

Legal Review of Consumer Protection Against Digital Transaction Service Disruptions by Banking Companies in Indonesia

Wahyu Apria Ningrum¹, Anggun Nurfani²

¹Faculty of Law, University of Lampung. Email:

wahyuapria28@gmail.com

²Faculty of Law, University of Lampung.

Email:anggunurfani@gmail.com

Abstract

The development of digital technology has driven significant transformation in the banking sector, particularly through digital banking services that offer high convenience and efficiency for customers. However, behind this progress, legal problems have also emerged due to disruptions in digital transaction services, both cyber and non-cyber in nature, which can harm customers and reduce public trust in the banking system. This study aims to examine the form of legal protection for consumers and the legal responsibility of banks in dealing with digital service disruptions in Indonesia. This research uses a normative juridical method with statutory and conceptual approaches and is based on laws and regulations, legal literature, and related library studies. The results show that legal protection for digital banking consumers has been comprehensively regulated through various regulations, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions, and Financial Services Authority Regulation Number 6/POJK.07/2022. The legal responsibility of banks covers three dimensions, namely civil liability, in the form of an obligation to provide compensation for customer losses; administrative liability, in the form of sanctions from supervisory authorities for violations of prudential and system security principles; and criminal liability, if the negligence or actions of the bank contain criminal elements that cause harm to consumers. Although the existing legal framework is quite comprehensive, there are still normative gaps, especially regarding the limits of bank responsibility for non-cyber disruptions. Therefore, it is necessary to strengthen regulations, implement good digital banking governance, and

enhance supervision by the Financial Services Authority (OJK) and Bank Indonesia to ensure legal certainty, consumer protection, and public trust in the digital banking system in Indonesia.

Keywords: *Consumer protection, Bank, Transaction Services.*

Submitted: 28-10-2025; Reviewed: 09-12-2025; Accepted: 08-01-2026

A. Introduction

In today's era, the banking sector has undergone major changes with the emergence of digital banking services. These services allow customers to carry out various financial transactions independently through electronic platforms, offering greater convenience and wider access compared to traditional banking systems.¹ According to the Financial Services Authority (OJK) Regulation Number 12/POJK.03/2018, digital banking services are a form of service that allows banks to provide information, establish interactions, and facilitate transactions with customers through electronic media. These services are developed by utilizing customer data wisely and securely to provide convenience, speed, and a service experience that suits customers' needs. Through this system, customers can independently carry out various banking activities, starting from registration, account opening, and financial transactions such as cash withdrawals, payments, and transfers, to account closure. In addition, customers also have access to various services beyond banking products, such as financial consultations, investments, e-commerce transactions, and other financial needs.²

Based on data from the Financial Services Authority (OJK) in 2021, the development of digital transactions showed a very significant increase, with growth reaching 1,556% during the 2017–2020 period. The value of electronic money transactions was recorded at Rp786.35

¹ Nora Helda Sari and Muhammad Iqbal Fasa, "Customer Understanding of Digital Banking and Its Implications for Islamic Banking Performance," *Journal of Academic Media (JMA)* 2, no. 11 (2024): pp. 2-3.

² Sindy Setiawan, Azarya Dicky, and Catharina Aprila Hellyani, "The Effect of Digital Banking Service Quality on Customer Satisfaction at Bank Indonesia," *Gymnastics Proceedings 2024: Economics And Business* 4 (2024): p. 3.,

trillion in 2021. This figure increased by Rp281.39 trillion (55.73%) compared to the previous year, which was only Rp504.96 trillion. These data illustrate that digital banking transaction activities in Indonesia have grown rapidly in line with the evolving digital behavior of society.³

In the realm of digital banking transactions, there is a possibility of disruptions that can interfere with the smooth process of transactions. These disruptions may be caused by cybercrime or non-cyber disturbances. Cybercrime includes deliberate digital attacks such as hacking, phishing, data theft, or malware attacks aimed at breaching systems and harming both customers and banks. Meanwhile, non-cyber disruptions are not caused by digital criminal acts but rather by technical, operational, or environmental factors that are non-criminal in nature. In the banking sector, non-cyber service disruptions occur when banks are unable to process transactions, provide access to digital services, ATMs, or other operational functions not due to cyberattacks, but because of technical failures, physical infrastructure issues, hardware malfunctions, or failures of supporting facilities such as cooling systems or data centers.

For example, several banks in Indonesia have experienced digital transaction service disruptions caused by non-cyber or technical factors. One case was Bank Syariah Indonesia, which faced a disruption in its BSI Mobile application for three days, from May 8 to May 10, 2023. During that period, customers were unable to access transaction services, either through the application or ATMs. In this case, the bank explained that the disruption was caused by system maintenance.⁴ Furthermore, Bank Central Asia (BCA) also experienced a similar disruption on June 26, 2024, where customers were unable to carry out several transactions through BCA Mobile and MyBCA due to a system error. BCA's management stated that the disruption was purely technical in nature, with no indication of a

³ Aisya Sylvana Putri, Irene Rini, and Demi Pangestuti, "The Influence of Digital Banking Services on the Profitability of Commercial Banks in Indonesia in 2017-2022," *Diponegoro Journal of Management* 13, no. 1 (2024): p. 3., <http://ejournal-s1.undip.ac.id/index.php/dbr>.

