Vol. 03 No. 02 (June 2025) ISSN: 2963-220X (p); 2964-626X (e)

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

Original paper

Evolution and Patterns of Crime in Banking Systems: From Traditional Fraud to Cybercrime

Mohamad Nur Efendi[1*], Mukhtar Adinugroho[2], Selvina Khomairoh[3]
[1] Faculty of Economics and Business, Universitas Terbuka, Indonesia
[2] Faculty of Economics, Business and Digital Technology, Universitas Nahdlatul Ulama Surabaya, Indonesia
[3] Department of Business Administration Science, Universitas Terbuka, Indonesia

Corresponding author: md.nur.efendi@gmail.com

Keywords:
Banking Crime Evolution, Banking Security, Cybercrime, Digital Fraud Trends, Traditional Fraud

Submitted: 1 August 2024
Accepted: 14 May 2025
Published: 27 June 2025

Abstract

This study examines evolving crime patterns in the banking sector, highlighting the shift from conventional fraud to sophisticated cybercrimes such as phishing, ransomware, and data breaches. Digitalization and financial innovation have had a profound impact on criminal strategies, exposing vulnerabilities in digital systems and creating new security challenges for banks. Utilising a literature review method, the research explores the nexus between cybercrime and money laundering (TPPU) as well as terrorism financing (TPPT). In these contexts, cyberattacks frequently facilitate the execution of untraceable international transactions. The study recommends the adoption of technologies such as AI-based anomaly detection, the tightening of cybersecurity regulations, and the improvement of cyber awareness among employees and customers. Furthermore, it emphasises the enhancement of the supervisory role of Indonesia's Financial Transaction Reports and Analysis Center (PPATK) in monitoring digital financial flows and the promotion of international information sharing. Cross-sector collaboration among financial institutions, regulators, and technology providers is deemed crucial to strengthening the global financial system's defences. These measures are intended to enhance Indonesia's Anti-Money Laundering and Countering the Financing of Terrorism (APU PPT) framework in response to the growing risks of the digital era.

To cite this article: Efendi, M. N., Adinugroho, M., & Khomairoh, S. 2025. *Evolution and Patterns of Crime in Banking Systems: From Traditional Fraud to Cybercrime. AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 3(2):168-196, https://doi.org/10.59593/amlcft.2025.v3i2.219

Introduction

Crime in the banking system has undergone significant evolution along with the development of technology and digitalization.[1] In the past, banking crimes generally took the form of traditional fraud, such as check forgery, embezzlement, and identity theft through

[1] Monica Violeta Achim and Sorin Nicolae Borlea, *Economic and Financial Crime: Corruption, Shadow Economy, and Money Laundering*, vol. 20, Studies of Organized Crime (Cham: Springer International Publishing, 2020), https://doi.org/10.1007/978-3-030-51780-9.

physical documents.[2] Traditional criminology theories, such as rational choice theory, assume that criminals commit criminal acts after considering the risks and benefits.[3] In the banking context, perpetrators usually exploit weaknesses in existing security systems, such as a lack of internal controls or inconsistencies in operational procedures.[4] Traditional fraud control models emphasize the importance of internal supervision, regular audits, and strict identity verification as an effort to prevent and detect crime.[5]

The advent of the digital era has caused the pattern of crime in banking to shift towards cybercrime, which includes various forms of crime such as phishing, malware, ransomware, and system hacking.[6] New theories in cyber criminology, such as activity routine theory and neutralization theory, have been developed to explain this phenomenon. According to activity routine theory, the opportunity for crime increases when there are viable targets, motivated perpetrators, and no supervisors.[7] In the digital context, the accessibility of information and data, coupled with weak security systems, creates an ideal environment for cybercriminals. In addition, neutralization theory explains how cybercriminals often justify their actions by downplaying or denying the harm they cause.[8] This shift suggests that criminals are increasingly adopting advanced technologies to exploit vulnerabilities in digital banking systems, requiring a new approach to crime control that is more adaptive and innovative.

The study of the evolution of crime in the banking system has attracted the attention of researchers, with a growing focus on the shift from traditional fraud to cybercrime. Choi et al. (2017) highlighted that traditional crimes such as identity theft and check fraud have declined with the improvement of physical security and stricter regulations in the banking system.[9] A report by Hasham et al. (2019) highlighted the rapid increase in cybercrime, especially in the form of phishing and ransomware attacks, which pose a significant threat to the integrity of the digital banking system.[10] The study by Lokanan (2018) also discussed how technological developments, such as the use of Internet banking, have created new opportunities for cybercriminals to exploit security gaps.[11]

Modus operandi generally refers to the distinctive method or pattern of behavior that an individual, particularly a criminal, consistently uses when committing unlawful acts. In the context of cybercrime, modus operandi encompasses the specific techniques, strategies, and tools employed by offenders to exploit vulnerabilities in digital systems. Pospisil et al. (2020) emphasized the importance of a deep understanding of the modus operandi of cybercrime for

[2] Mark Lokanan, “Theorizing Financial Crimes as Moral Actions,” *European Accounting Review* 27, no. 5 (2018): 901–38, https://doi.org/10.1080/09638180.2017.1417144.

[3] Shazeeda Ali, “Criminal Minds: Profiling Architects of Financial Crimes,” *Journal of Financial Crime* 28, no. 2 (2021): 324–44, https://doi.org/10.1108/JFC-11-2020-0221.

[4] Hafiza Aishah Hashim et al., “The Risk of Financial Fraud: A Management Perspective,” *Journal of Financial Crime* 27, no. 4 (2020): 1143–59, https://doi.org/10.1108/JFC-04-2020-0062.

[5] Nancy Reichman, “Managing Crime Risks: Toward an Insurance Based Model of Social Control,” in *Risk Management*, ed. Gerald Mars and David T. H. Weir (London: Routledge, 2020), 45–66.

[6] Yoga Pratama et al., “Cybercrime: The Phenomenon of Crime through the Internet in Indonesia,” *Proceeding International Conference Restructuring and Transforming Law* 1, no. 1 (2022): 294–301.

[7] Brian K. Payne, “Defining Cybercrime,” in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, ed. Thomas J. Holt and Adam M. Bossler (Cham: Palgrave Macmillan, 2020), 3–25, https://doi.org/10.1007/978-3-319-78440-3_1.

[8] Mochammad Fahlevi et al., “Cybercrime Business Digital in Indonesia,” *E3S Web of Conferences* 125 (2019): 21001, https://doi.org/10.1051/e3sconf/201912521001.

[9] Kwan Choi, Ju-lak Lee, and Yong-tae Chun, “Voice Phishing Fraud and Its Modus Operandi,” *Security Journal* 30, no. 2 (2017): 454–66, https://doi.org/10.1057/sj.2014.49.

[10] Salim Hasham, Shoan Joshi, and Daniel Mikkelsen, *Financial Crime and Fraud in the Age of Cybersecurity* (New Yok: McKinsey & Company, 2019).

[11] Lokanan, “Theorizing Financial Crimes as Moral Actions.”

the development of effective prevention strategies.[12] This study is in line with the findings by Reichman (2020) who showed that social engineering techniques have become a primary tool for criminals to defraud individuals and access sensitive data.[13] Van Nguyen (2022) examined how transnational criminal networks often carry cybercrime, demonstrating the problem's complexity and global scale of the problem.[14] The study by Trozze et al. (2022) adds that the emergence of cryptocurrencies has introduced a new dimension to banking crime, with hard-to-trace transactions providing a profit for criminals.[15]

Many studies have explored various aspects of banking crime, but there is a gap in understanding the impact of technological transformation on crime patterns and banking responses. Several studies, such as those by Jakšič and Marinč (2019), have highlighted the role of artificial intelligence and financial technology in mitigating cybercrime, but are still limited in linking the evolution from traditional fraud to cybercrime in a comprehensive manner.[16] This gap includes understanding how more complex banking crime patterns can potentially be used as a means of money laundering (TPPU) and terrorism financing (TPPT), given the development of techniques used to obscure the source of illicit funds. This study aims to fill this gap by comprehensively analyzing the evolution of banking crime typologies and their impact on crime prevention policies in the digital era. By mapping the transformed crime patterns and evaluating the effectiveness of existing security policies, it is hoped that more adaptive prevention measures can be identified to address TPPU and TPPT risks in the future.

This study uses a literature review method to analyze the evolution of crime patterns in the banking system, focusing on how digitalization and financial technology influence the modus operandi of criminals in Money Laundering (TPPU) and Terrorism Financing (TPPT). Literature was selected based on publications from 2017 to 2024, emphasizing peer-reviewed articles, regulatory reports, and policy papers in the fields of criminology, cybersecurity, anti-money laundering, and banking policy. Sources were identified through databases such as Scopus, ScienceDirect, JSTOR, and Google Scholar using relevant keywords. The selected studies specifically address cyber-enabled financial crimes, the role of digital platforms in concealing illicit funds, and regulatory responses, allowing the researcher to provide informed recommendations for improving detection and prevention strategies in the digital era.

This study aims to identify and analyze changes in the modus operandi, motivations, and methods used by criminals in the banking sector. This study explores how technological advances, such as digitalization and financial innovation, affect the banking crime landscape while assessing the effectiveness of prevention and law enforcement strategies implemented by financial institutions and the government. Given its relevance to Money Laundering (TPPU) and Terrorism Financing (TPPT), this study also highlights the close relationship between these crimes, where new banking techniques allow for a more hidden and rapid circulation of proceeds of crime, often involving international transfers and digital transactions.

Despite the growing body of literature addressing cyber-enabled financial crime, several research gaps remain. Some studies tend to focus narrowly on specific technologies or regions,

[12] Bettina Pospisil et al., "Modus Operandi in Cybercrime," in *Encyclopedia of Criminal Activities and the Deep Web* (IGI Global Scientific Publishing, 2020), 193–209, https://doi.org/10.4018/978-1-5225-9715-5.ch013.

[13] Reichman, "Managing Crime Risks."

[14] Trong Van Nguyen, "The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam," *Trends in Organized Crime* 25, no. 2 (2022): 226–47, https://doi.org/10.1007/s12117-021-09422-1.

[15] Arianna Trozze et al., "Cryptocurrencies and Future Financial Crime," *Crime Science* 11, no. 1 (2022): 1, https://doi.org/10.1186/s40163-021-00163-8.

[16] Marko Jakšič and Matej Marinč, "Relationship Banking and Information Technology: The Role of Artificial Intelligence and FinTech," *Risk Management* 21, no. 1 (2019): 1–18, https://doi.org/10.1057/s41283-018-0039-y.

lacking a comprehensive view of global trends and cross-border implications. In addition, there are conflicting findings regarding the effectiveness of regulatory frameworks, with some scholars emphasizing their progressiveness, while others criticize enforcement limitations and the adaptability of criminals. Although most literature acknowledges the rise of digital threats, only a few studies offer in-depth analysis of how banking institutions can practically respond to evolving risks. This study contributes by synthesizing recent findings and identifying underexplored areas such as the intersection of fintech, regulatory lag, and cross-border laundering schemes while offering recommendations for future research and policy improvement relevant to the digital banking context. Through a literature review approach, this study aims to identify existing research gaps, as well as provide recommendations for further research and more effective policy practices for various stakeholders, including governments, financial institutions, and the general public. The overall contribution of this study is expected to support global efforts in creating a safer banking environment from the threat of crime, as well as play a role in efforts to combat TPPU and TPPT in the digital era.

