

Legal Protection for Customers Against Loss of Funds Due to Online Fraud in Mobile Banking Services Reviewed from Law Number 8 of 1999 on Consumer Protection

Sindi¹, Anjani Sipahutar², and Apri Amalia³

^{1,2,3}Faculty of Law, Universitas Al-Azhar Medan, Medan, Indonesia

Abstract: This study analyzes legal protection for customers against loss of funds due to online fraud in mobile banking services under Law Number 8 of 1999 on Consumer Protection. The background is the rapid digitalization of banking, which brings risks such as phishing, social engineering, OTP misuse, and account hacking. This study uses normative legal research with statutory, conceptual, and case approaches, drawing on primary, secondary, and tertiary legal materials analyzed qualitatively. The results show that customer protection is both preventive and repressive, based on the Consumer Protection Law, Banking Law, ITE Law, PDP Law, and OJK regulations. Bank liability is not absolute; it depends on the cause of the loss. If the loss arises from system weaknesses or bank negligence, the bank may be held liable. Conversely, if the loss occurs because the customer voluntarily provided authentication data to fraudsters, the bank's liability is limited. Legal remedies include internal bank complaints, OJK facilitation, BPSK dispute resolution, and litigation. This study concludes that a balanced approach is needed, strengthening system security, customer education, and clear compensation mechanisms.

Keywords: Consumer Protection; Mobile Banking; Phishing; Bank Liability; Compensation.

1. Introduction

The development of information and communication technology has driven a significant transformation in the banking sector. Conventional services that previously required customers to visit a branch office or ATM have been replaced by digital services such as internet banking and mobile banking. Mobile banking allows customers to conduct transactions without being limited by space and time, enabling transfers, bill payments, mobile top-ups, and even investments through a smartphone (Candra et al., 2024; Handayani & Anitasari, 2022).

However, the digitalization of banking also brings significant security risks. Electronic banking transactions rely heavily on information technology systems that are vulnerable to misuse. Various forms of cybercrime have emerged, including phishing, malware, social engineering, identity theft, and account hacking. Phishing is one of the most common *modus operandi* because it targets human weaknesses rather than merely system vulnerabilities (Dewi & Fitri, 2025; Suwiknyo, 2021).

Data from the Financial Services Authority (OJK) through the Indonesia Anti-Scam Centre (IASC) show a significant increase in fraud and scam reports. Cases of fund loss due to phishing through SMS, WhatsApp, Telegram, and fake applications continue to rise. Perpetrators often impersonate bank officers, send fake links, or request OTP codes under the pretext of verification. As a result, customers suffer financial losses, personal data breaches, psychological distress, and reduced trust in digital banking services (Antara News, 2025; Lestari & Fasa, 2025).

In dispute resolution practice, there is often a difference of opinion between banks and customers. Banks argue that losses due to phishing are the result of customer negligence, so the bank cannot be held liable. Conversely, customers argue that the bank, as the operator of electronic banking services, is obliged to guarantee system security and

Correspondence:

Name: Sindi

Email: cindysaragih143@gmail.com

Received: Aug 08, 2026;

Revised: Aug 10, 2026;

Accepted: Sep 10, 2026;

Published : Oct 30, 2026;



Copyright: © 2026 by the authors. Submitted for possible open access publication under the terms and conditions of the Creative Commons

Attribution-NonCommercial 4.0 International License (CC BY-NC 4.0) license (<https://creativecommons.org/licenses/by-nc/4.0/>).

protect customer funds and data. This difference raises legal issues regarding the extent of bank liability for customer losses due to phishing (Oping & Gunadi, 2025; Putri et al., 2024).

Normatively, customer protection in banking is regulated in various laws and regulations, including Law Number 8 of 1999 on Consumer Protection (UUPK), Law Number 7 of 1992 as amended by Law Number 10 of 1998 on Banking, Law Number 11 of 2008 as amended by Law Number 1 of 2024 on Information and Electronic Transactions (ITE Law), Law Number 27 of 2022 on Personal Data Protection (PDP Law), and Financial Services Authority Regulations (POJK) Number 1/POJK.07/2013 and POJK Number 21 of 2023. Nevertheless, the effectiveness of these regulations is still debated, especially in phishing cases involving psychological manipulation (Huda, 2022; Widarto & Runekawati, 2025).

