ISO, *ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management* (Geneva, Switzerland: International Organization for Standardization (ISO), 2018).

[26] ISO, *ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management*.

[27] Ervina Anggraini, "Antisipasi 5 Tren Keamanan Siber Ini di 2024!," CTI - Biggest IT Distributor Company in Indonesia, last modified December 15, 2023, https://computradetech.com/id/blog-id/antisipasi-5-tren-keamanan-siber-ini-di-2024/.

ensure that their cloud infrastructure is securely configured in order to protect against malicious breaches.

4. *Social Engineering*

   One of the most significant emerging threats to the banking sector is social engineering. Human users often represent the weakest link in the security chain, making them vulnerable to manipulation. Individuals—including bank employees and customers—can be deceived into disclosing sensitive information or login credentials. Social engineering can occur in many forms, such as phishing or whaling attacks, or through the distribution of fraudulent invoices disguised as legitimate communications. It is therefore essential to continually educate employees about social engineering tactics and the ways in which these threats continue to evolve.

5. *Supply Chain Attacks*

   An increasingly popular method used by cybercriminals to distribute malware is by targeting software vendors and inserting malicious code that is then passed on to customers and other parties within a product's supply chain. This type of attack can compromise distribution systems and allow cybercriminals to infiltrate customer networks.

Several preventive measures must be undertaken by policymakers (in this case, the government) to combat cybercrime.[28] First, modernizing national criminal law and its procedural regulations in alignment with relevant international conventions on cybercrime. Second, strengthening the national computer network security infrastructure in accordance with international standards. Third, enhancing the knowledge and technical expertise of law enforcement authorities in preventing, investigating, and prosecuting cases related to cybercrime.

Fraud Schemes in the Banking Sector

Rapid technological developments have significantly influenced how people conduct banking activities. Today, customers can easily perform online banking transactions through their smartphones. This shift requires the banking sector to provide secure online banking services. Although banks have implemented sophisticated security features, criminals continue to seek vulnerabilities in order to carry out fraud and exploit victims. Two of the most common fraud schemes in online banking transactions are social engineering and phishing. In these schemes, perpetrators manipulate victims by leveraging moments of carelessness or trust, with the intention of gaining access to personal information and banking data such as user IDs, passwords, PINs, and other sensitive credentials.

The Financial Services Authority (Otoritas Jasa Keuangan/OJK) has reported emerging fraud schemes in the banking sector that continue to evolve and introduce new variations. One notable new modus operandi is the "*wrong transfer*" scam linked to illegal online lending platforms (Pinjol). This scheme is characterized by the unexpected transfer of funds into a victim's bank account from an illegal lending entity, despite the account holder never applying for a loan. The fraudulent transfer is typically followed by aggressive collection attempts via telephone, where victims are coerced into repaying the so-called debt—often with exorbitant and unlawful interest charges.

The most frequent fraud schemes occurring in the banking sector are phishing and social engineering. Perpetrators employ psychological manipulation techniques to deceive customers into disclosing personal information such as user IDs, passwords, and PINs. This information is then used to access the victim's bank account and drain their balance. These schemes exploit vulnerabilities in the confidentiality aspect of digital banking systems, demonstrating that

[28] Dista Amalia Arifah, "Kasus Cybercrime di Indonesia," *Jurnal Bisnis dan Ekonomi* 18, no. 2 (2011): 185–95.

despite advancements in banking technology, the human factor remains the primary point of weakness.

Another emerging scheme is the "*wrong transfer*" modus involving illegal online lending platforms (Pinjol). In such cases, funds are transferred into a customer's account without any loan request, followed by fraudulent collection attempts via telephone, accompanied by unreasonable and coercive interest charges. This scheme reflects a combination of technical vulnerabilities and social manipulation, highlighting the importance of strong oversight of data integrity and careful validation of transactions within banking systems.

Another method identified involves fraud through fake websites or illegal applications that impersonate official bank platforms. Victims are directed to confirm transactions and subsequently enter sensitive information. This technique exploits weaknesses in system availability and security, as offenders manipulate features intended to enhance customer convenience for fraudulent purposes.

Fraud in the banking system is unlikely to be completely eliminated, but its prevalence can be reduced. The expectation of lowering fraud levels depends heavily on each bank's readiness and commitment to implementing effective preventive measures. Addressing this issue requires concrete and decisive action rather than mere discussion. Government intervention is also essential to uncover and resolve the various systemic problems underlying these crimes. The banking sector faces two choices: to establish an environment with low fraud potential or risk repeating the failures experienced by compromised institutions in the past.

