




Legal Certainty of Customer Protection in Banking Fraud Cases Using Artificial Intelligence

Hijriani¹, Muhammad Nadzirin Anshari Nur², Sahyunu³, Marfua Hafid¹, Adrian Maulana⁴, Dwi Yuliantari⁴

¹ Universitas Sulawesi Tenggara, Kapten Piere Tendean, Indonesia

² Universitas Halu Oleo, Kampus Hijau, Indonesia

³ Universitas Sulawesi Tenggara, Kapten Piere Tendean, Indonesia

⁴ Universitas Sulawesi Tenggara, Kapten Piere Tendean, Indonesia

hijriani@gmail.com

Abstract. The rapid development of information technology in the digitalization era has significantly impacted various aspects of society, particularly in the financial services sector. Traditional financial institutions, including banks, have transitioned to digital services, bringing both benefits and challenges, especially in ensuring the security of digital financial systems. This research focuses on the increasing fraud and cybercrime in the banking sector as banks adapt to digital platforms. It explores the effectiveness of existing regulations and the role of artificial intelligence (AI) in detecting and preventing fraud. The study employs a normative approach supported by empirical data, involving the analysis of legal documents and interviews with experts. The main findings indicate that while AI is a powerful tool for fraud prevention, its integration into the legal framework is still lacking. The study concludes that clearer regulations and enhanced AI capabilities are crucial to providing legal certainty and protecting society from the misuse of AI in banking. These findings contribute to the ongoing discussion on the need to strengthen the legal framework and security measures for fraud prevention in the rapidly evolving landscape of digital banking.

Keywords: Banking Fraud, AI, Legal Certainty, Consumer Protection

1 Introduction

The advancement of Information Technology in the digital era has influenced various aspects of society, particularly the financial services sector [1]. In this era, many financial institutions that previously operated conventionally have started transitioning to digital services. This transformation has brought significant benefits to Indonesia's economy but also presents challenges, especially concerning the security of digital financial systems that are still in development [2]. These challenges have led to an increase in cybercrime and/or fraud, which affects both service providers, such as Digital Banks, and customers as consumers [3].

Banking, as one of the financial service industries that plays a crucial role in the economy, has undergone significant changes [4]. Traditional banks have now

transformed by providing digital banking services [5]. Digital banking services allow customers to conduct transactions quickly and easily through electronic media, such as banking apps and other digital platforms. Banks are required to have adequate IT infrastructure, perform customer identification and verification as per regulations, and implement at least two-factor authentication for transaction security [6]. Additionally, new digital products must obtain approval following the applicable mechanisms, allowing all forms of transactions to be conducted independently at any time and place. However, this transition also brings new risks in terms of security and consumer protection.

In recent years, fraud cases in the banking sector have increased alongside the digital transformation that facilitates access to financial services but also opens opportunities for crime. The rise of online transactions in e-commerce increases the risk of cybercrime, while banking criminals are becoming more adaptive to digital technology, using methods such as third-party applications and public WiFi networks to commit fraud. The 2022 ACFE report, which presents fraud data by industry, shows that the banking and financial services sector had the most fraud cases, with 22.30% of all industry groups, totaling 351 cases [7]. These cases not only harm banks but also customers. In this situation, the use of artificial intelligence (AI) technology in detecting and preventing fraud becomes crucial. AI has the ability to analyze large amounts of data quickly, allowing suspicious patterns to be identified before more significant losses occur.

The Financial Services Authority (OJK) has issued several regulations related to Digital Banks, including OJK Regulation Number 12/POJK.03/2021 concerning Commercial Banks, which complements previous regulations, such as OJK Regulation Number 21 of 2023 on Digital Services by Commercial Banks. These regulations stipulate that a Digital Bank is an Indonesian legal entity bank that provides and conducts business activities through electronic channels without physical offices other than the head office or with limited physical offices, including operations by the bank together with partners, which must have a license from the relevant authorities.

The emergence of various Digital Banks in Indonesia, such as PT Bank Digital BCA, BRI AGRO, PT Bank Jago, and others, marks a new era in banking services. However, this also opens the possibility for errors or fraud, whether intentional or unintentional. One example of fraud encountered is the case of a Jenius Bank BTPN customer who lost Rp 241.85 million from their account [8].