⁴ <https://finansial.bisnis.com/read/20230510/231/1654678/gangguan-mobile-banking-sampai-3-hari-bsi-lakukan-penelusuran-serangan-siber?utm> accessed on Saturday, October 11, 2025, at 11.00 WIB.

cyberattack.⁵ Then, on September 29, 2025, BCA Mobile and blu by BCA Digital were also reported to have experienced similar disruptions. Users had difficulty logging in and performing digital transactions due to technical errors in the system. It was suspected that the issue was related to system maintenance or internal system problems, not a cyberattack.⁶ This series of cases show that non-cyber disruptions in digital banking services in Indonesia still occur quite frequently, generally caused by system maintenance, technical errors, or device malfunctions rather than digital criminal activities.

The impact of disruptions on customers and public trust due to interruptions in digital banking transaction services is a crucial aspect that needs to be examined, as such conditions not only hinder customers' economic activities but also have the potential to reduce public confidence in the stability and credibility of the digital banking system. Based on the mobile banking service disruptions experienced by several banks, such as Bank Mandiri and Bank Central Asia (BCA), these incidents can cause both material and immaterial losses for customers as well as for the banks themselves. From the material loss perspective, both banks experienced a decrease in revenue derived from fee-based income commission-based earnings from digital transactions that were delayed or failed during the disruption period. The value of these losses was estimated to reach billions of rupiah, considering the high volume of daily transactions in these nationally scaled banks. In addition, there were extra costs incurred for system repairs, technological infrastructure recovery, and the implementation of recovery plans to ensure that the system could return to normal operation.

Meanwhile, immaterial losses were reflected in the decline of customer trust and satisfaction due to the disruption of access to digital transaction services. These disruptions caused disappointment and potential reputational damage for the banks in the eyes of the public, leading to negative perceptions of the credibility and

⁵ <https://finansial.bisnis.com/read/20240626/90/1777171/mobile-banking-bca-sempat-error-manajemen-update-informasi?utm> accessed on Saturday, October 11, 2025, at 11.10 WIB.

⁶ <https://www.antaraneews.com/berita/5142273/m-banking-bca-dan-blu-error-29-september-ini-penjelasan-nya?utm> accessed on Saturday, October 11, 2025, at 11.15 WIB.

reliability of their digital banking systems. Efforts to restore reputation and maintain public trust thus become an important consequence that banks must bear in order to recover their professional image and the stability of their affected digital financial services.⁷

The development of technology has driven the banking sector to shift toward faster and more efficient digital services. However, this shift has also introduced new legal risks, such as service disruptions, data breaches, fraud, and transaction system failures. Therefore, legal protection for digital banking consumers is essential to ensure security and legal certainty for customers.⁸ Legal protection also serves to safeguard customers' rights so that they are not harmed due to errors or negligence by banks in providing digital services. These rights are emphasized in Law Number 8 of 1999 concerning Consumer Protection, which provides a legal basis for consumers to claim compensation if they suffer losses caused by the mistakes or negligence of business actors, including banking institutions.⁹

From the perspective of legal responsibility, banks as providers of digital services have both legal and moral obligations to ensure system security, protect customer data confidentiality, and provide reliable and transparent services. This responsibility is not only ethical but also regulated under Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and the Financial Services Authority Regulation (POJK) on Digital Banking Services, which emphasizes the obligation of electronic system operators to be accountable for the management and operation of the services they

⁷ <https://keuangan.kontan.co.id/news/begini-taksiran-kerugian-bca-dan-mandiri-saat-layanan-mobile-banking-alami-kendala?page=1> accessed on Saturday, October 11, 2025, at 11.22 WIB.

⁸ Yudi Kornelis, "Digital Banking Consumer Protection: Developments & Challenges," *Journal of Legal Communication (JKH)* 8, no. 1 (2022): p. 4., <https://doi.org/10.23887/jkh.v8i1.44477>.

⁹ Reza Pahlevi et al., "Legal Protection for Consumers of Banking Services Reviewed from the Perspective of the Consumer Protection Law," *Indonesian Journal of Law and Justice* 3, no. 1 (2025): p. 3., <https://doi.org/10.47134/ijlj.v3i1.4672>.

provide.¹⁰ In addition to the aspect of responsibility, legal protection also plays an important role in maintaining public trust in the digital financial system. Bank Indonesia (2023) emphasized that the level of public trust is a key factor in the success of digitizing the payment system. When customers feel legally protected, public trust in digital banks will increase, thereby strengthening the stability of the national financial system.¹¹ However, there are still regulatory gaps that make legal protection for customers less than optimal, such as the lack of clarity regarding the extent of a bank's liability for loss of funds due to disruptions or digital crimes. Therefore, strengthening legal protection and clarifying the scope of banks' responsibilities are important steps toward ensuring fairness and security for digital banking consumers in Indonesia.

The method used in this research employs a statutory and conceptual approach. The sources of legal materials consist of primary legal materials, including laws and regulations. Data collection was carried out through library research, which includes legal books, legal journals, and legislation. The method of legal material analysis used is a qualitative normative analysis, which aims to describe and assess the appropriate regulations to address the research problem regarding the legal review of consumer protection against digital transaction service disruptions by banking companies in Indonesia

B. Discussion

Legal Regulation of Consumer Protection for Digital Transaction Services in the Banking Sector

The existence of law in social life plays a role in creating peace and social order. Through law, relationships between members of society can be organized, and the interests of each party can be protected. In essence, law functions as a means of protecting human interests,

¹⁰ Ahmad Farizal et al., "Legal Protection for Consumers in Digital Banking Transactions: Bank Responsibility and Customer Rights," *Legal Sciences* 2, no. 4 (2025): p. 3.