Based on the Financial Services Authority Regulation (Peraturan OJK) No. 39/POJK.03/2019, the following measures can be implemented to prevent fraud in the banking sector:[29]

1. *Establish Strong Internal Controls*. Effective internal controls must at minimum include a sound control environment, an advanced accounting system, and robust control mechanisms. A strong control environment requires integrity, ethical values, competent human resources, appropriate management philosophy and style, and clear oversight from the board of directors. Meanwhile, an effective accounting control system must provide accurate, complete, and timely information. Strong procedural controls should include several components: physical safeguards over assets, proper authorization, independent verification, and comprehensive documentation.
2. *Disseminate Information to Customers Regarding Bank Policies*. For example, banks should educate customers about policies related to bribery or illicit incentives associated with loan disbursement. Banks may periodically issue notices to customers clarifying that the institution does not tolerate or accept any form of bribery.
3. *Personnel Supervision*. Fraud perpetrators often use the illicit proceeds to support an extravagant lifestyle. By monitoring employees' lifestyles and exclusive facilities around them, banks can establish preventive measures, as employees who may be inclined to commit fraud will feel that their actions are subject to scrutiny.
4. *Create a Dedicated Fraud Reporting Channel (Online Tips).* Regardless of how sophisticated a fraud scheme may be, many cases are uncovered through internal tips. When employees feel they have access to a simple and confidential mechanism to report suspicious behavior, the likelihood of detecting fraud increases substantially.

Proactive fraud auditing. Fraud examinations are often conducted only after victims have been harmed, making them reactive in nature. A proactive audit approach is expected to foster awareness among personnel that their activities may be reviewed at any time. This creates a deterrent effect by instilling fear of detection among individuals who might otherwise engage

[29] Otoritas Jasa Keuangan (OJK), *Peraturan OJK Nomor 39/POJK.03/2019 Tentang Penerapan Strategi Anti-Fraud Bagi Bank Umum* (Jakarta: OJK, 2019).

in fraudulent behavior. Findings from the literature review, conducted using a Systematic Literature Review (SLR) approach and the PRISMA selection process, reveal common patterns in fraud schemes within the digital banking sector, including phishing, skimming, insider threats, and banking malware. Meta-analysis of quantitative data from selected studies shows that fraud involving a combination of technical weaknesses and human factors poses a significantly higher probability of financial loss than fraud attributed to a single factor alone. Furthermore, consistent implementation of the principles of confidentiality, integrity, and availability (the CIA Triad) is associated with a reduction in fraud incidents, although its effectiveness varies depending on the readiness of information technology (IT) infrastructure, organizational culture, and applicable regulations. Critical analysis of the literature indicates that most studies place greater emphasis on the technical aspects of cybersecurity, such as encryption, firewalls, and monitoring, while the integration of human factors, employee behavior, and organizational culture remains underexplored. Cross-study comparisons also reveal geographical and contextual variations: research from developed countries tends to exhibit more mature security frameworks, better-documented data, and a focus on technology-driven mitigation, whereas studies from developing countries highlight implementation challenges, resource limitations, and the need for stronger regulatory frameworks. These findings underscore that cybersecurity and fraud cannot be conceptually separated. Technical vulnerabilities that are not accompanied by effective management of human risk create opportunities for fraud to occur. Accordingly, this research provides critical insights into the interplay between technology, processes, and human behavior, and serves as a foundation for the development of more holistic security strategies, risk-mitigation policies, and future research guidelines aimed at understanding the complex interaction between cybersecurity and fraud schemes in the digital era.

Conclusion

Several cybersecurity trends must be carefully monitored by the banking sector. *First*, ransomware has become a major global problem for organizations. This type of malware is a form of cybercrime in which files are encrypted and users are locked out of their systems, while perpetrators demand payment in exchange for restoring access. *Second*, the persistent risks associated with remote work, which indicate that the banking sector now faces more cybersecurity vulnerabilities than ever before. Employees do not always access data through systems and networks controlled by the organization, making heightened vigilance essential. *Third*, cloud-based cyberattacks pose a growing threat as increasing volumes of software systems and data are stored in the cloud. Cybercriminals exploit these environments, and as a result, cloud-based attacks have become one of the most prevalent types of cyberthreats affecting the banking industry. *Fourth*, social engineering, which can occur in various forms such as phishing, whaling, and the distribution of fraudulent invoices impersonating trusted sources. These attacks exploit human vulnerability and remain one of the most effective techniques used by cybercriminals. *Fifth*, supply chain attacks, an increasingly common method of distributing malware by targeting software vendors and embedding malicious code into products that are subsequently delivered to customers and other parties within the supply chain.