To avoid fraud and/or cybercrime, strict supervision of the feasibility of Digital Bank electronic systems is required. The security level of these digital products is still in question, necessitating good testing procedures and implementation standards to ensure transaction security. Data from the Financial Services Authority on digital transaction growth shows that digital transactions grew much higher, by 1,556% between 2017–2020, with electronic money transactions reaching Rp786.35 trillion in 2021. This figure increased by Rp281.39 trillion (55.73%) compared to the previous year, which was only Rp504.96 trillion. This data reflects that digital banking service transactions in Indonesia have grown very rapidly in line with the development of digital behavior in society [9]. This means that with this increase, compliance by

Digital Banks with banking supervision conducted by the relevant authorities also becomes key to protecting customers.

Previous research has extensively discussed various aspects related to fraud in banking transactions, particularly with the digital transformation. Research by Hany Ayunda Mernisi Sitorus examines the legal protection of customers in digital bank transactions, focusing on electronic risks and fraud management. The supervision of digital products and services, as well as compliance by digital banks, are important aspects of the legal protection system [3]. Dzumira's research on legal aspects relevant to the digital transformation in the banking sector, including customer protection from fraud risks, focuses on policies and practices that can help prevent fraud in electronic transactions [10], Kaur et al.'s research on the legal challenges faced by digital banks in addressing cybersecurity threats, including fraud, also highlights these issues [11]. However, these studies focus more on general fraud detection and prevention methods, emphasizing legal protection and oversight of electronic systems in Digital Banks, but there is still little that specifically addresses the legal certainty of customer protection in banking cases using AI.

This study fills the gap by elaborating on various aspects to gain a clearer picture of customer protection and supervision. Additionally, this study also analyzes legal certainty in handling fraud cases involving AI technology and the protection provided to customers in banking fraud cases. This research offers significant regulatory contributions in the realm of legal protection and banking transaction security in the digital era. The results of this study are expected to serve as a reference for regulators, practitioners, and academics in developing more effective customer protection strategies amidst the rapid development of digital banking technology.

Based on the above background, this study aims to analyze the legal certainty of the protection provided to customers in handling banking fraud cases involving AI technology and to assess the effectiveness of existing regulations in facing the increasingly complex challenges of banking fraud. Thus, this study will provide an important contribution to addressing banking fraud challenges in the digital era.

2 Method

The research methodology used in this study is normative legal research supported by empirical data, employing a qualitative approach with case studies. Legal materials and data were collected through the analysis of legal documents, discussions with legal experts, and banking practitioners to obtain their perspectives on existing protections. Additionally, secondary data were sourced from the annual reports of the Financial Services Authority (OJK) and other related institutions.

3 Result and Discussion

3.1 Legal Certainty in Handling Banking Fraud Cases Involving AI Technology

In 2020, the European Banking Authority (EBA) and the European Central Bank (ECB) released a joint report on fraud data in payments. According to the report, the amount of fraud reported by the industry across the European Economic Area (EEA) reached €4.3 billion in 2022 and €2.0 billion in the first half of 2023. The losses due to fraud were distributed differently depending on the payment instrument. This report provides further insights into the trends and impact of fraud in the banking industry and underscores the importance of strong customer authentication (SCA) policies and the supporting technical standards issued by the EBA in 2021 [12].

On May 14, 2023, it was revealed that a service disruption at BSI was caused by a ransomware attack perpetrated by a group of hackers. Ransomware is a type of malicious software that locks access to the victim's computer system by encrypting data and demanding a ransom. This attack successfully infected the state-owned bank's system and held customer data hostage [13].

Increasingly sophisticated and organized cyberattacks are now capable of breaching banking security systems and stealing sensitive information. The banking sector is a vulnerable target for cyberattacks as it manages crucial data such as personal information, bank account details, and financial transactions, all of which are highly valuable to cybercriminals for identity theft. In addition to financial losses, victims of fraud may also experience psychological impacts, such as stress and anxiety, due to the loss of funds intended for daily necessities.