Discussion

Evolution of Crime in the Banking System

The history of banking crime has undergone significant evolution over time, reflecting changes in technology, regulation, and the global economy. In the early 20th century, banking crime was largely limited to practices such as embezzlement and financial statement manipulation, often involving bank officials or individuals with access to the bank's internal systems. Achim and Borlea (2020) explain that these types of crimes were often difficult to detect due to the lack of effective oversight mechanisms and technological limitations.[17] Masciandaro (2017) adds that during this period, banking crime was also closely associated with money laundering and the use of offshore financial centers to hide the proceeds of crime.[18]

The pattern of banking crime has changed dramatically with advances in technology and the emergence of digital banking systems. Van Driel (2019) identifies that the digital era has introduced new forms of crime such as hacking, identity fraud, and phishing schemes, which exploit vulnerabilities in banks' cybersecurity systems.[19] Hilal et al. (2022) note that as anomaly detection technology has become more sophisticated, new methods of fraud have also evolved to evade detection.[20] Wewege, Lee, and Thomsett highlight that the digitalization of banking has introduced new opportunities and risks, necessitating the rapid adaptation of regulations and security practices to protect consumers and financial institutions.[21] This history shows how banking crime has adapted to technological developments and how regulation continues to evolve to respond to emerging threats.

[17] Achim and Borlea, *Economic and Financial Crime*.

[18] Donato Masciandaro, *Global Financial Crime: Terrorism, Money Laundering and Offshore Centres* (New York: Taylor & Francis, 2017).

[19] Hugo van Driel, "Financial Fraud, Scandals, and Regulation: A Conceptual Framework and Literature Review," *Business History* 61, no. 8 (2019): 1259–99, https://doi.org/10.1080/00076791.2018.1519026.

[20] Waleed Hilal, S. Andrew Gadsden, and John Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," *Expert Systems with Applications* 193 (2022): 116429, https://doi.org/10.1016/j.eswa.2021.116429.

[21] Luigi Wewege, Jeo Lee, and Michael C. Thomsett, "Disruptions and Digital Banking Trends," *Journal of Applied Finance & Banking* 10, no. 6 (2020): 15–56.

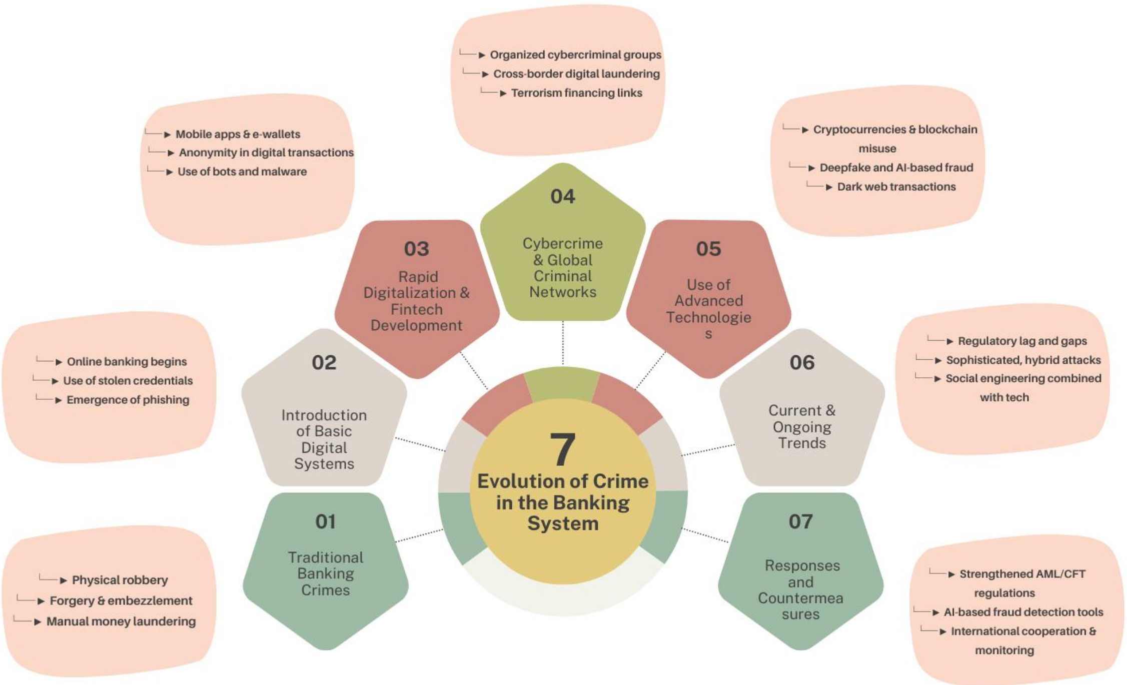

Organized cybercriminal groups
Cross-border digital laundering
Terrorism financing links
Mobile apps & e-wallets
Anonymity in digital transactions
Use of bots and malware
Cryptocurrencies & blockchain misuse
Deepfake and AI-based fraud
Dark web transactions
04
Cybercrime & Global Criminal Networks
03
Rapid Digitalization & Fintech Development
05
Use of Advanced Technologie s
Online banking begins
Use of stolen credentials
Emergence of phishing
02
Introduction of Basic Digital Systems
06
Current & Ongoing Trends
Regulatory lag and gaps
Sophisticated, hybrid attacks
Social engineering combined with tech
7
Evolution of Crime in the Banking System
01
Traditional Banking Crimes
07
Responses and Countermea sures
Physical robbery
Forgery & embezzlement
Manual money laundering
Strengthened AML/CFT regulations
AI-based fraud detection tools
International cooperation & monitoring

Figure 1. Evolution of Crime in the Banking System.
Source: Created by the author, 2024

Classic cases of banking fraud often involve sophisticated techniques that exploit weaknesses in the traditional banking system. One famous example is the Enron scandal, where executives used complex accounting practices to hide debts and artificially inflate profits. Shazeeda Ali identifies that perpetrators of such financial fraud often have a deep understanding of weaknesses in the financial system and the ability to manipulate financial information for personal gain.[22] In the case of Enron, executives used a series of shell companies to hide the company's debts, creating a much healthier financial picture than it was.

The modus operandi of classic banking fraud also includes Ponzi schemes, where perpetrators promise investors high returns from funds invested by new investors, rather than from legitimate profits. Another famous example is the case of Bernie Madoff, who successfully defrauded thousands of investors over decades. Kwan Choi et al. (2017) note that such schemes often rely on the perpetrators' charisma and ability to build trust with their victims.[23] Perpetrators often use their social and professional networks to attract new investors, keeping the scheme going until it eventually collapses when the flow of new funds dries up.

In the digital era, banking fraud modus operandi has evolved with the emergence of cybercrime. Phishing, one common form of fraud, involves attempts to obtain victims' personal information through fake emails or websites. Pospisil et al. (2020) explained that perpetrators often use social engineering techniques to make the communication appear legitimate, such as by imitating communications from known financial institutions.[24] This makes victims more likely to provide sensitive information such as bank account numbers or passwords. This modus operandi has evolved with the advancement of technology, with perpetrators using malware and other cyberattacks to access financial information.

In addition, banking fraud through transnational modus operandi is also on the rise. Jonathan M. Karpoff (2021) stated that with globalization and technological advancements, criminals can now operate fraud schemes from multiple locations around the world, often

[22] Ali, "Criminal Minds."
[23] Choi, Lee, and Chun, "Voice Phishing Fraud and Its Modus Operandi."
[24] Pospisil et al., "Modus Operandi in Cybercrime."

involving complex international networks.[25] Trong Van Nguyen (2022) pointed out that in many cases, these crimes involve the use of fake identities and shell companies to disguise the origin of funds and the perpetrators' identities.[26] This phenomenon adds to the challenges in law enforcement and regulation, as it involves multiple jurisdictions and often exploits legal loopholes across different countries.

The transition to the digital era has brought about major changes in the banking system. Technological innovations such as artificial intelligence (AI), blockchain, and fintech have introduced new efficiencies, improved customer service, and changed the way transactions are conducted. Jakšič and Marinč (2019) explain that these technologies have simplified the banking process and enabled banks to better understand and serve customers through data analytics and personalized services.[27] In addition, digital technologies such as FinTech have enabled banks to provide financial services to previously unreached populations, expanding financial inclusion globally.

Technology has also changed the banking business model. Digital banking has reduced reliance on physical branches and made it easier to access services through mobile devices and online. Mosteanu and Faccia (2020) highlight that the use of technologies such as blockchain in financial transactions has increased transparency and security, while cryptocurrencies offer new alternatives in payments and investments.[28] These changes are driving banks to adopt new technologies and integrate digital solutions into their operations to stay competitive in an increasingly tech-dominated market.

Cybercrime has also seen a significant increase as technology advances in banking. Cybercrime in banking takes many forms, including phishing, hacking, identity theft, and malware distribution. Leo et al. (2019) noted that these crimes exploit vulnerabilities in banks' digital security systems to access sensitive information and funds.[29] While technologies such as AI and machine learning are used to detect and prevent cybercrime, criminals are also continually developing new methods to evade detection, creating an arms race between perpetrators and law enforcement. One of the main challenges in combating cybercrime is its complexity and global reach. Azernikov et al. (2018) pointed out that cybercrime often involves complex international networks, making it difficult to track and prosecute.[30] In addition, cybercriminals often use encryption technology and the dark web to hide their identities and activities. This complicates law enforcement efforts and requires closer international cooperation in preventing and responding to cybercrime.

Several high-profile cases of cybercrime in the banking sector have demonstrated the significant impact that these attacks can have. One high-profile example is the WannaCry ransomware attack in 2017, which affected many organizations around the world, including financial institutions. Wewege et al. (2020) note that this attack locked victims' data and demanded payment in cryptocurrency, highlighting the risks that banks face in the digital age.[31] This attack demonstrated how cybercrime can disrupt bank operations and undermine customer trust. The 2016 SWIFT hack, in which cybercriminals managed to steal $81 million from the

[25] Jonathan M. Karpoff, "The Future of Financial Fraud," *Journal of Corporate Finance* 66 (2021): 101694, https://doi.org/10.1016/j.jcorpfin.2020.101694.

[26] Van Nguyen, "The Modus Operandi of Transnational Computer Fraud."

[27] Jakšič and Marinč, "Relationship Banking and Information Technology."

[28] Narcisa Roxana Mosteanu and Alessio Faccia, "Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies," *Quality – Access to Success* 21, no. 174 (February 2020): 159–66.