The rapid advancement of technology has significantly transformed how people conduct their banking activities. Customers can now perform online banking transactions digitally through their smartphones. This development requires the banking sector to provide secure and reliable online banking services. Although banks have implemented sophisticated security features, cybercriminals continue to search for vulnerabilities to carry out fraudulent activities and exploit victims. Among the fraud schemes most commonly found in online banking transactions are social engineering and phishing.

References

Afifah, Eka Febriantika Nur, Diny Widya Evriyanti Simatangkir, and Nafiza Salsabila Faliha. "Keamanan Siber dalam Perbankan Serta Tantangan dan Solusi di Era Digital." *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 33–42. https://doi.org/10.61722/jmia.v2i1.3119.

Alodhiani, Ahmed Abdulrhman B. "Financial Technology (Fintech) and Cybersecurity: A Systematic Literature Review." *Arab Journal for Humanities and Social Sciences*, no. 20 (2023). https://doi.org/10.59735/arabjhs.vi20.55.

Anggraini, Ervina. "Antisipasi 5 Tren Keamanan Siber Ini di 2024!" CTI - Biggest IT Distributor Company in Indonesia. Last modified December 15, 2023. https://computradetech.com/id/blog-id/antisipasi-5-tren-keamanan-siber-ini-di-2024/.

Arifah, Dista Amalia. "Kasus Cybercrime di Indonesia." *Jurnal Bisnis dan Ekonomi* 18, no. 2 (2011): 185–95.

Arofah, Nida Rafa, and Yeni Priatnasari. "Internet Banking dan Cyber Crime: Sebuah Studi Kasus di Perbankan Nasional." *Jurnal Pendidikan Akuntansi Indonesia* 18, no. 2 (2020): 107–19. https://doi.org/10.21831/jpai.v18i2.35872.

Azzahra, Nasywa Shafa, Aron Micael Tambunan, Najwa Nayra Aulia, Arista Binarsih, and Tubagus Hedi Saepudin. "Tinjauan Literatur Tentang Ancaman Cybercrime dan Implementasi Keamanan Siber di Industri Perbankan." *HUMANITIS: Jurnal Homaniora, Sosial dan Bisnis* 2, no. 7 (2024): 692–700.

Balaka, Kemal Idris, Aulia Rahman Hakim, and Frygyta Dwi Sulistyany. "Pencurian Informasi Nasabah di Sektor Perbankan: Ancaman Serius di Era Digital." *Yustitiabelen* 10, no. 2 (2024): 105–30. https://doi.org/10.36563/yustitiabelen.v10i2.1167.

Chintia, Ervina, Rofiqoh Nadiah, Humayyun Nabila Ramadhani, Zulfikar Fahmi Haedar, Adam Febriansyah, and Nur Aini Rakhmawati. "Kasus Kejahatan Siber yang Paling Banyak Terjadi di Indonesia dan Penanganannya." *JIEET (Journal of Information Engineering and Educational Technology)* 2, no. 2 (2018): 65–69. https://doi.org/10.26740/jieet.v2n2.p65-69.

Cressey, Donald R. *Other People's Money: A Study in the Social Psychology of Embezzlement*. Montclair, NJ: Patterson Smith, 1973.

Ernst and Young. *Detecting Financial Statement Fraud: What Every Manager Needs to Know*. London: E & Y LLP, 2009.

Faridi, Muhammad Khairul. "Kejahatan Siber dalam Bidang Perbankan." *Cyber Security dan Forensik Digital* 1, No. 2 (2018): 57–61. https://doi.org/10.14421/csecurity.2018.1.2.1373.

George, Md Zahin Hossain, Md Khorshed Alam, and Md Tarek Hasan. "Machine Learning for Fraud Detection in Digital Banking: A Systematic Literature Review REVIEW." *ASRC Procedia: Global Perspectives in Science and Scholarship* 3, no. 1 (2023): 37–61. https://doi.org/10.63125/913ksy63.