AI can be considered an "Electronic Agent" under the definition in Article 1(8) of the Electronic Information and Transactions Law (UU ITE), which stipulates that an "Electronic Agent is a device of an Electronic System created to carry out a specific action regarding certain Electronic Information automatically, which is operated by a Person." The concept of "automatic" in the definition of "Electronic Agent" can be applied to artificial intelligence (AI) technology as a form of an electronic agent. Under the UU ITE, the organizer of an electronic agent is essentially the organizer of an electronic system, meaning that the rights and obligations applicable to the electronic system organizer also apply to the electronic agent organizer [14].

The responsibilities of an electronic agent, as comprehensively regulated in the UU ITE, include the obligation to maintain data confidentiality, manage user personal data, protect user privacy, and provide information regarding the system being used to avoid harming users. However, when analyzed from the perspective of legal certainty theory, the regulation of AI in the UU ITE is not yet fully comprehensive, as the integration of AI technology into the legal domain should be clearly outlined without terminology that could lead to different interpretations.

AI cannot be considered a legal subject because it lacks awareness and the capacity to willfully act or bear moral responsibility for its actions, and it has no rights and obligations. Legal subjects are typically associated with entities that have

clear purposes and awareness, whereas AI is a human product that is regulated and programmed by humans. AI decision-making cannot be guaranteed as flawless without human intervention, and human authority in decision-making remains an essential element. Therefore, AI cannot perform legal acts independently and should be viewed as an intermediary or tool. The true legal subject is the person who controls or uses AI, and it is this person who is responsible for the risks posed by AI.

The issuance of the Circular of the Minister of Communication and Information Technology Number 9 of 2023 on Artificial Intelligence Ethics outlines three policies: ethical values, the implementation of ethical values, and responsibility in the utilization and development of artificial intelligence [15]. This circular is a response to the growing use of artificial intelligence in daily life. However, despite the law on AI as an electronic agent, there is a need for specific regulations that delineate the role, capabilities, limitations, and penalties related to its use.

Banking fraud regulations in Indonesia are governed by Law Number 10 of 1998 on Banking. This law includes provisions on the responsibility of banks to safeguard customer funds. Article 29(1) states that banks must protect the confidentiality and security of customer data. Additionally, Article 49 requires banks to take preventive measures against fraudulent acts that could harm customers.

The Financial Services Authority (OJK), as the regulatory body overseeing the financial services sector, plays a crucial role in regulating and supervising banking practices. Through OJK Regulation Number 38/POJK.03/2016, the OJK regulates risk management implementation in banking, including fraud risk. This regulation mandates banks to have effective internal control systems to detect and prevent fraud. Additionally, OJK Circular Letter Number 18/SEOJK.03/2017 on the Implementation of Good Corporate Governance (GCG) emphasizes the importance of transparency and accountability in bank management [16], which is a relevant step in ensuring good corporate governance and strengthening public trust in the banking sector. Data from OJK's annual reports indicate that banks implementing good corporate governance have lower fraud rates compared to those that do not.

Digitalization offers benefits for improving efficiency in various aspects. However, digitalization also presents challenges and risks for banking that must be anticipated and mitigated.

Digital banks that adopt AI face risks arising from information technology development, including potential fraud that exploits AI. Simultaneously, strong and secure telecommunications infrastructure is essential for the successful implementation of AI in digital banking, ensuring that services remain reliable and protected from security threats. Banks can develop comprehensive strategies that include AI risk management, fraud protection, and strengthening telecommunications infrastructure to ensure safe and effective AI adoption.

Additionally, to support banks in preparing for digital resilience, the OJK has developed a Digital Resilience Framework [17]. Generally, this digital resilience framework encompasses resilience to business dynamics and resilience to disruption. The Digital Resilience Framework issued by the OJK is closely related to handling banking fraud cases involving information technology. This framework is intended to be a reference for banks in preparing, facing, and recovering from operational

technology disruptions. The focus is on addressing disruptions or cyber incidents by minimizing customer losses, reputation damage, and financial losses.

The Digital Resilience Framework provides legal certainty for banks by offering a clear and definite framework for handling operational technology disruptions, which address disruptions or cyber incidents, allowing banks to be more responsive in facing fraud threats involving information technology.