¹¹ https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2530523.aspx?utm Accessed on Sunday, October 12, 2025, at 15.18 WIB.

manifested in the form of norms or rules that regulate social behavior. The relationship between legal subjects and objects gives rise to rights and obligations that must be guaranteed to ensure a sense of security in their implementation. Thus, legal protection serves as a guarantee and assurance for individuals to obtain their rights and fulfill their obligations in accordance with legal provisions. In a narrower sense, legal protection includes preventive and repressive efforts, both written and unwritten, which reflect the main function of law as a means to achieve peace, harmony, and balance.¹² Furthermore, Philipus M. Hadjon divides the forms of legal protection into two types. First, preventive legal protection, which gives the public the opportunity to express objections (*inspraak*) or opinions before a government decision becomes final. This type of protection aims to prevent disputes and is highly important in government actions that are based on discretionary authority. Second, repressive legal protection, which functions to resolve disputes when they occur.¹³

The trust relationship between customers and banks is a fundamental principle that underlies their interaction. A bank's performance in managing the assets entrusted by customers requires responsibility to maintain, protect, and preserve that trust. In this context, the contractual relationship serves as the main foundation of the legal relationship between banks and customers, in which the rights and obligations of each party are determined through a mutually agreed contract. Banking laws provide legal protection for customers in using banking services, which includes several important aspects, such as:¹⁴

- a. Banks are obliged to provide transparent access to information regarding their business activities and

¹² Sihombing, A. (2023). *Consumer Protection Law*. CV. Azka Pustaka. p. 5.

¹³ Muhaimin Rahman Hakim, Hirsanuddin, "Legal Protection for Customers Who Use Banking Credit Facilities (Study in PD. BPR NTB Central Lombok)," *Journal of Education and Development* 10, no. 2 (2022): p. 4.

¹⁴ Aldina Sri Wahyuni Jefry Tarantang, Ibnu Elmi A.S. Pelu, Wahyu Akbar, Rahmad Kurniawan, "Legal Protection of Bank Customers in Digital Transactions," *Morality: Journal of Legal Science* 9, no. 1 (2023): p. 6.

financial conditions to ensure openness and minimize potential losses that customers may experience.

- b. Banks are required to maintain the confidentiality of customer data, claims, and funds to prevent misuse, as part of efforts to preserve public trust in banking institutions.

Banks must ensure the security of public funds deposited through deposit insurance mechanisms, as a form of protection against the risk of fund loss caused by system failures or the bank's financial instability.

Furthermore, consumer protection can be described as a series of efforts aimed at ensuring that consumers' rights are respected and protected in every transaction involving goods and services. This concept covers several important aspects, such as product safety assurance, information transparency, and the availability of dispute resolution mechanisms. From a legal perspective, consumer protection is intended to create a balance between business actors and consumers, considering that consumers are often in a weaker position. Law Number 8 of 1999 concerning Consumer Protection (UUPK) serves as the legal foundation for consumer protection in goods and services transactions, including digital banking transaction services. The UUPK guarantees consumers' rights to accurate information, service security, and compensation for losses arising from system failures or the negligence of the bank. On the other hand, business actors—in this case, banking institutions are obligated to provide digital services that meet security standards, are transparent, and reliable .¹⁵

Article 2 of Law Number 8 of 1999 concerning Consumer Protection states that consumer protection is based on the principles of benefit,

¹⁵ Muhammad Fadly Nasution et al., "Legal Protection for Consumers in E-Commerce Transactions Based on the Consumer Protection Law," *PESHUM: Journal of Education, Social and Humanities* 4, no. 2 (2025): p.3.

justice, balance, consumer safety and security, and legal certainty. The explanation of Article 2 can be elaborated as follows:¹⁶

- a. The principle of benefit emphasizes that all activities in the implementation of consumer protection must provide the greatest possible benefit for both consumers and business actors, thereby creating a mutually beneficial relationship between the two parties.
- b. The principle of justice means that consumer protection must ensure optimal public participation and guarantee the fulfillment of rights and obligations between consumers and business actors in a fair and proportional manner.
- c. The principle of balance aims to create harmony among the interests of consumers, business actors, and the government both materially and spiritually to ensure the sustainability of a healthy economic relationship.
- d. The principle of consumer safety and security is intended to provide protection for consumers so that their safety and security are guaranteed when using, utilizing, or consuming goods and/or services offered by business actors.
- e. The principle of legal certainty stresses the importance of compliance with the law by both business actors and consumers, and ensures the presence of justice and definite legal protection from the state in the implementation of consumer protection.

The five principles above serve as an essential foundation in realizing digital banking services that prioritize customer protection. The principle of benefit requires that digital innovations provide convenience and efficiency without causing harm to customers; the principle of justice ensures that the rights and obligations between banks and customers are fulfilled proportionally; the principle of balance maintains a harmonious relationship among the interests of customers, banks, and regulators; the principle of consumer safety and security emphasizes the importance of a reliable digital system protected from risks of loss or cyber threats; and the principle of legal

¹⁶ Syaharie Jaang, "Analysis of Legal Protection for Consumers Based on the Principle of Justice," *Journal of Law and Human Rights Wara Science 2*, no. 05 (2023): p. 5.

certainty guarantees that every issue related to digital services can be resolved through a clear and fair legal mechanism.