[29] Martin Leo, Suneel Sharma, and K. Maddulety, "Machine Learning in Banking Risk Management: A Literature Review," *Risks* 7, no. 1 (2019): 29, https://doi.org/10.3390/risks7010029.

[30] A. D. Azernikov et al., "Innovative Technologies in Combating Cyber Crime," *KnE Social Sciences* 3, no. 2 (2018): 248–52, https://doi.org/10.18502/kss.v3i2.1550.

[31] Wewege, Lee, and Thomsett, "Disruptions and Digital Banking Trends."

Central Bank of Bangladesh, demonstrated that even systems designed for high security can be vulnerable to attack. This case highlights the need for tighter security and better oversight of international financial transactions. The incident also highlights the importance of international cooperation in combating cybercrime, given that the attacks involved actors from multiple countries.

Another high-profile case is the massive Equifax data breach in 2017, in which the personal information of over 147 million people was stolen. This incident highlights the significant risks associated with the storage and management of digital data by financial institutions. Navaretti et al. (2018) show that such incidents not only result in significant financial losses but also impact the reputation of the institutions involved.[32] This underscores the importance of data security and privacy protection in digital banking.

Overall, the transition to the digital age has brought significant benefits to the banking system, but it has also created new challenges in the form of cybercrime. Cybercrime continues to evolve as technology advances, and banks must continually adapt and improve their security systems to protect assets and customer information. Collaboration between banks, law enforcement, and regulatory bodies is essential to developing effective strategies to combat these threats and maintain the integrity of the global financial system.

Crime Patterns in the Banking System

The characteristics of traditional crimes and cybercrimes in the banking context show significant differences in terms of modus operandi, impact, and law enforcement challenges. Traditional crimes, such as embezzlement and fraud, often involve physical contact or direct interaction between the perpetrator and the victim. For example, fraud cases involving counterfeit checks or embezzlement typically require the manipulation of physical documents or the use of fake identities in person. Lokanan (2018) explains that these crimes are often perceived as morally deviant acts, where perpetrators seek personal gain through system manipulation or abuse of trust.[33]

Cybercrimes tend to occur without physical interaction between the perpetrator and the victim. These crimes often involve the use of information and communication technologies to carry out illegal acts. Common examples include phishing, where the perpetrator tricks the victim into providing personal information through fake emails or websites, and malware attacks that damage or steal data from computer systems. Pospisil et al. (2020) noted that cybercrimes have unique characteristics because they can be carried out remotely, allowing perpetrators to hide their identities and locations, and complicating law enforcement.[34]

Another difference lies in the scale and impact of the two types of crimes. Traditional crimes are typically confined to a specific geographic area and often involve relatively small amounts of money compared to cybercrime. Hasham et al. (2019) point out that cybercrime can have a much broader impact, involving thousands of victims in multiple countries, and causing huge financial losses.[35] Examples of ransomware attacks such as WannaCry show how cyberattacks can cripple critical systems worldwide and cause billions of dollars in damage.

In addition, cybercrime often leverages sophisticated technology to avoid detection and prosecution. Choi et al. (2017) explain that cybercriminals often use techniques such as encryption, dark web, and other anonymity tools to hide their tracks.[36] This is in contrast to traditional crimes that typically leave physical evidence or more easily traceable traces. Payne

[32] Giorgio Barba Navaretti et al., "Fintech and Banking. Friends or Foes?," *Friends or Foes* (2018), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099337.

[33] Lokanan, "Theorizing Financial Crimes as Moral Actions."

[34] Pospisil et al., "Modus Operandi in Cybercrime."

[35] Hasham, Joshi, and Mikkelsen, *Financial Crime and Fraud in the Age of Cybersecurity*.

[36] Choi, Lee, and Chun, "Voice Phishing Fraud and Its Modus Operandi."

(2020) notes that the definition of cybercrime has also evolved as technology has evolved, adding complexity to efforts to detect and prevent these crimes.[37]

Law enforcement challenges also differ between the two types of crimes. Traditional crimes can usually be addressed using conventional law enforcement methods, such as field investigations and physical arrests. However, cybercrime requires a more technical approach and often involves international cooperation due to its cross-border nature. Fahlevi et al. (2019) highlight that countries such as Indonesia face particular challenges in addressing cybercrime, particularly due to the lack of technological infrastructure and expertise in dealing with digital crime.[38]

Finally, cybercrime has the potential to grow with the advancement of new technologies such as cryptocurrency and blockchain technology. Trozze et al. (2022) note that cryptocurrency can be used to fund or hide the proceeds of cybercrime, making it more difficult to trace funds.[39] These crimes require innovative regulatory and law enforcement approaches to prevent and address these evolving threats. Overall, the differences in characteristics between traditional and cybercrime demonstrate the need to adapt law enforcement strategies and security policies to address the threats that exist in this digital era.

Cybercrime in banking encompasses a variety of attacks aimed at stealing data, money, or damaging systems. These crimes can impact individuals, businesses, and financial institutions in significant ways. Phishing and social engineering are techniques used to trick individuals into providing their personal or financial information. Phishing is often carried out through emails or text messages that appear to come from a trusted source, such as a bank or technology company, to gain access to a user's account. Gomes et al. (2020) explain that phishing attacks exploit victims' trust in a respected institution, leading them to click on a link or open a malicious attachment.[40] Social engineering, on the other hand, involves psychological manipulation to deceive individuals into disclosing sensitive information or performing actions that could compromise security.

Social engineering does not necessarily involve sophisticated technology but instead exploits human weaknesses, such as overconfidence or ignorance about security threats. Spoorthi et al. (2024) show that this tactic can be particularly effective in e-banking, where users are often unaware of the threats they face.[41] For example, a perpetrator may contact a victim by phone and pretend to be a bank employee to obtain login information. These attacks can cause significant financial losses and damage the reputation of the targeted institution.

Identity and data theft is a type of cybercrime in which a perpetrator gains unauthorized access to an individual's personal or financial information with the intent of misusing it. This data can include credit card numbers, bank account information, or other personal data. Burnes et al. (2020) state that identity theft often occurs through phishing attacks or massive data breaches, where perpetrators gain access to databases containing sensitive information.[42] This data can then be sold on the black market or used to commit fraud.

Data security is critical in preventing identity theft. Nicholls et al. (2021) emphasize that banks must implement strong security measures, such as data encryption and two-factor

[37] Payne, "Defining Cybercrime."

[38] Fahlevi et al., "Cybercrime Business Digital in Indonesia."

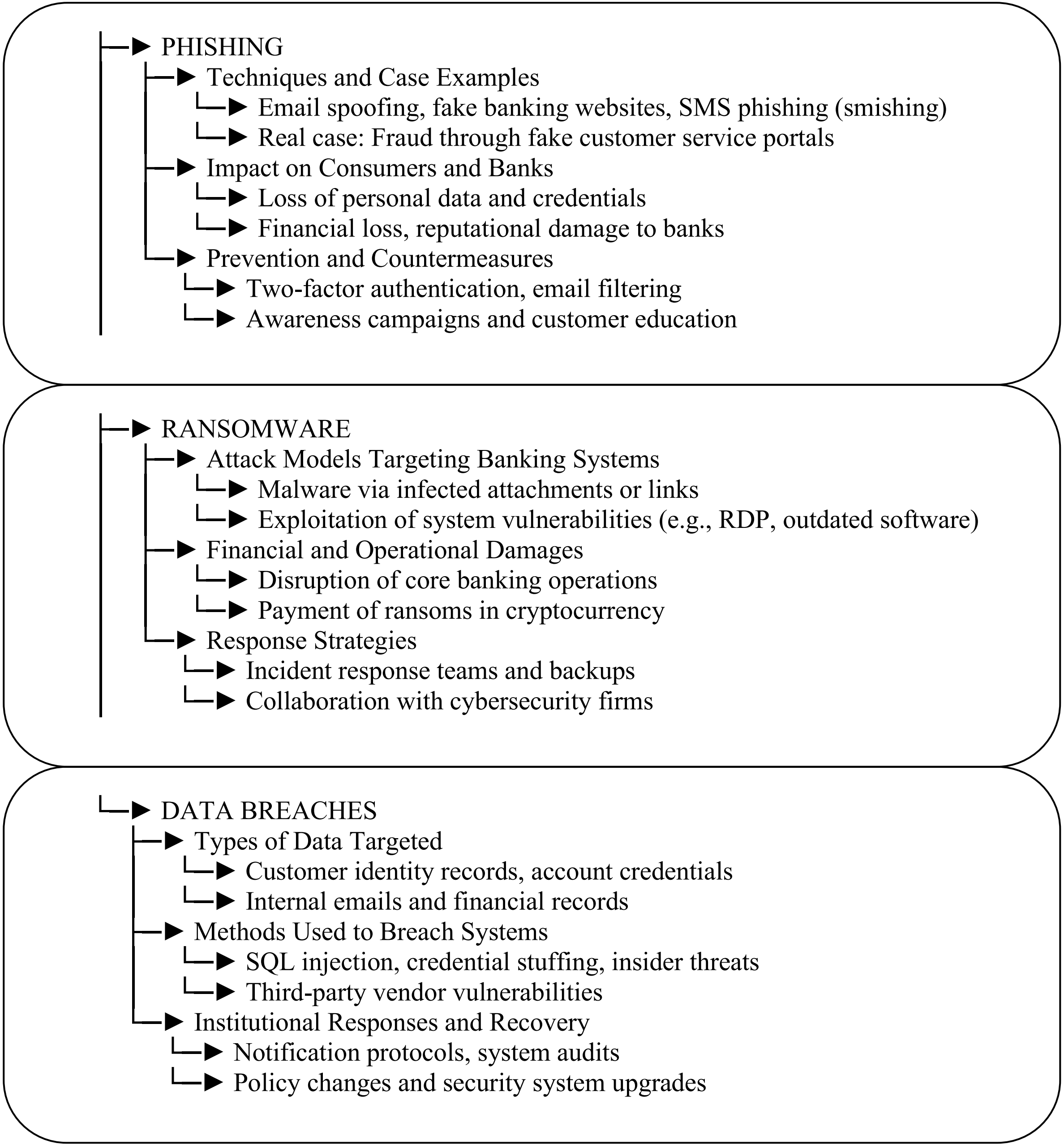
[39] Trozze et al., "Cryptocurrencies and Future Financial Crime."

[40] Vanessa Gomes, Joaquim Reis, and Bráulio Alturas, "Social Engineering and the Dangers of Phishing," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)* (IEEE, 2020), 1–7, https://ieeexplore.ieee.org/abstract/document/9140445/.

[41] M. Spoorthi et al., "Impacts of Social Engineering on E-Banking," in *Social Engineering in Cybersecurity*, ed. H. L. Gururaj, V. Janhavi, and V. Ambika (Boca Raton: CRC Press, 2024).

[42] David Burnes, Marguerite DeLiema, and Lynn Langton, "Risk and Protective Factors of Identity Theft Victimization in the United States," *Preventive Medicine Reports* 17 (2020): 101058, https://doi.org/10.1016/j.pmedr.2020.101058.

authentication, to protect customer information.[43] However, even with stringent security measures, data leaks can still occur, either due to technical weaknesses or human error. This shows the need for high awareness and vigilance from all parties involved.