Previous studies have examined consumer protection in digital banking from various angles. For instance, Putri et al. (2024) focused heavily on the criminal law perspective of digital fraud, while Oping and Gunadi (2025) analyzed bank liability but were limited to a specific BPSK court decision. Other studies, such as Dewi and Fitri (2025), explored the *modus operandi* of phishing but did not comprehensively link it to the legal parameters of bank liability under the Consumer Protection Law. These existing studies tend to be fragmented; they either discuss the technical aspects of cybercrime or the general principles of consumer protection without clearly constructing the boundaries of bank liability when facing fraud that exploits psychological manipulation (social engineering) rather than system breaches. Furthermore, there is a lack of comprehensive analysis regarding the intersection of preventive protection, repressive liability, and the practical recovery of funds for customers.

Therefore, this study offers a specific novelty by bridging this gap. It positions mobile banking customers not merely as contractual parties, but as consumers who must be protected under the principles of justice and legal certainty. By systematically integrating the UUPK, Banking Law, ITE Law, and PDP Law, this study constructs a proportional liability framework that distinguishes between system negligence (bank liability) and voluntary disclosure of authentication data (customer negligence). Additionally, this study provides a comprehensive mapping of legal remedies—both non-litigation and litigation—to ensure effective compensation recovery.

Based on this background, the research questions are refined into three main focuses. First, this study seeks to analyze how legal protection is constructed for mobile banking customers under Indonesian laws and regulations. Second, it aims to examine to what extent banks can be held legally liable for customer fund losses due to online fraud (phishing) under Law Number 8 of 1999 on Consumer Protection. Third, it explores the most effective legal remedies available for customers to recover their financial losses, as well as the criteria for determining compensation between the bank and the customer. The purpose of this study is to analyze these three issues in a normative legal manner to provide legal certainty and a balanced protection framework for both customers and banks in the digital era.

2. Materials and Methods

This study constitutes normative legal research, positioning law as a system of norms and rules prevailing in society, with a focus on statutory regulations, legal principles, doctrines, and relevant court decisions (Ali, 2021; Suyanto, 2023).

Research Approaches. Three approaches are employed, each with a distinct function. The statutory approach functions to map and examine the hierarchy of relevant regulations (UUPK, Banking Law, ITE Law, PDP Law, and POJK) to answer the first research question regarding the construction of legal protection. The conceptual approach functions to examine doctrines of fault, negligence, and proportional liability to answer the second research question on the limits of bank liability. The case approach functions to provide factual context for the application of legal norms in practice, specifically analyzing the phishing case affecting a BRI customer to answer the third research question

on legal remedies. To interpret the legal norms, this study employs grammatical interpretation (to understand the literal meaning of statutory articles) and systematic interpretation (to ensure consistency across regulations within the Indonesian legal hierarchy).

Legal Materials and Their Classification. This study relies on secondary data categorized by issue relevance, hierarchical standing, and current legal status. Primary legal materials include Law No. 8 of 1999 on Consumer Protection (UUPK), Law No. 7 of 1992 as amended by Law No. 10 of 1998 on Banking, Law No. 11 of 2008 as amended by Law No. 1 of 2024 on ITE, Law No. 27 of 2022 on PDP, POJK No. 1/POJK.07/2013, and POJK No. 21 of 2023, all of which are currently in force. Secondary legal materials include academic books, scientific journals, and legal articles relevant to consumer protection and digital banking. Tertiary legal materials include legal dictionaries and encyclopedias. These materials are collected through library research.

The Case. The case approach focuses on a phishing incident affecting a BRI mobile banking customer, documented in Putusan Nomor 3/Pdt.Sus BPSK/2022/PN Lsm (Oping & Gunadi, 2025). The chronology is as follows: the perpetrator sent a fake link resembling the official BRI website; the victim entered their user ID, password, PIN, and OTP code into the fake site; the perpetrator then used this data to access the victim's account and transfer funds without authorization. The primary source for this case is the BPSK decision document, ensuring the factual basis is verifiable.