In the context of digital banking services, consumer or customer protection is not only regulated under Law Number 8 of 1999 concerning Consumer Protection (UUPK), but is also extended through Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) and its amendment, Law Number 19 of 2016. The ITE Law provides the legal foundation for the implementation of electronic transactions, including digital banking services, covering aspects such as personal data security, information authenticity, and the validity of electronic transactions, which are explained in the following articles:

- a. Article 4 letters (c) and (d) of the ITE Law affirm every individual's right to legal protection in the use of information technology, as well as the right to data security and integrity.
- b. Article 15 paragraph (1) of the ITE Law requires electronic system providers (including digital banks) to operate systems that are reliable and secure, and to take responsibility for their operation.
- c. Article 26 of the ITE Law also provides protection for personal data as part of an individual's right to privacy, which must be kept confidential by electronic system providers, including banking institutions.

This provision aligns with Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE), which reinforces the obligation of electronic system providers to maintain the confidentiality, integrity, and availability of consumers' personal data. In the banking context, this regulation is further strengthened by Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector, which applies to both conventional and digital bank customers. This regulation emphasizes that every financial institution must implement the principles of transparency, fairness, reliability, data security, and effective complaint handling in all of its business

activities. The three main responsibilities of financial institutions mentioned earlier are explained in detail as follows:

- a. Providing accurate, clear, and non-misleading information
Articles 6 and 7 of POJK No. 6/POJK.07/2022 emphasize that financial institutions are required to provide transparent and accurate information to consumers from the very beginning whether in the form of promotions, product offerings, or service agreements. This includes detailed explanations regarding fees, risks, benefits, and terms of banking products or services; a prohibition against providing manipulative, incomplete, or misleading information that could harm consumers; and an obligation to ensure that every customer fully understands their rights and obligations before using digital banking products or services. For example, digital banks must explain the risks of using online services such as potential system disruptions or transaction delays so that consumers can make informed decisions.
- b. Ensuring the security and confidentiality of customer data
Articles 11 to 13 of POJK No. 6/POJK.07/2022 regulate the obligation of financial institutions to maintain the security, integrity, and confidentiality of consumers' personal data.
- c. Handling Consumer Complaints with an effective mechanism
Articles 34 to 39 of POJK No. 6/POJK.07/2022 require every financial institution to have a clear, fast, and fair mechanism for handling consumer complaints. This measure aims to ensure legal certainty and fairness for customers while also strengthening public trust in the digital banking system.

Referring to POJK No. 6/POJK.07/2022 mentioned above, this regulation provides a fairly comprehensive legal protection framework for digital banking customers, covering aspects such as information transparency, data security, and consumer dispute resolution. This regulation also serves as a concrete implementation of both preventive and repressive legal protection, as recognized in the theory of consumer protection law.

Legal Responsibility of Bank Indonesia for Digital Transaction Service Disruptions in Indonesia

In the era of digital transformation, marked by the increasing use of electronic-based banking services, new risks have also emerged such as cyberattacks, phishing, and the leakage of customers' personal data. This situation requires banks not only to perform their financial intermediation functions but also to ensure legal protection for consumers against potential losses arising from digital system disruptions. Therefore, the legal responsibilities of banks are strictly regulated through various legal instruments, including the Consumer Protection Law, the Banking Law, and regulations issued by the Financial Services Authority (OJK).

In general, a bank's responsibility is rooted in its contractual relationship with the public as users of banking services, in which this agreement gives rise to obligations for each party.¹⁷ From a legal perspective, the position of banks as financial service providers places them within the scope of responsibility as regulated under Law Number 8 of 1999 concerning Consumer Protection (UUPK). Based on the provisions of Article 19 of the UUPK, business actors are required to provide compensation, restitution, or replacement for services that do not conform to the promises made to consumers. In the context of digital service disruptions, including customer data breaches, this provision reinforces the concept of strict liability, which imposes responsibility on banks without the need to prove fault or negligence.

In addition, the provisions in Law Number 10 of 1998 concerning Banking and Law Number 21 of 2008 concerning Islamic Banking strengthen the aspect of bank accountability. Banks are required to conduct their business activities based on the principle of prudence as stipulated in Article 29 paragraph (2) of the Banking Law and to ensure the confidentiality of customer data as stated in Article 40 paragraph (1) of the same law. In the event of a data breach or misuse of customer information, banks bear legal responsibility for any

¹⁷ Gentur Cahyo Setiono and Irham Rahman, "Bank Responsibility as a Form of Legal Protection for Banking Contract Customers," *Legal Transparency* 5, no. 1 (2022).

resulting losses. This principle aligns with the bank's obligation to provide accurate and transparent information regarding transaction risks to customers.¹⁸ Therefore, violations of these obligations may result in legal consequences, either in the form of civil lawsuits or administrative sanctions imposed by the relevant authorities.

If a dispute arises between a bank and a customer due to digital service disruptions, the resolution mechanism can be pursued through either litigation or non-litigation channels. Customers have the right to file a lawsuit in the district court based on the losses they have suffered. However, non-litigation dispute resolution through mediation or negotiation is often considered more efficient, particularly through institutions such as the Consumer Dispute Settlement Agency (BPSK) or the Alternative Dispute Resolution Institution for the Financial Services Sector (LAPS SJK). In terms of complaint handling, banks are obligated to provide 24-hour customer service mechanisms, respond proportionally to complaints, and offer compensation if the customer's claim is proven to be valid.

Thus, the legal responsibility of banks in the digital banking era is not only oriented toward fulfilling contractual obligations but also includes aspects of legal protection for consumers. Banks are required to maintain the reliability of electronic systems, ensure the confidentiality of personal data, and apply the principles of prudence and transparency. In the Indonesian legal system, the legal responsibility of banks has a broad scope and consists of three main aspects: civil, criminal, and administrative liability.