Legal certainty is a principle that ensures laws are applied consistently and fairly. In banking, legal certainty can instill confidence in customers that their rights will be protected. According to John Rawls in "A Theory of Justice", legal certainty is a prerequisite for achieving social and economic justice [18]. With legal certainty, customers can feel secure in conducting transactions and investing their funds in banks.

Legal certainty in handling banking fraud cases is crucial because it ensures a sense of security for customers. Fraud can be subject to criminal sanctions, but law enforcement often faces various challenges. For example, in fraud cases involving advanced technology, the evidence required for legal proceedings is often difficult to obtain.

OJK Regulation Number 39 of 2019 on the Implementation of Anti-Fraud Strategies for Commercial Banks defines fraud as an intentional act of deviation or omission to deceive, trick, or manipulate a bank, customer, or other parties that occur within the bank's environment and/or use bank facilities, resulting in financial losses for the bank, customers, or other parties, or financial gain for the fraudster, either directly or indirectly. Through OJK Regulation Number 39 of 2019, regulators require banks to develop and implement effective anti-fraud strategies. The anti-fraud strategy must include at least four pillars: Prevention, Detection, Investigation, Reporting, and Sanctions, Monitoring, Evaluation, and Follow-up [19].

The effectiveness of regulations in protecting Indonesian banking customers from increasingly complex fraud faces various challenges. Although Indonesia has implemented several regulations, such as OJK Regulations on Consumer Protection and Bank Indonesia (BI) Regulations related to digital transaction security, the main challenge lies in consistent implementation and law enforcement. Existing regulations often struggle to keep pace with the rapid development of technology and the new *modus operandi* used by criminals.

Fraud cases involving skimming, phishing, and digital identity theft are still frequent, indicating that banking customers are not fully protected. One of the main weaknesses is the lack of understanding and digital literacy among customers, making them vulnerable to various forms of fraud. Moreover, although banks have adopted more advanced security technologies, such as two-factor authentication (2FA) and data encryption, criminals continue to seek new vulnerabilities in the system.

Law enforcement also poses a challenge, particularly in terms of coordination between relevant institutions, such as OJK, BI, and law enforcement agencies, to effectively prosecute fraudsters. Efforts to protect customers are often hampered by slow responses to fraud cases, ultimately disadvantaging customers.

Despite these challenges, there are efforts to enhance protection through new initiatives, such as strengthening regulations related to cybersecurity and increasing

customer awareness through financial education. However, to achieve optimal protection, Indonesia needs a more holistic approach that includes improving digital literacy, adopting more advanced technologies, and enforcing laws more strictly and in a coordinated manner to address increasingly complex fraud threats.

Furthermore, the effectiveness of international regulations in combating banking fraud can be implemented in various aspects: 1) Integrated international regulations can enhance the effectiveness of banking supervision, enabling countries to collaborate in identifying and stopping cross-border banking fraud [20]; 2) Regulations that strengthen transparency and sanctions can help prevent and stop banking fraud [21]. Transparency allows governments, financial institutions, and banks to monitor banking activities more effectively, while strict sanctions can serve as a significant deterrent for fraudsters; 3) International cooperation allows countries to share information and strategies, as well as develop consistent standards to address global banking crime threats [22].

In handling fraud cases, the role of the judiciary is also crucial. However, there are often challenges related to time constraints and limited resources. The legal process for bank fraud cases is lengthy and complex [23], which can lead to dissatisfaction among customers who are victims of fraud and reduce public trust in the banking system. Therefore, reform in the legal system is needed to expedite the handling of fraud cases. This includes the necessity for an information system about an early warning system, as well as a shared understanding between law enforcement and the banking sector regarding fraud prevention strategies in the banking industry [24].

Enhancing cooperation between the Financial Services Authority (OJK), Bank Indonesia, the police, and technology providers is important to strengthen oversight and response to fraud cases. Stronger law enforcement with severe penalties for financial crime perpetrators and expediting case resolution should also be prioritized. Furthermore, regulations must continually be updated to remain relevant to technological advancements and new threats, accompanied by the development of higher security standards for the banking sector. With this approach, it is hoped that the protection of banking customers can be further enhanced and be more effective in addressing increasingly complex fraud challenges.