- PHISHING
  - Techniques and Case Examples
    - Email spoofing, fake banking websites, SMS phishing (smishing)
    - Real case: Fraud through fake customer service portals
  - Impact on Consumers and Banks
    - Loss of personal data and credentials
    - Financial loss, reputational damage to banks
  - Prevention and Countermeasures
    - Two-factor authentication, email filtering
    - Awareness campaigns and customer education
- RANSOMWARE
  - Attack Models Targeting Banking Systems
    - Malware via infected attachments or links
    - Exploitation of system vulnerabilities (e.g., RDP, outdated software)
  - Financial and Operational Damages
    - Disruption of core banking operations
    - Payment of ransoms in cryptocurrency
  - Response Strategies
    - Incident response teams and backups
    - Collaboration with cybersecurity firms
- DATA BREACHES
  - Types of Data Targeted
    - Customer identity records, account credentials
    - Internal emails and financial records
  - Methods Used to Breach Systems
    - SQL injection, credential stuffing, insider threats
    - Third-party vendor vulnerabilities
  - Institutional Responses and Recovery
    - Notification protocols, system audits
    - Policy changes and security system upgrades

Figure 2. Cybercrime in Digital Banking.

Source: Modification from Karpoff (2021)[44] and Haitham M. Alzoubi et al. (2022)[45]

Hacking and data breaches are forms of attacks in which an attacker gains unauthorized access to a computer system or network to steal, modify, or destroy data. Alzoubi et al. (2022) point out that these attacks can be carried out through a variety of methods, such as the use of

[43] Jack Nicholls, Aditya Kuppa, and Nhien-An Le-Khac, "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape," *Ieee Access* 9 (2021): 163965–86.

[44] Karpoff, "The Future of Financial Fraud."

[45] Haitham M. Alzoubi et al., "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)* (IEEE, 2022), 1–4, https://ieeexplore.ieee.org/abstract/document/9896966/.

hacking tools, exploiting software vulnerabilities, or manipulating network protocols.[46] Data breaches often result in large-scale exfiltration of sensitive information, which can be used for a variety of illegal purposes, including identity theft or fraud.

High-profile hacking cases, such as the Equifax data breach, demonstrate how damaging these attacks can be. Pratama et al. (2022) note that the incident exposed the personal data of millions of people, which was then used for criminal activity.[47] Data breaches not only cause direct financial losses but can also damage a company's reputation and undermine public confidence in the security of digital systems.

Ransomware and malware are types of malicious software used to damage or take control of computer systems. Ransomware, in particular, encrypts data on a victim's computer and demands a ransom to restore access. Karpoff (2021) notes that ransomware attacks are becoming increasingly sophisticated, with perpetrators often targeting financial institutions and other critical infrastructure.[48] Once a system is infected, victims are forced to pay in cryptocurrency, which is difficult to trace, to obtain the decryption key.

Malware, on the other hand, includes a variety of malicious software designed to steal data, monitor user activity, or otherwise harm a system. Ghelani et al. (2022) note that malware can be installed through phishing emails, malicious downloads, or infected websites.[49] Malware can result in significant losses, including data theft, system failure, and financial loss. In some cases, malware can also be used as part of a larger attack, such as a system hack or data breach.

The study of crime in the banking sector must not only focus on traditional crimes that have adapted to digital technologies (cyber-enabled crimes), such as fraud and money laundering conducted through online platforms, but also explore the emergence of entirely new forms of crime that are inherently dependent on technology (cyber-dependent crimes). Cyber-enabled crimes typically involve the use of digital tools to amplify conventional criminal acts for example, phishing scams that use email or fake websites to steal user credentials. These crimes exploit the internet as a medium, but do not necessarily require it to exist. Their evolution demonstrates how classic criminal motives can take on new dimensions when paired with technological advancements.

In contrast, cyber-dependent crimes represent a newer and more complex challenge because they exist solely due to the presence of digital infrastructure. Examples include distributed denial-of-service (DDoS) attacks, ransomware, data breaches, and cryptojacking, which target system vulnerabilities, financial data, or institutional networks. These crimes require a digital environment to operate and often involve sophisticated technical knowledge and transnational coordination. Their emergence highlights the need for policymakers and banking institutions to recognize that security strategies must go beyond updating old methods; they must also anticipate and respond to the risks posed by crimes that are unique to the digital era. This dual approach is essential for protecting financial systems and maintaining public trust in a rapidly digitizing world.

Overall, cybercrime in banking continues to evolve as technology advances and the complexity of digital systems increases. Banks and financial institutions must remain vigilant and continually update their security measures to protect data and assets from a variety of cyber threats. User awareness and education are also key in preventing these crimes, given that many cyber attacks exploit human weaknesses.

[46] Alzoubi et al.

[47] Pratama et al., "Cybercrime."

[48] Karpoff, "The Future of Financial Fraud."

[49] Diptiben Ghelani, Tan Kian Hua, and Surendra Kumar Reddy Koduru, "Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking," *American Journal of Computer Science and Technology* (2022) 1–8, https://doi.org/10.22541/au.166385206.63311335/v1.

Table 1. Crime Patterns Based on Perpetrators and Victims.

Crime Pattern	Perpetrator	Victim	Description
Phishing	Hacker or scammer	Individuals, bank customers	An attack that attempts to obtain personal information by masquerading as a trusted entity through fake emails or messages.
Social Engineering	Manipulator	Bank employees, customers	Psychological manipulation techniques to obtain sensitive information by exploiting the victim's trust or ignorance.
Identity Theft	Cybercriminals	Individuals, bank customers	Theft of personal information to access accounts or steal identities for illegal purposes.
Data Breach	Hacker	Financial institutions	Unauthorized access to company or customer data through a breach of security systems.
Ransomware	Cybercriminals	Financial institutions, individuals	An attack that encrypts the victim's data and demands a ransom for the decryption key.
Malware	Hackers or malware creators	Individuals, companies	Malicious software is used to steal data, spy on users, or damage systems.
System Hacking	Hacker	Financial institutions, companies	The act of gaining illegal access to a computer system or network for data theft or sabotage.
Fraud	Fraudster	Individuals, companies	The use of false or manipulated information to gain financial or other material advantage.
Credit Card Fraud	Fraudster	Individuals, bank customers	Theft of credit card information for use in illegal purchases or theft of funds.
Investment Fraud	Scammer, illegal fund manager	Individuals, investors	Offering fake investment opportunities or tricking investors into investing money for unreal rewards.

Source: processed data, 2024.

Table 1 illustrates the variety of crime methods carried out by perpetrators and the types of victims they usually target. These patterns illustrate the broad spectrum of threats encountered by individuals and organizations in the digital era. The results of the crime pattern table based on perpetrators and victims show that crimes in the banking system can be classified into several main categories based on the entities involved. In terms of perpetrators, individuals are the most common perpetrators, especially in cases of simple fraud such as phishing and identity theft. Organized criminal groups are prominent in more complex crimes such as money laundering and large-scale system hacking. State actors, though relatively rare, have a significant impact, particularly in cases of economic espionage and state-sponsored cyberattacks. In terms of victims, individuals are often targeted for fraud and data theft, while companies, including banks and other financial institutions, are more vulnerable to larger attacks such as ransomware and system hacking.

Table 1 shows that the evolution of technology has changed the landscape of banking crime, with more perpetrators using sophisticated technology to carry out their crimes. This is evident from the increasing number of cases involving organized criminal groups and state actors, who use more sophisticated and difficult-to-track methods. Individuals as perpetrators also showed adaptation in their methods, moving away from direct fraud to a more focused cyber-based attack. On the victim side, individuals remain vulnerable to various forms of fraud, but companies are experiencing an increase in financial and reputational losses from cyberattacks. This data indicates the need for more comprehensive and adaptive security strategies, both at the individual and institutional level, to address these evolving threats.

Table 2. Motives and Aims of Crime.

Type of Crime	Motive	Purpose
Phishing	Financial benefits	Obtaining personal information to steal money or identity
Social Engineering	Psychological manipulation, profit	Tricking victims into providing sensitive information or access to systems
Identity Theft	Financial gain, disguise	Accessing accounts, gaining profits with fake identities
Data Breach	Financial gain, sabotage	Obtaining sensitive data to sell or use illegally, disrupting operations
Ransomware	Ransom	Forcing victims to pay to restore access to data
Malware	Espionage, financial gain	Infecting systems to steal data, spy, or damage
System Hacking	Financial gains, challenges	Accessing a system to steal data, cause damage, or demonstrate technical skills
Fraud	Financial gain, manipulation	Tricking victims into getting money or goods
Credit Card Fraud	Financial benefits	Using credit card information for illegal transactions
Investment Fraud	Financial benefits	Tricking investors into investing money in fake schemes

Source: processed data, 2024.

Table 2 identifies the various reasons behind criminal acts in the banking system. From the data presented, economic motives are the most dominant, with perpetrators often seeking quick and easy financial gain. This motive includes acts such as theft of money, money laundering, and embezzlement of funds. In addition, political motives are also found, especially in cases involving state actors or organized criminal groups, where their goals can include destabilizing the economy or damaging the reputation of a particular country. Other goals include sabotage of the system, which is often intended to damage the financial infrastructure or cause harm to a specific target.

Analysis of the data on motives and objectives shows that financial crimes are not only driven by the desire for financial gain but can also have political and strategic dimensions. The dominant economic motive reflects the vulnerability of the financial system to exploitation by individuals or groups seeking illicit gain. However, the presence of political and sabotage motives suggests that the banking system can also be targeted in the context of broader conflicts, including inter-state conflicts or attacks by extremist groups. This underscores the importance of comprehensive security, which focuses not only on preventing theft and fraud, but also on protecting against broader and more complex threats. These results indicate the need for a more holistic security policy, including increased international cooperation and strengthening regulations and technology in addressing the various types of threats faced by the banking system.