1) Civil Liability

Civil liability is a central aspect of legal protection for customers, especially amid the development of digital banking services that present increasingly complex risks of fund loss and personal data breaches.¹⁹ In the context of consumer protection law, civil liability

¹⁸ Ema Irmawati, John Pieries, and Wiwik Sri Widiarty, "Legal Protection of Personal Data of Bank Customers Using Mobile Banking in the Perspective of Law No. 27 of 2022 concerning Data Leakage," *Syntax Admiration Journal* 5, no. 1 (2024): 12–27.

¹⁹ Chika Ghassani, Fadhil Pratama Putra, and Zainudin Firdaus, "Juridical Analysis of Civil Liability for the Leakage of Customer Personal Data by Pt Bank Central Asia Kupang

emphasizes the importance of providing fair compensation to consumers who suffer losses due to the use of banking services, whether caused by system failures, negligence by the bank, or breaches of data security.²⁰ Therefore, a bank's civil liability does not solely arise from the contractual relationship between the bank and its customers, but also encompasses general legal principles that protect consumers as the weaker party in their legal relationship with business actors.

Normatively, the civil liability of banks is based on two main legal foundations: Law Number 8 of 1999 concerning Consumer Protection (UUPK) and the Indonesian Civil Code (KUHPerdata). Under the UUPK, banks as business actors are obligated to provide compensation, restitution, or replacement for services that do not conform to the agreement or the promises made to consumers. This provision also covers losses arising from threats to customers' personal data, including cyber incidents that affect fund security. Forms of compensation may include;

- a. Refund of funds;
- b. Replacement with services of an equivalent value;
- c. Or other forms of compensation mutually agreed upon by the bank and the customer.

The Consumer Protection Law (UUPK) also stipulates that compensation must be provided within a maximum period of seven days from the date of the transaction, and it allows consumers the option to seek resolution through the Consumer Dispute Settlement Agency (BPSK) or the courts if the bank fails to fulfill its obligations.

In addition to the UUPK, the bank's civil liability is further elucidated by the principle of Unlawful Acts (PMH) as regulated in Article 1365 of the Indonesian Civil Code. This provision states that any act in violation of the law that causes harm to another obliges the

Branch (Study of the Decision of the Kupang District Court Number 230/PDT. G/2022/PN KPG)," *Juris Prudentia: An Excellent Law Journal* 7, no. 2 (2025).

²⁰ Rayvind Onggianto and Gatot P Soemartono, "Legal Responsibility for Inconsistencies in Information in Credit Agreements by Financial Services Business Actors," *Domain Research: Journal of Multidisciplinary Research and Development*. 6, no. 4 (2024): 1118–32.

perpetrator to make restitution for the loss. In practice, actions or omissions by the bank that result in data breaches, loss of funds, or disruptions to digital services may be categorized as PMH if elements of fault or negligence are proven. Furthermore, specific regulations contained in Law Number 21 of 2008 concerning Islamic Banking as well as various Financial Services Authority Regulations (POJK) reinforce the obligation of banks to be accountable for losses suffered by customers. This accountability is inseparable from the principles of civil liability that encompass several aspects:²¹

- a. The principle of liability based on fault implies that an individual may be held accountable if it is proven that they have committed a wrongful act. This aligns with Article 1365 of the Indonesian Civil Code, which requires compensation for losses resulting from unlawful acts.
- b. The presumption of liability principle places the burden of proof on the defendant, who is presumed responsible until proven otherwise. This principle encourages accountability for all losses arising from wrongful conduct.
- c. The principle of presumption against liability applies only to consumer transactions with limitations that can be justified by common sense.
- d. The principle of presumption against liability applies only to consumer transactions with limitations that can be justified by common sense.
- e. The principle of strict liability establishes responsibility regardless of fault, though exceptions such as force majeure may apply.

Nevertheless, there are certain exceptions that may exempt the bank from civil liability. One such exception arises when the bank can demonstrate that the customer's loss was caused by the customer's own fault, such as negligence in maintaining the confidentiality of their PIN, OTP code, or other personal data. In such cases, liability shifts to the customer as a consequence of their negligence. Overall,

²¹ Dewi Fatmala Putri, Widya Ratna Sari, and Faricha Lita Nabbila, "Analysis of BSI Customer Protection Against Data Leakage in Using Digital Banking," *Scientific Journal of Economics and Management* 1, no. 4 (2023): 173–81.

the bank's civil liability in the context of consumer legal protection in the digital era is both broad and complex. Banks are not only obligated to provide compensation for financial losses but are also responsible for data security, service transparency, and the reliability of the digital systems utilized. The principles of strict liability, fault-based liability, and sectoral regulations collectively reinforce the consumer's position as a party meriting protection from systemic risks and institutional negligence. Therefore, the consistent application of civil liability is a crucial prerequisite for achieving justice, legal certainty, and public trust in Indonesia's digital banking system.

2) Administrative Responsibility

Administrative liability constitutes a form of accountability arising from violations of statutory regulations in the financial services sector, particularly with respect to compliance obligations stipulated by the Financial Services Authority (OJK) and Bank Indonesia (BI).²² In the context of consumer protection, administrative liability serves as a public oversight instrument that underscores the bank's obligation to adhere to the principles of prudence, information transparency, and the security of customer systems and data in digital transaction services.²³ The normative basis of administrative liability for banks is established in various sectoral regulations issued by the Financial Services Authority (OJK) and Bank Indonesia (BI). One of the principal provisions is Financial Services Authority Regulation Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector, Article 2, which affirms that the financial services sector must implement the principle:

- a. education;
- b. Openness and transparency of information;
- c. Fair treatment and responsible business conduct;

²² M Irwansyah Putra, Bismar Nasution, and Ramli Siregar, "The Role of Financial Services Authorities in Regulating and Supervising Banks," *Transparency Journal of Economic Law* 2, no. 1 (2013): 14659.