3.2 Legal Protection for Customers in Bank Fraud Cases

Legal protection for customers in fraud cases is governed by Law No. 8 of 1999 on Consumer Protection. Customers have the right to compensation if they become victims of fraud. However, in practice, many customers face difficulties in obtaining compensation due to a lack of evidence or complex procedures.

Legal protection for customers is a key aspect in maintaining public trust in the banking system by providing a legal basis for customers to file claims if they suffer losses due to fraudulent activities. Article 4 of the Consumer Protection Act emphasizes that every consumer has the right to accurate, clear, and honest information about the products and services offered. However, in practice, many customers are unaware of their rights, leading them to feel resigned when they experience fraud.

The Financial Services Authority issues regulations to protect consumers in the financial services sector, including OJK Regulation No. 6/POJK.07/2022 on Consumer and Community Protection in the Financial Services Sector. This regulation covers principles such as adequate education, information transparency, fair treatment, protection of consumer assets and data, and efficient and effective complaint handling. In the context of legal protection for customers in bank fraud cases, this regulation ensures that customers receive clear and accurate information, along with a fast and fair complaint mechanism, thereby enhancing trust and legal certainty for customers who fall victim to fraud.

Many customers still do not fully understand their rights when facing fraud [25]. Therefore, education for customers is necessary to raise awareness of the available legal protections. Banks can also provide clear and transparent information regarding the complaint procedures and the handling of fraud cases. Additionally, OJK can play a role in educating the public through financial literacy programs.

An effective and efficient dispute resolution mechanism for customers who fall victim to fraud, by offering alternative dispute resolution through mediation, can help customers and banks reach an agreement without going through a lengthy legal process.

According to data from the Indonesian National Arbitration Board (BANI), dispute resolution through mediation has a fairly high success rate [26]. This high success rate indicates that mediation is an effective method for resolving disputes outside of court. Mediation allows disputing parties to discuss their differences privately with the assistance of a neutral third party (mediator), who helps them reach a mutually beneficial agreement. Thus, legal protection for customers can be more optimal if supported by a sound dispute resolution mechanism.

Banks have a responsibility to protect their customers from fraud risks, and there are various preventive measures that can be taken to achieve this goal. One of the most important actions is the implementation of strong and sophisticated security systems. Banks must invest in the latest security technology, such as data encryption, two-factor authentication, and real-time transaction monitoring to detect suspicious activities [27].

Moreover, banks also need to educate their customers on how to protect themselves from fraud. These educational programs can include information on common signs of fraud, how to secure personal information, and steps to take if they suspect fraud. Customers feel safer when their bank provides information and resources to protect themselves from fraud [28].

Another preventive measure is to conduct regular audits and risk assessments. Banks routinely evaluate their systems and procedures to identify potential loopholes that fraudsters could exploit. By conducting these audits, banks can take proactive steps to address weaknesses.

Despite regulations such as the Consumer Protection Act and Digital Banking Regulations being in place, the main challenge lies in the lack of digital literacy among banks, hindering their ability to handle various forms of fraud. Although advanced technology such as two-factor authentication and data encryption has been implemented, banks still struggle to maintain a competitive edge. To improve this

situation, Indonesia requires a holistic approach that includes digital literacy, adoption of advanced technology, and effective law enforcement. This can be achieved through the integration of banking regulations, increased transparency and trust, the development of international cooperation, and the enhancement of public services.

Bank Indonesia (BI) plays an important role in handling bank fraud cases through supervision and regulation [29]. These efforts include the implementation of prudential principles and Good Corporate Governance (GCG) in the banking sector [30]. Additionally, BI coordinates with other agencies such as the Financial Services Authority (OJK) and law enforcement agencies to handle fraud cases effectively and efficiently. However, in direct mediation between customers and banks, BI's role is not very dominant. Direct mediation between customers and banks is usually handled more by other institutions such as OJK or through the bank's own internal mechanisms [31]. Banking mediation is often underutilized, and BI does not have a primary task to mediate banking disputes. BI's main focus is more on prevention and supervision to ensure banks' compliance with applicable regulations, as well as coordination with related institutions for handling fraud cases.