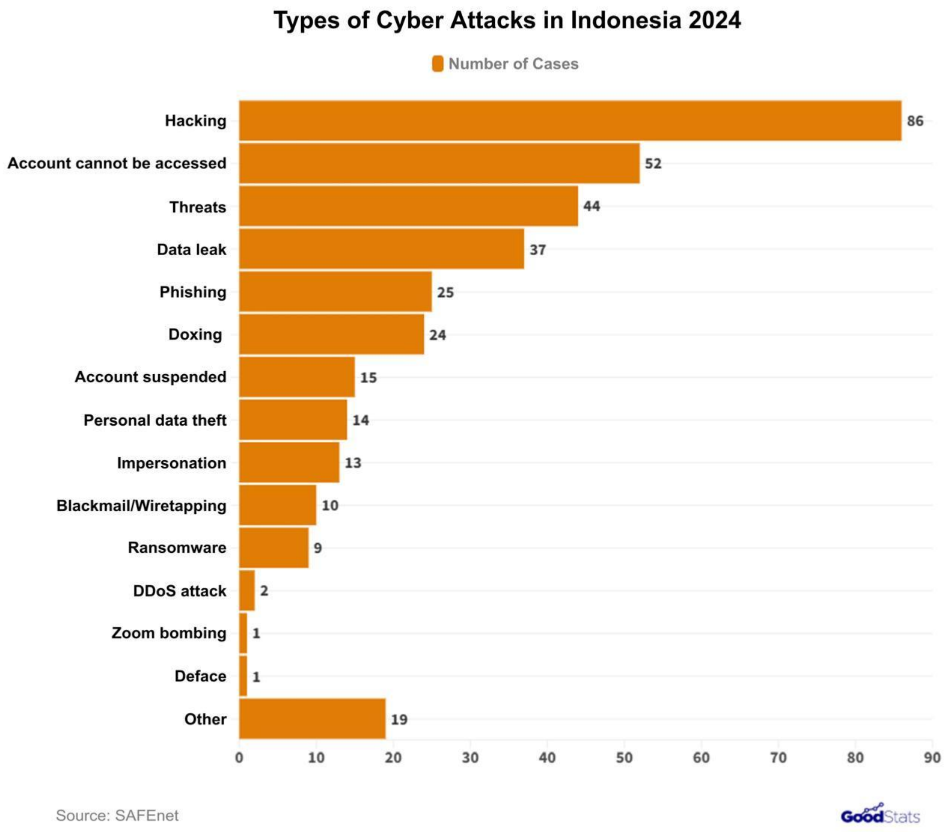


Figure 3. Types of Cyber Attacks in Indonesia 2024.
Source: SAFEnet

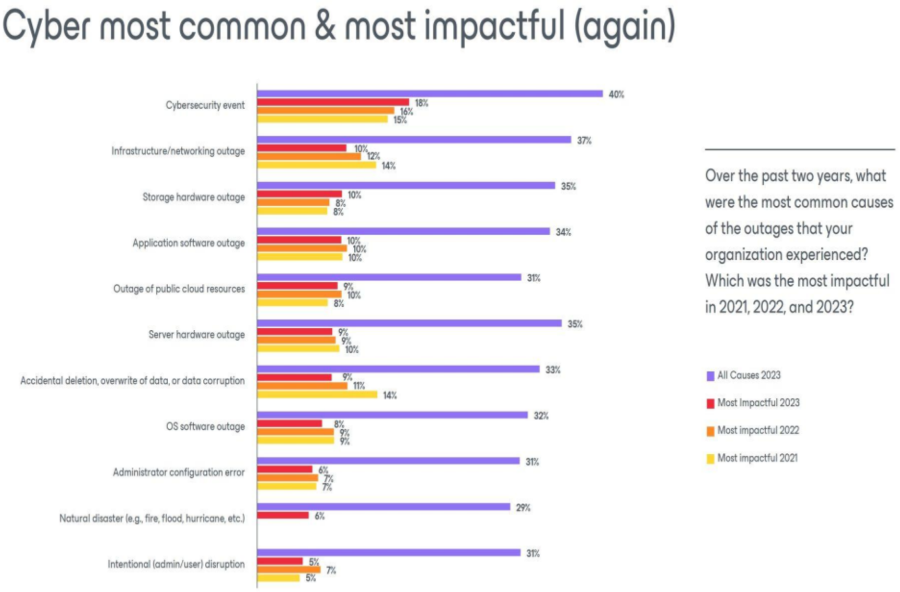


Figure 4. Cyber most Common and most Impactful.
Source: 2024 Data Protection Trends Report

Table 3. Impact of Banking Crime.

Types of Crime	Impact on Victims	Impact on Financial Institutions	Impact on the Economy and Society
Phishing	Loss of money, identity theft, emotional loss	Damaged reputation, recovery costs, decreased customer confidence	Declining public trust, increasing security costs
Social Engineering	Loss of sensitive information, financial loss	Data loss, privacy breach	Distrust of technology and online services
Identity Theft	Identity misuse, financial loss	Fraudulent claims increase, handling costs	Increased incidents of fraud, burden on legal system
Data Breach	Loss of privacy, potential financial loss	Reputational damage, lawsuits, recovery costs	Loss of customer data, impact on data security
Ransomware	Loss of data access, potential financial loss	Operational disruption, ransom fees, financial losses	Increased security costs, impact on local economy
Malware	Loss of personal data, device damage	System failure, recovery costs	Declining trust in technology, economic losses
System Hacking	Data loss, financial loss	Service disruption, loss of critical data	Financial system instability, increased security costs
Fraud	Loss of money, emotional loss	Fraud claims increase, financial losses	Declining consumer confidence, impact on the market
Credit Card Fraud	Loss of money, burden to prove innocence	Replacement costs, increased transaction monitoring	Increased transaction costs, impact on consumer confidence
Investment Fraud	Loss of investment, huge financial loss	Bad reputation, reduced investors	Increased distrust in investment markets, impact on the economy

Source: processed data, 2024.

Table 3 outlines the various consequences that arise from criminal activity in the financial sector. These impacts include direct financial losses, such as the loss of customer or bank funds, as well as the costs incurred to deal with the impact of the incident. In addition, the table also includes non-financial losses, such as damage to the reputation of the financial institution, which can lead to a loss of customer trust and a decrease in market value. Psychological impacts are also evident, where victims may experience stress or trauma due to the loss of money or identity theft. These impacts are not only felt by the individuals or entities who are directly victimized but can also affect the economy as a whole, for example through a decrease in financial stability.

Analysis of the impact of banking crime shows that the consequences of crime in this sector are complex and far-reaching. In addition to immediate financial losses, long-term impacts such as reputational damage and loss of public trust have serious implications for financial stability and trust in the banking system as a whole. For example, financial institutions that experience attacks or are involved in scandals can lose customers, which in turn reduces revenue and profitability and creates instability in the banking industry as a whole. This domino effect not only impacts the institutions involved, but also erodes public trust in the entire financial system.

Banking crime is often closely linked to Money Laundering (TPPU) and Terrorism Financing (TPPT) Crimes, as criminals exploit weaknesses in the system to hide the origins of illicit funds or support illicit activities. For example, complex money laundering methods utilize cross-border transactions and digital platforms, which often make it difficult for authorities to trace the flow of funds and minimize the potential for abuse of the banking system. The long-term impacts of these schemes include increased national and global security risks, requiring stronger oversight systems and cross-border efforts to identify and prevent such activities. This reinforces the urgency for banks and regulators to collaborate in strengthening security and building adaptive prevention policies, to maintain the integrity and public trust in the banking sector in the digital era.

Banking crime is often closely linked to Money Laundering (TPPU) and Terrorism Financing (TPPT), as criminals exploit systemic vulnerabilities to conceal the origins of illicit funds or facilitate illegal activities. Sophisticated laundering techniques such as layering through cross-border transfers, the use of shell companies, and integration via digital payment systems—create a complex financial web that challenges national and international monitoring efforts. In Indonesia, Afriansyah et al. (2023) highlight the evolution of legal and institutional frameworks in tackling terrorism financing, emphasizing the importance of stronger financial intelligence cooperation and regulatory enforcement. The digitalization of banking, while offering convenience, has also expanded the risk landscape, enabling faster, anonymous, and borderless fund flows that can be exploited for TPPT purposes.[50]

These dynamics underscore the urgent need for robust preventive frameworks and inter-agency collaboration. As Broby suggests (2021), the rapid rise of financial technology (fintech) demands a reassessment of risk models and regulatory capacities, as conventional oversight mechanisms are increasingly outdated.[51] In response, Meiryani et al. (2023) stress the growing relevance of Regulatory Technology (RegTech) in enabling real-time monitoring and automated compliance to counter TPPU and TPPT threats in Indonesia's banking sector.[52] Therefore, preserving public trust and safeguarding the integrity of the banking system in the digital era requires a proactive, adaptive approach that aligns legal frameworks, technological tools, and international cooperation in the fight against financial crime.

Transformation of Banking Crime Patterns and Their Relation to TPPU and TPPT

Technological developments in the banking system have significantly changed the pattern of banking crimes, making them increasingly complex and difficult to detect. Along with the digitalization of banking services, technology-based crimes, such as hacking, phishing, and digital fraud, have increased. This phenomenon not only has an impact on bank security threats, but also increases the risk of money laundering (TPPU) and terrorism financing (TPPT). In the international context, a report from the Financial Action Task Force (FATF) states that cybercrime and banking crimes are often used as a means to commit TPPU and TPPT, given their cross-border nature and utilizing digital anonymity. In Indonesia, the case of PT Bank Rakyat Indonesia (Persero) Tbk involving the theft of customer data in 2018 is a clear example

[50] Arie Afriansyah, Ahmad Ghozi, and M Akila Wargadalem, "Indonesia's Laws and Policies in Combatting Terrorism Financing: An Update Analysis," *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 1 (2023): 1–18, https://doi.org/10.59593/amlcft.2023.v2i1.49.

[51] Daniel Broby, "Financial Technology and the Future of Banking," *Financial Innovation* 7, no. 1 (2021): 47, https://doi.org/10.1186/s40854-021-00264-y.

[52] Meiryani Meiryani, Gatot Soepriyanto, and Jessica Audrelia, "Effectiveness of Regulatory Technology Implementation in Indonesian Banking Sector to Prevent Money Laundering and Terrorist Financing," *Journal of Money Laundering Control* 26, no. 4 (2022): 892–908, https://doi.org/10.1108/JMLC-04-2022-0059.

that banks in this country are vulnerable to digital crimes that are potentially related to TPPU and TPPT.[53]

The technological advantages of the banking system also create loopholes that are exploited by perpetrators of TPPU and TPPT. In international cases, for example, the Panama Papers in 2016 revealed a network of shell companies used to evade taxes and launder money by various world elites. This shell company scheme used banks as a channel to disguise the flow of illegal funds, showing how banks can be used for money laundering purposes on a global scale.[54] In Indonesia, many TPPU cases related to corruption have also emerged, such as the e-KTP corruption case where the proceeds of the crime were diverted through several national banks before finally being hidden or invested.[55]

The use of sophisticated technology in TPPU and TPPT modes also continues to grow. One increasingly popular method is the use of digital currency or cryptocurrency which is difficult for authorities to track. In a case study in the United States, an FBI investigation in 2021 revealed that international criminal groups used cryptocurrency to hide funds from crimes, including terrorism funding.[56] This is because the pseudonymous and difficult-to-trace nature of crypto makes it easier to transfer funds quickly and anonymously. In Indonesia, Bank Indonesia and the Financial Services Authority (OJK) have issued warnings regarding the risks of using crypto for money laundering activities, although strict regulations have not been fully implemented.[57]

On the other hand, banks and financial institutions are increasingly aware of the need to implement prevention technologies, such as Know Your Customer (KYC) and Anti-Money Laundering (AML) systems. KYC and AML help banks verify customer identities and monitor suspicious transactions that may be related to TPPU or TPPT. In Europe, the European Union issued the fifth AMLD regulation requiring transparency of customer data to minimize money laundering and terrorism financing practices.[58] In Indonesia, the OJK also requires banks to implement stronger KYC and AML systems. However, challenges remain in implementing effective regulations, especially in monitoring transactions that use high technology and are often international.[59]

Law enforcement and regulation must keep up with developments to be able to overcome increasingly complex crimes with the evolution of banking crime patterns. Collaboration between countries and institutions is important in overcoming TPPU and TPPT crimes that involve sophisticated technology and spread across borders. For example, international cooperation between Interpol, FATF, and global financial institutions helps in identifying and handling global criminal networks that use banks as a means of money laundering.[60] For

[53] Mohammad Fadil Imran, "Preventing and Combating Cybercrime in Indonesia," *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–35.