²³ Muhammad Irvan Syafri and Harits Abdurrahman, "OJK's Supervision Strategy for Digital Banking Services in Ensuring Legal Compliance and Consumer Protection," *Media Legal Indonesia (MHI)* 3, no. 3 (2025).

- d. Protection of consumer assets, privacy, and data; and
- e. Effective and efficient complaint handling and dispute resolution.

Financial Service Providers (PUJK), including banks, are obliged to maintain the confidentiality and security of consumers' personal data. Negligence on the part of banks in fulfilling this obligation may result in administrative sanctions, such as written warnings, restrictions on business activities, or monetary fines of up to IDR 15,000,000,000.00, as stipulated in Article 45 of POJK 6/2022. This provision illustrates that aspects of data protection and digital risk management have become an integral part of the legal responsibilities of banks in the era of information technology-based banking.²⁴

In addition, Financial Services Authority Regulation Number 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks also serves as an important foundation for enforcing administrative liability. According to Article 12, which stipulates:

"Banks are required to ensure the continuity and stability of Information Technology operations and to mitigate risks that have the potential to disrupt the bank's operational activities."

According to Article 16, which state:

"Banks are required to ensure that information security is implemented effectively with due regard to at least the following considerations:

- a. Information security measures aimed at ensuring that managed information remains confidential (confidentiality), intact (integrity), and accessible (availability) in an effective and efficient manner, with due regard for regulatory compliance;
- b. Information security implemented across technological aspects, human resources, and processes in the use of Information Technology;

²⁴ Diana Afifah, "Consumer Protection in the Financial Services Sector in the Case of Ransomware Cyber Attack That Hit Banks," *JIIIP-Scientific Journal of Education* 6, no. 11 (2023): 9318–23.

- c. Information security measures applied based on the results of risk assessments conducted on the information held by the bank; and
- d. Availability of incident management systems in the context of information security."

This regulation underscores the bank's obligation to ensure the continuity, reliability, and security of information technology systems through the application of effective risk management. Violations of these provisions may result in administrative sanctions, such as written warnings, downgrading the bank's soundness rating, suspension of certain business activities, or listing bank officials as having failed the fit and proper test. Thus, non-compliance by banks with information technology risk management not only constitutes a breach of internal obligations, but also has the potential to cause systemic disruptions to public trust and consumer protection.

Provisions on administrative liability also originate from Law Number 10 of 1998 concerning Banking, which grants authority to Bank Indonesia, and now to the Financial Services Authority (OJK), to impose sanctions on banks that fail to comply with banking laws. These sanctions may include fines, written warnings, assessment downgrades, prohibition from participating in clearing activities, suspension of certain business operations, dismissal of bank management, and the inclusion of management or staff in the list of discredited individuals in the banking sector. The primary purpose of these sanctions is not only repressive but also preventive, ensuring that banks consistently operate in accordance with governance standards and the principle of prudence. The main factors triggering administrative liability include

- a. Violations of the prudential principle,
- b. Negligence in safeguarding systems and data,
- c. As well as a lack of transparency of information to the public.

Violations of the prudential principle occur when banks fail to maintain the security of their network or server systems on digital applications. For instance, in the cases of disruptions to the Mandiri Online service and the cyberattack on Bank Syariah Indonesia (BSI)

in 2023, weaknesses were identified in the management of digital security systems. These failures represent breaches of the prudential obligation and risk management duty that banks are required to uphold to ensure the reliability of electronic systems.

Accordingly, the legal protection system for customers in digital transactions is comprehensive and layered, with each type of violation potentially resulting in different legal consequences depending on the nature of the error. This legal protection not only seeks to provide compensation for sustained losses but also serves to guarantee accountability and legal certainty in digital banking practices. Therefore, banks are required to implement the principles of prudential banking, compliance, and proportional legal responsibility towards their customers. In the increasingly complex era of digital banking transformation, such legal responsibility serves as a crucial foundation for creating a balance between service innovation and the protection of consumer rights as legal subjects safeguarded by the state.

3) Criminal Liability

In the context of digital banking, criminal liability arises when the bank or its management commits unlawful acts that directly cause harm to consumers, particularly in cases involving intent or gross negligence.²⁵ Unlike civil liability, which is compensatory in nature, and administrative liability, which serves a regulatory oversight function, criminal liability is repressive, aiming to provide a deterrent effect and safeguard the integrity of the national financial system. Therefore, the existence of criminal sanctions forms an integral part of multidimensional legal protection encompassing civil, administrative, and criminal law simultaneously.

From a legal perspective, the potential for criminal prosecution of banks or their management is grounded in various statutory regulations, including Law Number 10 of 1998 concerning Banking, Law Number 11 of 2008 in conjunction with Law Number 19 of 2016

²⁵ Dina Elisa Putri, Elly Sudarti, and Elizabeth Siregar, "Fraud Crimes Through Digital Applications (The Idea of Accountability by Banks)," *PAMPAS: Journal of Criminal Law* 5, no. 1 (2024): 72–87.

concerning Electronic Information and Transactions (ITE Law), as well as the Indonesian Penal Code (KUHP). In the context of digital banking, criminal liability may arise in cases of serious violations of the prudential principle, misuse of customers' personal data, or the allowance of insecure systems resulting in substantial losses to consumers. The Banking Law explicitly states that the imposition of administrative sanctions by supervisory authorities (Bank Indonesia or OJK) does not preclude the possibility of criminal liability, as underscored by the provision "without prejudice to criminal stipulations" in Articles 47, 47A, 48, 49, and 50A. Thus, if an administrative violation contains criminal elements, perpetrators may still be subject to criminal penalties even if administrative sanctions have already been applied.