Legal protection for customers is one of the key aspects in maintaining public trust in the banking system. OJK also plays a role in educating the public through financial literacy programs. Creating an effective and efficient dispute resolution mechanism for customers who fall victim to fraud is essential.

Consumer protection agencies play a role in protecting customers from bank fraud. These agencies are tasked with ensuring that consumer rights are respected and protected, as well as providing assistance to consumers who fall victim to fraud. In Indonesia, the National Consumer Protection Agency (BPKN) is responsible for protecting consumer rights, including in the banking sector [32]. One of BPKN's main roles is to educate consumers about their rights and how to protect themselves from fraud risks. By increasing consumer awareness of fraud risks and how to avoid them, this agency can help reduce the number of fraud victims.

In addition, BPKN also serves as a mediator between customers and banks in cases involving fraud. If a customer feels that their rights have been violated, they can file a complaint with BPKN, which will then try to resolve the issue amicably. This mediation process ensures that customers receive justice and that banks are held accountable for their actions. BPKN also has the authority to investigate banks suspected of engaging in practices harmful to consumers. If violations are found, the agency can recommend legal action or sanctions against the bank.

Consumer protection agencies play an urgent role in protecting customers from bank fraud. Through education, mediation, and oversight, they can help create a safer environment for the public to conduct transactions in the banking sector. Therefore, it is necessary for financial institutions to provide clear and efficient mechanisms for customers to file claims.

To enhance the effectiveness of banking in combating complex fraud, Indonesia needs to improve digital and financial literacy through public education and awareness campaigns. Banks must adopt advanced technologies, such as biometrics and AI, to detect fraud in real-time.

Collaboration with other institutions is also a good step in fraud prevention. Banks can work with law enforcement agencies and other organizations to share information about the latest fraud trends and effective prevention strategies. By sharing information, banks can improve their ability to detect and prevent fraud.

Overall, the preventive measures taken by banks are crucial in protecting customers from fraud risks. By implementing strong security systems, educating customers, conducting regular audits, and collaborating with other institutions, banks can create a safer environment for their customers.

4 Conclusion

Although regulations on handling banking fraud and protecting customers exist, the implementation and enforcement of these regulations still face various challenges. The presence of artificial intelligence (AI) technology in the banking system adds complexity to handling fraud cases, but AI has not yet been comprehensively regulated by law, leading to legal uncertainty.

Legal protection for customers is crucial to maintaining public trust in the banking system. Efforts that have been made, such as the implementation of risk management, anti-fraud regulations, and digital literacy, need to be enhanced in their effectiveness through stricter law enforcement and coordination among related institutions, including the Financial Services Authority (OJK), Bank Indonesia (BI), and consumer protection agencies. To address the increasingly complex threat of fraud, a more holistic approach is required, encompassing improved digital literacy, the adoption of more advanced technology, and more effective law enforcement. Additionally, international cooperation and integrated regulations can help prevent and address cross-border banking fraud.

5 Acknowledgements

Our gratitude goes to the Directorate of Research, Technology, and Community Service (DRTPM) of the Directorate General of Higher Education, Research, and Technology (Ditjen Dikristek) of the Ministry of Education, Culture, Research, and Technology (Kemendikbudristek) for funding this research program under the Fundamental Research – Regular scheme. We also thank the Rector of Universitas Sulawesi Tenggara and his team, Bank Indonesia, the Financial Services Authority (OJK), the High Prosecutor's Office of Southeast Sulawesi, as well as the research team who assisted and supported the completion of this research and the resulting article.