[54] Fausto Martin De Sanctis, *International Money Laundering Through Real Estate and Agribusiness: A Criminal Justice Perspective from the "Panama Papers"* (Cham: Springer International Publishing, 2017), https://doi.org/10.1007/978-3-319-52069-8.

[55] Afriansyah, Ghozi, and Wargadalem, "Indonesia's Laws and Policies in Combatting Terrorism Financing"; Riswanto Riswanto et al., "Legal Aspects in Handling Money Laundering Cases in Indonesia," *Asian Journal of Social and Humanities* 2, no. 8 (2024): 1818–23, https://doi.org/10.59888/ajosh.v2i8.318.

[56] Samira Ibrahim et al., "Cybercrimeand Cryptocurrency," *American Journal of Engineering Research* 10, no. 12 (2021): 103–6.

[57] Meiryani, Soepriyanto, and Audrelia, "Effectiveness of Regulatory Technology Implementation in Indonesian Banking Sector to Prevent Money Laundering and Terrorist Financing."

[58] Joni Rönkkö, "Key Changes of the 5th EU AML Directive and Its Effects on the Finnish Banking Sector," LUT University, last modified 2022, https://lutpub.lut.fi/handle/10024/163950.

[59] Alina Bukhtiarova et al., "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine," *Banks and Bank Systems* 15, no. 1 (2023): 98–106.

[60] O. V. Prokopenko et al., "The Role of Banks in National Innovation System: General Strategical Analytics," *Financial and Credit Activity Problems of Theory and Practice* 3, no. 30 (2019): 26–35, https://doi.org/10.18371/fcaptp.v3i30.179455.

Indonesia, cooperation with other countries in detecting and handling financial crimes can improve the security of the national banking system and protect customers from the potential impacts of these increasingly complex crimes.[61]

Efforts to Prevent and Handle Banking Crimes

Government policies and regulations play a crucial role in preventing and addressing banking crimes. Governments can set strict security standards and regulate banking practices to prevent vulnerabilities. Anti-money laundering (AML) laws and personal data protection regulations, such as the GDPR in the European Union, provide a legal framework to combat financial crimes. Bukhtiarova et al. (2023), the effectiveness of financial monitoring in the banking system depends on the implementation of strict regulations and ongoing supervision.[62] Comprehensive regulations help in identifying and mitigating financial risks, and force financial institutions to strengthen their security practices.[63]

Banking institutions implement various preventive practices to protect themselves from banking crimes. These measures include implementing strict access controls, regular audits, and fraud detection systems. According to Suh et al. (2019) reducing fraud risk factors and opportunities for fraud is an important strategy to minimize crime incidents in financial institutions.[64] In addition, banking institutions also invest in employee training to recognize and address potential threats. Abad-Segura et al. (2020) noted that the integration of advanced financial technology in banking systems can improve operational efficiency and security.[65]

Technology and innovation play a vital role in enhancing the security of banking systems. The use of technologies such as blockchain and artificial intelligence (AI) can strengthen security systems and reduce the risk of crime. Demirkan et al. (2020) explained that blockchain technology can increase data transparency and security, while AI can detect anomalies and suspicious activities faster.[66] These technologies support crime prevention by providing sophisticated tools to monitor and secure transactions and customer data.[67]

Public education and awareness are key components in preventing banking crimes. Educational programs for customers and employees on cybersecurity risks and data protection practices can reduce the likelihood of crimes occurring. Spoorthi et al. (2024) emphasized the importance of raising awareness about social engineering and phishing to protect individuals and institutions from attacks.[68] In addition, Sahoo and Kotiya (2022) showed that continuous training in security technologies can strengthen the resilience of banking institutions to cyber threats.[69] Efforts to prevent and address banking crimes require a multi-faceted approach involving government policies, banking practices, advanced technology, and public education.

[61] Fany Dewi Rengganis and Dwi Setiawan Susanto, "Evaluation of the Anti-Money Laundering Programs Implementation in Indonesia," *Integritas: Jurnal Antikorupsi* 9, no. 2 (2023): 229–40, https://doi.org/10.32697/integritas.v9i2.973.

[62] Bukhtiarova et al., "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine."

[63] Prokopenko et al., "The Role of Banks in National Innovation System."

[64] Joon B. Suh, Rebecca Nicolaides, and Richard Trafford, "The Effects of Reducing Opportunity and Fraud Risk Factors on the Occurrence of Occupational Fraud in Financial Institutions," *International Journal of Law, Crime and Justice* 56 (2019): 79–88, https://doi.org/10.1016/j.ijlcj.2019.01.002.

[65] Emilio Abad-Segura et al., "Financial Technology: Review of Trends, Approaches and Management," *Mathematics* 8, no. 6 (2020): 951, https://doi.org/10.3390/math8060951.

[66] Sebahattin Demirkan, Irem Demirkan, and Andrew McKee, "Blockchain Technology in the Future of Business Cyber Security and Accounting," *Journal of Management Analytics* 7, no. 2 (2020): 189–208, https://doi.org/10.1080/23270012.2020.1731721.

[67] Broby, "Financial Technology and the Future of Banking"; Albert Tan, David Gligor, and Azizi Ngah, "Applying Blockchain for Halal Food Traceability," *International Journal of Logistics Research and Applications* 25, no. 6 (2022): 947–64, https://doi.org/10.1080/13675567.2020.1825653.

[68] Spoorthi et al., "Impacts of Social Engineering on E-Banking."

[69] Bhagyashree Sahoo and Minal Kotiya, "E-Banking: Innovation Challenges and Opportunities," *International Journal of Research in Engineering, Science and Management* 5, no. 5 (2022): 103–8.

A combination of these strategies can significantly reduce the risk and impact of banking crimes.

Table 4. Analysis of The Roles of Various Actors.

Actor	Main Role	Prevention & Mitigation Measures	Expected Outcomes
Customers	End-users of banking services	- Enhance digital and financial literacy - Use two-factor authentication (2FA, OTP) - Report suspicious activities	Increased awareness and personal resilience against cybercrime
Banks	Service providers and financial system managers	- Implement advanced security tech (AI, biometrics, encryption) - Real-time transaction monitoring - Customer education	Strong internal security systems and secure banking services
Regulators	Supervisors and policy makers in the financial sector	- Enforce AML/CFT regulations - Conduct regular audits and compliance checks - Provide reporting tools (e.g., PPATK, GRIPS)	High regulatory compliance and early detection of suspicious activities
Government	National policy makers and legal framework guardians	- Align national and international policies - Strengthen law enforcement agencies - Invest in tech infrastructure and HR	Systemic stability and strong legal protection for all stakeholders

Source: processed data, 2024

Banking crime cases provide valuable lessons on the importance of implementing a comprehensive security system. Cases such as major data breaches expose weaknesses in existing security protocols and emphasize the need for regular technology updates. For example, Demirkan et al. (2020) highlight how blockchain technology can strengthen banking security systems by increasing transparency and reducing the possibility of fraud.[70] This realization has prompted banking institutions to implement the latest technological solutions, such as encryption and more sophisticated fraud detection systems, to protect sensitive data and reduce the risk of cyberattacks.

Another important lesson from banking crime cases is the need for tight integration of security policies and practices. Major fraud cases often reveal gaps in existing regulations or a lack of compliance with security standards. Bukhtiarova et al. (2023) note that the effectiveness of financial monitoring is highly dependent on the consistent application of regulations and strict supervision.[71] Therefore, banking institutions must actively participate in the design and implementation of security policies and ensure compliance with applicable regulations to prevent similar incidents from happening in the future.

[70] Demirkan, Demirkan, and McKee, “Blockchain Technology in the Future of Business Cyber Security and Accounting.”

[71] Bukhtiarova et al., “Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine.”

Strategy for Prevention and Handling of TPPU and TPPT in Modern Banking System

In facing the threat of TPPU and TPPT, banking institutions need to implement a comprehensive approach that combines technology, regulation, and a deep understanding of risk. One of the first steps in preventing this financial crime is through the implementation of a Know Your Customer (KYC) system, which allows banks to better verify customer identities and detect suspicious transactions early. KYC has become a standard requirement in many countries and continues to be improved as financial crime modes evolve. According to Kandachamy (2023), the implementation of strict KYC in Europe has proven effective in reducing the risk of money laundering, especially through the implementation of more accurate customer data verification.[72] In Indonesia, the Financial Services Authority (OJK) requires all banks to implement KYC as part of their TPPU and TPPT prevention strategy.

In addition to KYC, the implementation of an effective Anti-Money Laundering (AML) system is essential in identifying and stopping suspicious fund flows. AML systems work by monitoring unusual or suspicious transactions that could be indicative of money laundering or terrorism financing. In their study, Jiao (2023) and Kumar et al. (2021) showed that the integration of technology into AML systems, such as big data and machine learning, allows banks to analyze transaction data in real time and detect anomalous patterns that were previously difficult to recognize.[73] Thus, banks can respond quickly to potential TPPU and TPPT threats, minimize losses, and ensure operational transparency.

The application of blockchain technology is also starting to be considered as one way to track and reduce the risk of TPPU and TPPT. Blockchain offers additional security through transparent and difficult-to-manipulate records. In a study conducted by Dhanawat (2022) and Javaid et al. (2022), blockchain was shown to provide a strong traceability path to transactions, making it easier for regulators and financial institutions to follow the flow of funds suspected of being involved in TPPU.[74] Several countries, such as Singapore, have implemented blockchain technology in the banking sector as part of their TPPU prevention efforts, with results showing increased detection of suspicious fund flows.

On the regulatory side, international collaboration in preventing TPPU and TPPT is further strengthened through initiatives such as the Financial Action Task Force (FATF), which sets global standards to combat money laundering and terrorism financing. The FATF provides guidance for countries to adopt a uniform regulatory framework, enabling cross-border cooperation in addressing international financial crimes. Based on a report from the FATF 2021, countries that implement FATF standards have experienced a decrease in TPPU and TPPT cases, indicating the effectiveness of this policy in preventing global financial crimes.