The imposition of criminal liability on banks or their management may occur through two mechanisms: independent criminal prosecution and cumulative criminal prosecution.²⁶ Independent criminal charges mean that criminal proceedings can be conducted separately even if the bank has provided compensation or damages to the aggrieved customer. This is in line with the principle in consumer protection law which emphasizes that the payment of damages does not negate the state's right to press criminal charges if there are elements of crime or gross negligence.²⁷ Meanwhile, in cumulative criminal charges, criminal liability can be enforced concurrently with civil liability, for example when bank executives are required to pay compensation and are also sentenced to criminal penalties for committing crimes involving violations of public law.

Within the framework of criminal law, banks can be held criminally liable on the basis of individual fault (personal liability) or corporate fault (corporate criminal liability). Based on the doctrine of vicarious liability, corporations such as banks can be held criminally liable if a criminal act is committed by a director or employee within the scope of their work for the benefit of the corporation. In this case, the

²⁶ Yohana Yohana and Alpi Sahari, "Criminal Liability of Banking Corporations," *Mercatoria Journal* 10, no. 1 (2017): 32–44.

²⁷ Sri Mahanur Lakoi, Sabrina Hidayat, and Fuad Nur, "Corporate Criminal Liability Based on Consumer Protection Law That Causes Losses," *Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research* 2, no. 1b (2025): 1694–1702.

criminal liability of banks can take the form of fines, freezing of business activities, or even revocation of operating licenses, while individuals who are directly responsible can be sentenced to imprisonment. This doctrine has been accepted in the Indonesian legal system through various jurisprudence and regulations, including the ITE Law and the Banking Law, which recognize the possibility of imposing criminal penalties on legal entities

Although most cases of violations in digital banking services are resolved through civil mechanisms such as compensation, this choice of resolution does not eliminate the potential for criminal liability. Criminal law works independently of civil and administrative resolutions, as affirmed in the *ne bis in idem* principle, which only applies when there is similarity in the parties, actions, and legal basis. Thus, even if customers choose to resolve disputes through non-litigation mechanisms such as the Consumer Dispute Resolution Agency (BPSK) or the Alternative Dispute Resolution Institution (LAPS SJK), criminal proceedings may still be pursued if criminal elements are found in the act. This demonstrates that legal protection for consumers is multi-layered and complementary.

Thus, the criminal liability of banks or their management in the context of digital banking services is an inevitable legal consequence in the event of a serious violation of legal obligations that protect customer rights. The existence of criminal penalties serves not only as a means of repression, but also as a preventive mechanism to foster a culture of compliance, prudence, and integrity in digital banking governance. The strict and proportional application of criminal liability will strengthen the legal protection system for consumers, while ensuring that banks as financial institutions have full accountability for the security of customer transactions and data in this risk-filled digital era

C. Conclusion

Based on normative studies, such legal protection is regulated in various laws and regulations, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 11 of 2008

concerning Electronic Information and Transactions and its amendments, Law No. 10 of 1998 concerning Banking, and Financial Services Authority Regulation No. 6/POJK.07/2022 concerning Consumer Protection in the Financial Services Sector. Substantively, the legal responsibility of banks covers three main aspects. Civil liability, which is the bank's obligation to compensate customers for losses resulting from negligence or system failures under its control, as stipulated in Article 19 of the UUPK and Article 1365 of the Civil Code. Administrative liability, in the form of sanctions imposed by the Financial Services Authority or Bank Indonesia for violations of the principles of prudence, system security, or violations of digital service standards as stipulated in POJK No. 6/POJK.07/2022 and POJK No. 38/POJK.03/2016. Meanwhile, criminal liability arises if the bank's negligence or actions cause systemic losses to customers or violate criminal law provisions in the field of information technology as stipulated in the ITE Law and the Criminal Cod.

The results of the study show that the legal protection system for digital banking customers in Indonesia has a comprehensive and multi-layered legal basis, but there are still normative gaps, especially in terms of clarity regarding the limits of banks' liability for losses resulting from non-cyber service disruptions. Therefore, strengthening oversight mechanisms, implementing good digital banking governance, and improving regulations are important steps to ensure legal certainty, consumer protection, and public trust in the digital banking system in Indonesia.

References

Book:

Sihombing, A. (2023). *Consumer Protection Law*. CV. Azka Pustaka.

Journal:

Afifah, Diana. "Consumer Protection in the Financial Services Sector in the Case of Ransomware Cyberattacks That Hit Banks."

JHIP-Scientific Journal of Education 6, no. 11 (2023): 9318–23.

Ahmad Farizal et al., "Legal Protection for Consumers in Digital Banking Transactions: Bank Responsibility and Customer Rights," *Legal Sciences* 2, no. 4 (2025).

Aisya Sylvana Putri, Irene Rini, and Demi Pangestuti, "The Influence of Digital Banking Services on the Profitability of Commercial Banks in Indonesia in 2017-2022," *Diponegoro Journal of Management* 13, no. 1 (2024): p. 3., <http://ejournal-s1.undip.ac.id/index.php/dbr>.

Aldina Sri Wahyuni Jefry Tarantang, Ibnu Elmi A.S. Pelu, Wahyu Akbar, Rahmad Kurniawan, "Legal Protection of Bank Customers in Digital Transactions," *Morality: Journal of Legal Science* 9, no. 1 (2023).