ISO. *ISO/IEC 27005:2018 Information Technology - Security Techniques - Information Security Risk Management*. Geneva, Switzerland: International Organization for Standardization (ISO), 2018.

Manurung, Daniel T. H., and Andhika Ligar Hardika. "Analysis of Factors that Influence Financial Statement Fraud in the Perspective Fraud Diamond: Empirical Study on Banking Companies Listed on the Indonesia Stock Exchange Year 2012 to 2014." *International Conference on Accounting Studies (ICAS) 2015* (2015): 280–86. https://doi.org/10.13140/RG.2.1.2058.8563.

Meliana, Meliana, and Trie Rundi Hartono. "Fraud Perbankan Indonesia: Studi Eksplorasi." *Prosiding Seminar Nasional Pakar* 1, no. 1 (2019): 2521–27. https://doi.org/10.25105/pakar.v0i0.4335.

Munajat, Andi Ahmad, and Hudi Yusuf. "Peran Teknologi Informasi dalam Pencegahan dan Pengungkapan Tindak Pidana Ekonomi Khusus: Studi Tentang Kejahatan Keuangan Berbasis Digital." *Jurnal Intelek Insan Cendikia* 1, no. 9 (2024): 4853–65.

Naam, Jufriadif. "Metoda Pertahan Diri Program Virus." *Jurnal PROCESSOR* 8, no. 2 (2013): 36.

Otoritas Jasa Keuangan (OJK). *Peraturan OJK Nomor 39/POJK.03/2019 Tentang Penerapan Strategi Anti-Fraud Bagi Bank Umum*. Jakarta: OJK, 2019.

Radiyah, Anisyah Nur, and Abshoril Fithry. "Kejahatan Keuangan Pada Tindak Pidana Money Laundering Dalam Menghilangkan Jejak Kejahatan." *Prosiding SNAPP: Sosial Humaniora, Pertanian, Kesehatan dan Teknologi* 2, no. 1 (2023): 39–45. https://doi.org/10.24929/snapp.v2i1.3179.

Schmidt, Nikola. "Critical Comments on Current Research Agenda in Cyber Security." *Obrana a Strategie* 14, no. 1 (2014): 29–38.

Setiawan, Nanang, and Imam Wahyudi. "Pencegahan Fraud pada Kejahatan Siber Perbankan." *Kabillah: Journal of Social Community* 8, no. 1 (2023): 508–18. https://doi.org/10.35127/kabillah.v8i1.280.

Stoneburner, Gary, Alice Goguen, and Alexis Feringa. "Risk Management Guide for Information Technology Systems." *NIST Special Publication* 800, no. 30 (2002): 800–830.

Subyanto, Wahyu. "Statistik Kejahatan Siber Indonesia 2023, Jual Beli Online Terbanyak Penipuan." nextren.grid.id. Last modified November 27, 2023. https://nextren.grid.id/read/013955948/statistik-kejahatan-siber-indonesia-2023-jual-beli-online-terbanyak-penipuan?page=all.

Suhartadi, Imam. "Survei GBG: RI Duduki Peringkat Teratas Kasus Money Mule dan Pencurian Identitas." Investor.Id. Last modified August 5, 2024. https://investor.id/business/369245/survei-gbg-ri-duduki-peringkat-teratas-kasus-money-mule-dan-pencurian-identitas.

Syahraeni, Syahraeni, Nur Hikmah, and Sitti Nikmah Marzuki. "Kasus Penipuan di Perbankan Syariah: Analisis Fraud Internal dan Implikasinya terhadap Kepercayaan Nasabah." *Lan Tabur: Jurnal Ekonomi Syariah* 6, no. 1 (2024): 122–40. https://doi.org/10.53515/lantabur.2024.6.1.122-140.

Waliullah, Md, Md Zahin Hossain George, Md Tarek Hasan, Md Khorshed Alam, Mosa Sumaiya Khatun Munira, and Noor Alam Siddiqui. "Assessing the Influence of Cybersecurity Threats and Risks on the Adoption and Growth of Digital Banking: A Systematic Literature Review." *American Journal of Advanced Technology and Engineering Solutions* 1, no. 1 (2025): 226–57. https://doi.org/10.63125/fh49gz18.

Whitman, M. E., and H. J. Mattord. *The CIA Triad: Confidentiality, Integrity, and Availability*. 4th ed. Waltham, MA: Elsevier/Morgan Kaufmann, 2017.