However, the implementation of advanced policies and technologies also faces challenges, especially in terms of costs, infrastructure, and human resource competency. In Indonesia, these challenges often arise in regional banks that have limitations in implementing AML systems or blockchain technology due to limited funds. Zavoli and King (2021) stated that these obstacles

[72] Archana Gokul Kandachamy, "Overview of Anti-Money Laundering in the Banking Industry: An Explanation of AML and the Importance of It in the Banking Sector," *Management and Quality* 5, no. 3 (2023): 79–89.

[73] Mingyuan Jiao, "Big Data Analytics for Anti-Money Laundering Compliance in the Banking Industry," *Highlights in Science, Engineering and Technology* 49 (2023): 302–9, https://doi.org/10.54097/hset.v49i.8522; Ashwini Kumar et al., "Analysis of Classifier Algorithms to Detect Anti-Money Laundering," in *Computationally Intelligent Systems and Their Applications*, ed. Jagdish Chand Bansal et al. (Singapore: Springer, 2021), 143–52, https://doi.org/10.1007/978-981-16-0407-2_11.

[74] Vineet Dhanawat, "Anomaly Detection in Financial Transactions Using Machine Learning and Blockchain Technology," *International Journal of Business Management and Visuals* 5, no. 1 (2022): 34–41; Mohd Javaid et al., "A Review of Blockchain Technology Applications for Financial Services," *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 2, no. 3 (2022): 100073, https://doi.org/10.1016/j.tbench.2022.100073.

can be overcome through government support and increased training of banking employees to be more competent in handling financial crime prevention technology.[75] Thus, the success of TPPU and TPPT prevention strategies in the modern banking system requires synergy between technology, regulation, and ongoing government support.

One of the more recent and notable cases related to money laundering (TPPU) in Indonesia is the 2023 case involving suspicious fund transfers linked to illegal online gambling networks. According to the Financial Transaction Reports and Analysis Center (PPATK), billions of rupiah were traced to accounts under false identities, often using third-party intermediaries and fintech platforms to obscure the source and destination of the funds. This case highlights how digital financial services when left unchecked can be exploited for laundering criminal proceeds. It also reflects weaknesses in the verification processes of certain digital banking and e-wallet services. In response, Indonesian authorities, including Bank Indonesia and the Financial Services Authority (OJK), intensified regulatory scrutiny by revising Know Your Customer (KYC) and customer due diligence protocols, especially for fintech and peer-to-peer lending institutions. This incident demonstrates the evolving nature of TPPU threats and reinforces the urgent need for cross-sector collaboration and technological innovation in AML enforcement.

In addition to the illegal online gambling case, TPPU in the Indonesian banking sector is also closely related to terrorism financing. Cases of terrorism financing through bank transactions occur in the financing of several acts of terror carried out by terrorist groups in Indonesia. For example, several local terrorist groups use regular bank accounts to receive donations from certain parties, the funds of which are then used to finance terrorist activities. Based on data from the National Counterterrorism Agency (BNPT), it was found that terrorist groups often exploit loopholes in the transaction monitoring system at banks to obscure the origin of funds. This has prompted the Indonesian government to increase supervision of suspicious banking transactions and strengthen collaboration between PPATK, BNPT, and banking institutions to prevent terrorism financing.

The latest case in Indonesia shows the increasing complexity of risks related to Money Laundering (TPPU) and terrorism financing in the digital era. The Financial Transaction Reports and Analysis Center (PPATK) reported an increase in digital fraud and money laundering triggered by innovations in digital finance, such as electronic payments and cryptocurrency platforms. This phenomenon raises concerns in financial institutions because these digital tools can be used for cross-border money laundering without direct detection. In response, Indonesia has strengthened its digital financial threat response framework by tightening regulations related to digital identity verification and transaction monitoring. In addition, Indonesia has also focused on countering terrorism financing by improving inter-agency coordination and working closely with international partners. Recent efforts have focused on monitoring funds transferred through trading schemes and ensuring that non-profit organizations are not misused to finance terrorism. While these measures are promising, ongoing adjustments are needed to keep pace with rapid developments in financial technology and the tactics used by organized criminal groups.

Regulations in Indonesia relating to Money Laundering (TPPU) and Terrorism Financing (TPPT) have undergone significant developments in recent years. Law No. 8 of 2010 concerning the Prevention and Eradication of TPPU and Law No. 9 of 2013 concerning the Prevention and Eradication of TPPT are the main legal basis. These regulations aim to strengthen efforts to prevent, detect, and prosecute money laundering and terrorism financing practices. In addition, Indonesia has also established the Financial Transaction Reports and

[75] Ilaria Zavoli and Colin King, "The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis," *The Modern Law Review* 84, no. 4 (2021): 740–71, https://doi.org/10.1111/1468-2230.12628.

Analysis Center (PPATK) as an institution that monitors financial institutions' compliance with anti-money laundering regulations and reports suspicious transactions that can be indicated as TPPU or TPPT.

However, the main weakness of this regulation lies in its implementation, especially related to strict supervision and the application of sanctions for violations. Although PPATK is active in collecting data and reporting suspicious transactions, challenges arise in the limited resources to conduct in-depth investigations on each report. Another weakness is the gap in international collaboration, where cross-border transactions are often difficult to trace due to limited data access or differences in regulations between countries. In the context of terrorism financing, this challenge is even more complex because it involves hidden financial networks that are difficult to trace.

This study offers several recommendations to strengthen the regulation and prevention of Money Laundering (TPPU) and Terrorism Financing (TPPT) in Indonesia. First, increasing the institutional capacity of PPATK and related authorities is essential in the digital era, where the volume and complexity of financial transactions continue to rise. With the increasing use of digital payment systems, such as QRIS, fraud schemes have also evolved often involving fake merchant codes or misleading payment links circulated through online marketplaces like Shopee and Tokopedia. These tactics make it more difficult for authorities to monitor suspicious activities without sophisticated detection tools and well-trained investigators. Strengthening institutional resources, including human capital and technological infrastructure, is therefore a critical foundation for enhancing national resilience against financial crimes.

Second, the importance of international cooperation lies in the transnational nature of modern financial crime. Many recent fraud cases involve not only domestic actors but also international networks that exploit cross-border transaction systems to hide illicit flows. For example, fake delivery notifications pretending to be from major shipping services are used as a vector to extract payments, which are then funneled through online lending platforms or digital wallets and quickly transferred across jurisdictions. Without a comprehensive and transparent framework for cross-border information exchange, efforts to trace these funds often stall at national borders. Thus, collaborative engagement through global AML/CFT mechanisms will help Indonesia close critical enforcement gaps.

Third, enhancing training and public awareness among banking and fintech employees is essential to recognize red flags in transactions. A growing number of money laundering cases are linked to the misuse of personal data from online loan applications or account openings, where perpetrators use forged identities to manipulate systems. Frontline employees often encounter these irregularities first, yet lack the training to interpret them as potential threats. Increasing education and early warning mechanisms can empower these institutions to act promptly and report suspicious activities. Together, these three strategies—strengthened institutional capacity, international collaboration, and proactive financial sector training—form an integrated approach to securing Indonesia’s financial ecosystem from the evolving threats of TPPU and TPPT.

Conclusion

This study identifies a clear shift in crime patterns within the banking system, where technological advancements have transformed traditional fraud such as check and credit card scams into sophisticated forms of cybercrime including phishing, ransomware, and data breaches. These crimes reflect an evolving modus operandi in which perpetrators exploit weaknesses in digital infrastructure, often bypassing outdated security mechanisms. The study also finds that cybercrime is increasingly intertwined with Money Laundering (TPPU) and Terrorism Financing (TPPT), as international digital platforms and anonymous transactions are used to obscure the origin and purpose of illicit funds. These developments reveal not only a technical but also a regulatory and institutional vulnerability that demands a coordinated response.

This study proposes several recommendations to address these challenges. First, institutions such as PPATK must be strengthened in terms of resources and technical capabilities, particularly for monitoring the massive volume of digital transactions. Second, the financial sector including banks and fintechs should enhance internal controls by adopting AI-based systems for anomaly detection and fraud prediction. At the same time, regulatory bodies like OJK and Bank Indonesia must enforce adaptive and proactive regulations aligned with the pace of digital innovation. Third, at the industry level, collaborative international mechanisms are essential to track cross-border fund transfers, particularly those suspected to be linked with TPPU and TPPT. Lastly, comprehensive education and training programs must be provided not only to frontline employees but also to banking customers and fintech users. This is crucial for increasing digital literacy, improving threat awareness, and enabling faster institutional responses to suspicious activities. By taking these steps, stakeholders at all levels can build a more resilient, transparent, and secure digital banking environment in Indonesia.

References

Abad-Segura, Emilio, Mariana-Daniela González-Zamar, Eloy López-Meneses, and Esteban Vázquez-Cano. "Financial Technology: Review of Trends, Approaches and Management." *Mathematics* 8, no. 6 (2020): 951. https://doi.org/10.3390/math8060951.

Achim, Monica Violeta, and Sorin Nicolae Borlea. *Economic and Financial Crime: Corruption, Shadow Economy, and Money Laundering*. Vol. 20. Studies of Organized Crime. Cham: Springer International Publishing, 2020. https://doi.org/10.1007/978-3-030-51780-9.

Afriansyah, Arie, Ahmad Ghozi, and M Akila Wargadalem. "Indonesia's Laws and Policies in Combatting Terrorism Financing: An Update Analysis." *AML/CFT Journal: The Journal of Anti Money Laundering and Countering the Financing of Terrorism* 2, no. 1 (2023): 1–18. https://doi.org/10.59593/amlcft.2023.v2i1.49.

Ali, Shazeeda. "Criminal Minds: Profiling Architects of Financial Crimes." *Journal of Financial Crime* 28, no. 2 (2021): 324–44. https://doi.org/10.1108/JFC-11-2020-0221.

Alzoubi, Haitham M., Taher M. Ghazal, Mohammad Kamrul Hasan, Asma Alketbi, Rukshanda Kamran, Nidal A. Al-Dmour, and Shayla Islam. "Cyber Security Threats on Digital Banking." In *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 1–4. IEEE, 2022. https://ieeexplore.ieee.org/abstract/document/9896966/.

Azernikov, A. D., A. N. Norkina, E. R. Myseva, and K. A. Chicherov. "Innovative Technologies in Combating Cyber Crime." *KnE Social Sciences* 3, no. 2 (2018): 248–52. https://doi.org/10.18502/kss.v3i2.1550.

Broby, Daniel. "Financial Technology and the Future of Banking." *Financial Innovation* 7, no. 1 (2021): 47. https://doi.org/10.1186/s40854-021-00264-y.

Bukhtiarova, Alina, Andrii Semenog, Mila Razinkova, Nataliia Nebaba, and Józef Antoni Haber. "Assessment of Financial Monitoring Efficiency in the Banking System of Ukraine." *Banks and Bank Systems* 15, no. 1 (2023): 98–106.

Burnes, David, Marguerite DeLiema, and Lynn Langton. "Risk and Protective Factors of Identity Theft Victimization in the United States." *Preventive Medicine Reports* 17 (2020): 101058. https://doi.org/10.1016/j.pmedr.2020.101058.