References

1. A. Irawati, H. B. Fadholi, A. N. Alamsyah, D. P. Dwipayana, and M. Muslih, "Urgensi Cyber Law dalam Kehidupan Masyarakat Indonesia di Era Digital," in *Proceeding of Conference on Law and Social Studies*, 2021.
2. R. T. Tambunan and M. I. P. Nasution, "Tantangan dan Strategi Perbankan Dalam Menghadapi Perkembangan Transformasi Digitalisasi di Era 4.0," *Sci-tech Journal (STJ)*, vol. 2, no. 2, pp. 148–156, 2023.
3. H. A. M. Sitorus, "Perlindungan Hukum Terhadap Nasabah Atas Fraud Pada Transaksi Bank Digital," *JISIP (Jurnal Ilmu Sosial Dan Pendidikan)*, vol. 7, no. 1, pp. 554–569, 2023.
4. B. A. I. H. Hijriani, "Justice Corrects Criminal Accountability of Fraud Banking Corporation," *ITALIENISCH*, vol. 12, no. 2, pp. 1005–1010, 2022.
5. S. B. Fatimah and A. Hendratmi, "Digitalisasi Pada Bank Mandiri Syariah di Tengah Persaingan dan Perubahan Teknologi," *Jurnal Ekonomi Syariah Teori dan Terapan* Vol. 7 No. 4 April 2020.; vol. 7, no. 4, pp. 795–813, 2020.
6. OJK, "Layanan Digital oleh Bank Umum," Otoritas Jasa Keuangan. Accessed: Aug. 28, 2024. [Online]. Available: <https://www.ojk.go.id/id/regulasi/Pages/Layanan-Digital-oleh-Bank-Umum.aspx>
7. N. Nadia, N. Nugraha, and S. Sartono, "Analisis Pengaruh Fraud Diamond Terhadap Kecurangan Laporan Keuangan Pada Bank Umum Syariah," *Jurnal Akuntansi Dan Governance*, vol. 3, no. 2, pp. 125–139, 2023.
8. CNN Indonesia, "Uang Nasabah Lagi-lagi Raib Rp241,85 Juta dari Jenius BTPN." Accessed: Aug. 28, 2024. [Online]. Available: <https://www.cnnindonesia.com/ekonomi/20210726102022-78-672153/uang-nasabah-lagi-lagi-raib-rp24185-juta-dari-jenius-btpn>
9. A. S. Putri and I. R. D. Pangestuti, "Pengaruh Layanan Digital Perbankan Terhadap Profitabilitas Bank Umum di Indonesia Tahun 2017-2022," *Diponegoro Journal of Management*, vol. 13, no. 1, 2024.
10. S. Dzomira, "Financial Consumer Protection: Internet Banking Fraud Awareness by the Banking Sector," *Banks & bank systems*, no. 11, Iss. 4 (cont.), pp. 127–134, 2016.
11. [11] M. M. Kaur, H. Kaur, and R. Kaur, "Cyber Security Attacks in Digital Banking: Emerging Security Challenges and Threats," *SAGACITY: Researchers' Perspective*, 2021, p. 95, 2022.
12. European Banking Authority, "The EBA and ECB Release a Joint Report on Payment Fraud," European Central Bank. Accessed: Aug. 30, 2024. [Online]. Available: <https://www.eba.europa.eu/publications-and-media/press-releases/eba-and-ecb-release-joint-report-payment-fraud>
13. Agdelia Meiva Azarine, "Bank BSI Pasca Serangan Siber: Mengungkap Potensi Kompensasi Bagi Nasabah – LK2 FHUI," *LEMBAGA KAJIAN KEILMUAN FAKULTAS HUKUM UNIVERSITAS INDONESIA*. Accessed: Aug. 30, 2024. [Online]. Available: <https://lk2fhui.law.ui.ac.id/portfolio/bank-bsi-pasca-serangan-siber-mengungkap-potensi-kompensasi-bagi-nasabah/>
14. E. K. Sebayang, M. Mulyadi, and M. Ekaputra, "Potensi Pemanfaatan Teknologi Artificial Intelligence Sebagai Produk Lembaga Peradilan Pidana di Indonesia," *Locus Journal of Academic Literature Review*, vol. 3, no. 4, pp. 317–328, 2024.
15. Kementerian Komunikasi dan Informatika, "Resmi Terbitkan SE, Menkominfo: Jadi Pedoman Bagi PSE Publik dan Privat," Kominfo. Accessed: Aug. 30, 2024. [Online]. Available: <https://www.kominfo.go.id/content/detail/53722/siaran-pers-no->

582hmkominfo122023-tentang-resmi-terbitkan-se-menkominfo-jadi-pedoman-bagi-pse-publik-dan-privat/0/siaran_pers