Ghassani, Chika, Fadhil Pratama Putra, and Zainudin Firdaus. "Juridical Analysis of Civil Liability for the Leakage of Customer Personal Data by Pt Bank Central Asia Kupang Branch (Study of the Kupang District Court Decision Number 230/PDT. G/2022/PN KPG)." *Juris Prudentia: Journal of Exceptional Law* 7, no. 2 (2025).

Irmawati, Ema, John Pieries, and Wiwik Sri Widiarty. "Legal Protection of Personal Data of Bank Customers Using Mobile Banking in the Perspective of Law No. 27 of 2022 concerning Data Leakage." *Journal of Syntax Admiration* 5, no. 1 (2024): 12–27.

Lakoi, Sri Mahanur, Sabrina Hidayat, and Fuad Nur. "Criminal liability of companies under consumer protection laws that cause losses." *Journal of Multidisciplinary Inquiry in Science, Technology and Educational Research* 2, no. 1b (2025): 1694–1702

Muhaimin Rahman Hakim, Hirsanuddin, "Legal Protection for Customers Who Use Banking Credit Facilities (Study in PD. BPR NTB Central Lombok)," *Journal of Education and Development* 10, no. 2 (2022).

- Muhammad Fadly Nasution et al., "Legal Protection for Consumers in E-Commerce Transactions Based on the Consumer Protection Law," *PESHUM: Journal of Education, Social and Humanities* 4, no. 2 (2025).
- Nora Helda Sari and Muhammad Iqbal Fasa, "Customer Understanding of Digital Banking and Its Implications for Islamic Banking Performance," *Journal of Academic Media (JMA)* 2, no. 11 (2024).
- Onggianto, Rayvind, and Gatot P Soemartono. "Legal Responsibility for Inconsistencies in Information in Credit Agreements by Financial Services Business Actors." *Domain Research: Journal of Multidisciplinary Research and Development* 6, no. 4 (2024): 1118–32.
- Putra, M Irwansyah, Bismar Nasution, and Ramli Siregar. "The Role of the Financial Services Authority in Regulating and Supervising Banks." *Transparency Journal of Economic Law* 2, no. 1 (2013): 14659.
- Putri, Dewi Fatmala, Widya Ratna Sari, and Faricha Lita Nabbila. "Analysis of BSI Customer Protection Against Data Leakage in Using Digital Banking." *Scientific Journal of Economics and Management* 1, no. 4 (2023): 173–81.
- daughters, Dina Elisa, Elly Sudarti, and Elizabeth Siregar. "Fraud Through Digital Applications (The Idea of Accountability by Banks)." *PAMPAS: Journal of Criminal Law* 5, no. 1 (2024): 72–87.
- Reza Pahlevi et al., "Legal Protection for Consumers of Banking Services Reviewed from the Perspective of the Consumer Protection Law," *Indonesian Journal of Law and Justice* 3, no. 1 (2025): p. 3., <https://doi.org/10.47134/ijlj.v3i1.4672>.
- Setiono, Gentur Cahyo, and Irham Rahman. "Bank Responsibility as a Form of Legal Protection for Banking Contract Customers." *Legal Transparency* 5, no. 1 (2022).
- Sindy Setiawan, Azarya Dicky, and Catharina Aprila Hellyani, "The Effect of Digital Banking Service Quality on Customer

Satisfaction at Bank Indonesia," *Gymnastics Proceedings 2024: Economics And Business* 4 (2024).

Syafri, Muhammad Irvan, and Harits Abdurrahman. "OJK's Supervision Strategy for Digital Banking Services in Ensuring Legal Compliance and Consumer Protection." *Media Hukum Indonesia (MHI)* 3, no. 3 (2025).

Syaharie Jaang, "Analysis of Legal Protection for Consumers Based on the Principle of Justice," *Journal of Law and Human Rights Wara Science* 2, no. 05 (2023).

Yohana, Yohana, and Alpi Sahari. "Criminal Liability of Banking Corporations." *Mercatoria Journal* 10, no. 1 (2017): 32–44.

Yudi Kornelis, "Digital Banking Consumer Protection: Developments & Challenges," *Journal of Legal Communication (JKH)* 8, no. 1 (2022):., <https://doi.org/10.23887/jkh.v8i1.44477>.

Regulations:

Law Number 8 of 1999 concerning Consumer Protection

Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE)

Law No. 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions (PP PSTE),

Financial Services Authority Regulation No. 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks

POJK No. 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector

Internet:

https://finansial.bisnis.com/read/20230510/231/1654678/gangguan-mobile-banking-sampai-3-hari-bsi-lakukan-penelusuran-serangan-siber?utm_ accessed on Saturday, October 11, 2025, at 11.00 WIB.

https://finansial.bisnis.com/read/20240626/90/1777171/mobile-banking-bca-sempat-error-manajemen-update-informasi?utm_ accessed on Saturday, October 11, 2025, at 11.10 WIB.

https://www.antaranews.com/berita/5142273/m-banking-bca-dan-blu-error-29-september-ini-penjasannya?utm_ accessed on Saturday, October 11, 2025, at 11.15 WIB.

<https://keuangan.kontan.co.id/news/begini-taksiran-kerugian-bca-dan-mandiri-saat-layanan-mobile-banking-alami-kendala?page=1> accessed on Saturday, October 11, 2025, at 11.22 WIB.

https://www.bi.go.id/id/publikasi/ruang-media/news-release/Pages/sp_2530523.aspx?utm_ Retrieved on Sunday, October 12, 2025, at 15.18 WIB.