Choi, Kwan, Ju-lak Lee, and Yong-tae Chun. "Voice Phishing Fraud and Its Modus Operandi." *Security Journal* 30, no. 2 (2017): 454–66. https://doi.org/10.1057/sj.2014.49.

De Sanctis, Fausto Martin. *International Money Laundering Through Real Estate and Agribusiness: A Criminal Justice Perspective from the "Panama Papers."* Cham: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-52069-8.

Demirkan, Sebahattin, Irem Demirkan, and Andrew McKee. “Blockchain Technology in the Future of Business Cyber Security and Accounting.” *Journal of Management Analytics* 7, no. 2 (2020): 189–208. https://doi.org/10.1080/23270012.2020.1731721.

Dhanawat, Vineet. “Anomaly Detection in Financial Transactions Using Machine Learning and Blockchain Technology.” *International Journal of Business Management and Visuals* 5, no. 1 (2022): 34–41.

Driel, Hugo van. “Financial Fraud, Scandals, and Regulation: A Conceptual Framework and Literature Review.” *Business History* 61, no. 8 (2019): 1259–99. https://doi.org/10.1080/00076791.2018.1519026.

Fahlevi, Mochammad, Mohamad Saparudin, Sari Maemunah, Dasih Irma, and Muhamad Ekhsan. “Cybercrime Business Digital in Indonesia.” *E3S Web of Conferences* 125 (2019): 21001. https://doi.org/10.1051/e3sconf/201912521001.

Ghelani, Diptiben, Tan Kian Hua, and Surendra Kumar Reddy Koduru. “Cyber Security Threats, Vulnerabilities, and Security Solutions Models in Banking.” *American Journal of Computer Science and Technology* (2022): 1–8. https://doi.org/10.22541/au.166385206.63311335/v1.

Gomes, Vanessa, Joaquim Reis, and Bráulio Alturas. “Social Engineering and the Dangers of Phishing.” In *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7. IEEE, 2020. https://ieeexplore.ieee.org/abstract/document/9140445/.

Hasham, Salim, Shoan Joshi, and Daniel Mikkelsen. *Financial Crime and Fraud in the Age of Cybersecurity*. New Yok: McKinsey & Company, 2019.

Hashim, Hafiza Aishah, Zalailah Salleh, Izzati Shuhaimi, and Nurul Ain Najwa Ismail. “The Risk of Financial Fraud: A Management Perspective.” *Journal of Financial Crime* 27, no. 4 (2020): 1143–59. https://doi.org/10.1108/JFC-04-2020-0062.

Hilal, Waleed, S. Andrew Gadsden, and John Yawney. “Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances.” *Expert Systems with Applications* 193 (2022): 116429. https://doi.org/10.1016/j.eswa.2021.116429.

Ibrahim, Samira, Daniel Ikechukwu Nnamani, Ojeifoh Okosun, and Olumuyiwa Ezekiel Soyele. “Cybercrimeand Cryptocurrency.” *American Journal of Engineering Research* 10, no. 12 (2021): 103–6.

Imran, Mohammad Fadil. “Preventing and Combating Cybercrime in Indonesia.” *International Journal of Cyber Criminology* 17, no. 1 (2023): 223–35.

Jakšič, Marko, and Matej Marinč. “Relationship Banking and Information Technology: The Role of Artificial Intelligence and FinTech.” *Risk Management* 21, no. 1 (2019): 1–18. https://doi.org/10.1057/s41283-018-0039-y.

Javaid, Mohd, Abid Haleem, Ravi Pratap Singh, Rajiv Suman, and Shahbaz Khan. “A Review of Blockchain Technology Applications for Financial Services.” *BenchCouncil Transactions on Benchmarks, Standards and Evaluations* 2, no. 3 (2022): 100073. https://doi.org/10.1016/j.tbench.2022.100073.

Jiao, Mingyuan. “Big Data Analytics for Anti-Money Laundering Compliance in the Banking Industry.” *Highlights in Science, Engineering and Technology* 49 (2023): 302–9. https://doi.org/10.54097/hset.v49i.8522.

Kandachamy, Archana Gokul. “Overview of Anti-Money Laundering in the Banking Industry: An Explanation of AML and the Importance of it in the Banking Sector.” *Management and Quality* 5, no. 3 (2023): 79–89.

Karpoff, Jonathan M. “The Future of Financial Fraud.” *Journal of Corporate Finance* 66 (February 2021): 101694. https://doi.org/10.1016/j.jcorpfin.2020.101694.

Kumar, Ashwini, Sanjoy Das, Vishu Tyagi, Rabindra Nath Shaw, and Ankush Ghosh. “Analysis of Classifier Algorithms to Detect Anti-Money Laundering.” In *Computationally Intelligent Systems and Their Applications*, edited by Jagdish Chand

Bansal, Marcin Paprzycki, Monica Bianchini, and Sanjoy Das, 143–52. Singapore: Springer, 2021. https://doi.org/10.1007/978-981-16-0407-2_11.

Leo, Martin, Suneel Sharma, and K. Maddulety. "Machine Learning in Banking Risk Management: A Literature Review." *Risks* 7, no. 1 (2019): 29. https://doi.org/10.3390/risks7010029.

Lokanan, Mark. "Theorizing Financial Crimes as Moral Actions." *European Accounting Review* 27, no. 5 (2018): 901–38. https://doi.org/10.1080/09638180.2017.1417144.

Masciandaro, Donato. *Global Financial Crime: Terrorism, Money Laundering and Offshore Centres*. New York: Taylor & Francis, 2017.

Meiryani, Meiryani, Gatot Soepriyanto, and Jessica Audrelia. "Effectiveness of Regulatory Technology Implementation in Indonesian Banking Sector to Prevent Money Laundering and Terrorist Financing." *Journal of Money Laundering Control* 26, no. 4 (2022): 892–908. https://doi.org/10.1108/JMLC-04-2022-0059.

Mosteanu, Narcisa Roxana, and Alessio Faccia. "Digital Systems and New Challenges of Financial Management – FinTech, XBRL, Blockchain and Cryptocurrencies." *Quality – Access to Success* 21, no. 174 (2020): 159–66.

Navaretti, Giorgio Barba, Giacomo Calzolari, José Manuel Mansilla-Fernandez, and Alberto F. Pozzolo. "Fintech and Banking. Friends or Foes?" *Friends or Foes* (2018). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3099337.

Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial Cybercrime: A Comprehensive Survey of Deep Learning Approaches to Tackle the Evolving Financial Crime Landscape." *Ieee Access* 9 (2021): 163965–86.

Payne, Brian K. "Defining Cybercrime." In *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by Thomas J. Holt and Adam M. Bossler, 3–25. Cham: Palgrave Macmillan, 2020. https://doi.org/10.1007/978-3-319-78440-3_1.

Pospisil, Bettina, Edith Huber, Gerald Quirchmayr, and Walter Seboeck. "Modus Operandi in Cybercrime." In *Encyclopedia of Criminal Activities and the Deep Web*, 193–209. IGI Global Scientific Publishing, 2020. https://doi.org/10.4018/978-1-5225-9715-5.ch013.

Pratama, Yoga, Krisna Indra Sakti, Firmawan Setyadi, Nur Ahmad Azi Ibrahim, and Ali Mukti Nur Hidayat. "Cybercrime: The Phenomenon of Crime through the Internet in Indonesia." *Proceeding International Conference Restructuring and Transforming Law* 1, no. 1 (2022): 294–301.

Prokopenko, O. V., N. V. Biloshkurska, M. V. Biloshkurskyi, and V. A. Omelyanenko. "The Role of Banks in National Innovation System: General Strategical Analytics." *Financial and Credit Activity Problems of Theory and Practice* 3, no. 30 (2019): 26–35. https://doi.org/10.18371/fcaptp.v3i30.179455.

Reichman, Nancy. "Managing Crime Risks: Toward an Insurance Based Model of Social Control." In *Risk Management*, edited by Gerald Mars and David T. H. Weir, 45–66. London: Routledge, 2020.

Rengganis, Fany Dewi, and Dwi Setiawan Susanto. "Evaluation of the Anti-Money Laundering Programs Implementation in Indonesia." *Integritas: Jurnal Antikorupsi* 9, no. 2 (2023): 229–40. https://doi.org/10.32697/integritas.v9i2.973.

Riswanto, Riswanto, Muhammad Akbar Rachmatullah, Alip Rahman, and Diky Dikrurahman. "Legal Aspects In Handling Money Laundering Cases In Indonesia." *Asian Journal of Social and Humanities* 2, no. 8 (2024): 1818–23. https://doi.org/10.59888/ajosh.v2i8.318.

Rönkkö, Joni. "Key Changes of the 5th EU AML Directive and Its Effects on the Finnish Banking Sector." LUT University. Last modified 2022. https://lutpub.lut.fi/handle/10024/163950.

Sahoo, Bhagyashree, and Minal Kotiya. “E-Banking: Innovation Challenges and Opportunities.” *International Journal of Research in Engineering, Science and Management* 5, no. 5 (2022): 103–8.

Spoorthi, M., H. L. Gururaj, V. Ambika, V. Janhavi, and H. Najmusher. “Impacts of Social Engineering on E-Banking.” In *Social Engineering in Cybersecurity*, edited by H. L. Gururaj, V. Janhavi, and V. Ambika. Boca Raton: CRC Press, 2024.

Suh, Joon B., Rebecca Nicolaides, and Richard Trafford. “The Effects of Reducing Opportunity and Fraud Risk Factors on the Occurrence of Occupational Fraud in Financial Institutions.” *International Journal of Law, Crime and Justice* 56 (2019): 79–88. https://doi.org/10.1016/j.ijlcj.2019.01.002.

Tan, Albert, David Gligor, and Azizi Ngah. “Applying Blockchain for Halal Food Traceability.” *International Journal of Logistics Research and Applications* 25, no. 6 (2022): 947–64. https://doi.org/10.1080/13675567.2020.1825653.

Trozze, Arianna, Josh Kamps, Eray Arda Akartuna, Florian J. Hetzel, Bennett Kleinberg, Toby Davies, and Shane D. Johnson. “Cryptocurrencies and Future Financial Crime.” *Crime Science* 11, no. 1 (2022): 1. https://doi.org/10.1186/s40163-021-00163-8.

Van Nguyen, Trong. “The Modus Operandi of Transnational Computer Fraud: A Crime Script Analysis in Vietnam.” *Trends in Organized Crime* 25, no. 2 (2022): 226–47. https://doi.org/10.1007/s12117-021-09422-1.

Wewege, Luigi, Jeo Lee, and Michael C. Thomsett. “Disruptions and Digital Banking Trends.” *Journal of Applied Finance & Banking* 10, no. 6 (2020): 15–56.

Zavoli, Ilaria, and Colin King. “The Challenges of Implementing Anti-Money Laundering Regulation: An Empirical Analysis.” *The Modern Law Review* 84, no. 4 (2021): 740–71. https://doi.org/10.1111/1468-2230.12628.