16. “Surat Edaran Otoritas Jasa Keuangan Nomor 18/SEOJK.02/2017.” Accessed: Aug. 30, 2024. [Online]. Available: <https://www.ojk.go.id/id/regulasi/otoritas-jasa-keuangan/surat-edaran-ojk-dan-dewan-komisioner/Pages/SEOJK-Tata-Kelola-dan-Manajemen-Risiko-Teknologi-Informasi-pada-Layanan-Pinjam-Meminjam-Uang-Berbasis-Teknologi-Informasi.aspx>
17. Departemen Pengaturan dan Pengembangan Perbankan Otoritas Jasa Keuangan, *Panduan Resiliensi Digital (Digital Resilience)*. 2024.
18. A. Yunus, “Aspek Keadilan Perjanjian Baku (Standard Contract) Dalam Perjanjian Kredit Perbankan,” *Maleo Law Journal*, vol. 1, no. 1, pp. 106–118, 2017.
19. B. A. I. H. Hijriani, “Legal Certainty Against Banking Fraud Criminal Liability,” *Baltic Journal of Law & Politics*, vol. 15, no. 7, pp. 1361–1366, 2022.
20. B. Rahmanda, “Hambatan Dan Upaya Pemberantasan Tindak Pidana Perbankan Di Indonesia,” 2022.
21. R. Binanggal, “Perlindungan Hukum Terhadap Nasabah Bank yang Menjadi Korban Kejahatan ITE,” *Lex et Societatis*, vol. 4, no. 5, 2016.
22. O. M. Syaputri, N. Erdila, T. Widodo, and B. Ardianto, “Peran Organisasi Internasional dalam Mempromosikan Perdamaian dan Keamanan,” *Causa: Jurnal Hukum dan Kewarganegaraan*, vol. 4, no. 9, pp. 91–100, 2024.
23. B. Fitrianto, “Aspek Hukum Pidana Pada Kejahatan Perbankan dalam Perspektif Undang Republik Indonesia Nomor 10 Tahun 1998 Tentang Perbankan,” *Jurnal SOMASI (Sosial Humaniora Komunikasi)*, vol. 1, no. 2, pp. 239–247, 2020.
24. *Liputan6.com*, “Kejagung: Kasus Fraud Perbankan Bisa Terjadi Mulai dari Teller Sampai Direksi,” *Liputan6.com*. Accessed: Aug. 30, 2024. [Online]. Available: <https://www.liputan6.com/news/read/4662931/kejagung-kasus-fraud-perbankan-bisa-terjadi-mulai-dari-teller-sampai-direksi?page=3>
25. H. Umar, R. B. Purba, S. Safaria, W. Mudiari, and H. Sariyo, *The New Strategy in Combating Corruption (Detecting Corruption: HU-Model)*. Merdeka Kreasi Group, 2021.
26. G. P. S. RM, *Arbitrase dan Mediasi di Indonesia*. Gramedia Pustaka Utama, 2006.
27. C. I. Sectors, “Cybersecurity & Infrastructure Security Agency,” 2021.
28. J. Tarigan, S. Yenewan, and G. Natalia, “MERGER DAN AKUISISI dari perspektif strategis dan kondisi indonesia (Pendekatan Konsep dan Studi Kasus),” Yogyakarta: ekuilibria, 2016.
29. A. D. Damayanti, A. Irgeuzazhara, A. Fitria, and D. D. Y. Tarina, “Peran Bank Indonesia Terhadap Kasus Fraud dalam Perbankan,” *Journal de Facto*, vol. 10, no. 2, pp. 228–247, 2024.
30. I. Budiarti, “Penerapan Prinsip-Prinsip Good Corporate Governance (GCG) Pada Dunia Perbankan,” *Majalah Ilmiah UNIKOM*, 2011.
31. S. H. Wilhelmus Renyaan, *Peranan Lembaga Mediasi Perbankan Dalam Penyelesaian Sengketa Non Litigasi*. CV. AZKA PUSTAKA, 2022.
32. O. T. G. Rondonuwu, “Kedudukan Badan Perlindungan Konsumen Sebagai Lembaga yang Membantu Pengaduan Konsumen Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen,” *Lex Privatum*, vol. 6, no. 7, 2018.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