Analytical Technique. The legal materials are analyzed qualitatively using normative juridical analysis, carried out in four sequential steps: (1) identification of bank obligations under Articles 4, 7, and 19 of the UUPK, Article 2 and Article 29 paragraph (2) of the Banking Law, the ITE Law, the PDP Law, and POJK; (2) assessment of fault or negligence, examining whether the bank's security system functioned optimally, whether adequate education was provided, and whether security mechanisms met regulator standards; (3) establishment of causal link between the bank's conduct and the customer's loss, pointing either to bank liability (system failure) or customer negligence (voluntary disclosure of authentication data); and (4) determination of customer losses and compensation, including available legal remedies. Every conclusion in this study is drawn from this traceable chain of legal reasoning and factual evidence (Firmanto et al., 2024).

3. Results and Discussion

3.1 *The Interrelationship of Regulations in Legal Protection for Mobile Banking Customers*

Legal protection for mobile banking customers in Indonesia is not built on a single statute but on a layered and interconnected regulatory framework. Understanding the interrelationship between these regulations is essential to answer the first research question, because no single law can fully address the complexity of mobile banking fraud. The framework operates on three hierarchical levels: the statutory level, the regulatory level, and the operational level.

At the statutory level, Law No. 8 of 1999 on Consumer Protection (UUPK) serves as the foundational normative umbrella. Article 1 number 2 of the UUPK defines a consumer as every person who uses goods or services available in society for personal, family, or other non trading purposes. In the banking context, mobile banking customers fall squarely within this definition because they use bank services to fulfill personal financial transaction needs. Article 4 of the UUPK grants consumers four fundamental rights: the right to comfort, security, and safety in using services; the right to correct, clear, and honest information; the right to be heard regarding complaints; and the right to dispute resolution and compensation. These rights form the normative basis for any claim brought by a customer against a bank.

The Banking Law, namely Law No. 7 of 1992 as amended by Law No. 10 of 1998, complements the UUPK by imposing sectoral obligations on banks. Article 2 of the Banking Law requires banks to conduct their business activities based on the prudential banking principle. This principle is not merely an administrative guideline but a legal

obligation that requires banks to provide a secure and reliable service system capable of protecting customer funds and data. Article 29 paragraph 2 of the Banking Law further imposes bank secrecy obligations, covering customer identity, account numbers, balances, transaction histories, and transaction data. The Banking Law thus establishes the standard of care expected of banks in operating mobile banking services.

The ITE Law, namely Law No. 11 of 2008 as amended by Law No. 1 of 2024, functions as the procedural bridge between substantive consumer protection and practical dispute resolution. Banks as electronic system operators must organize reliable, secure, and responsible systems. The ITE Law recognizes the validity of electronic information and documents as legal evidence, so account mutations, transaction notifications, and electronic transfer receipts can be used in dispute resolution. This is crucial because in mobile banking fraud, the primary evidence is almost always digital. The ITE Law also prohibits unauthorized access to electronic systems, illegal interception, and manipulation of electronic data, thereby providing a basis for prosecuting cybercriminals who commit phishing or account hacking.

The PDP Law, namely Law No. 27 of 2022 on Personal Data Protection, reinforces data security by obligating banks as personal data controllers to ensure that the collection, processing, storage, use, and disclosure of customer data are carried out in accordance with the law. Banks must implement technical and organizational measures such as encryption, multi factor authentication, and monitoring of transaction activities. Personal data protection is crucial because data breaches often become the entry point for online fraud. Without strong data protection, even the most sophisticated security system can be compromised.

At the regulatory level, POJK No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector operationalizes the UUPK principles within the financial sector. It requires banks to apply the principles of transparency, fair treatment, service reliability, confidentiality and security of consumer data, and effective complaint handling. POJK No. 21 of 2023 on Digital Bank Services by Commercial Banks specifically governs the implementation of digital services, including information technology risk management and customer protection. These regulations translate the broad principles of the UUPK and the Banking Law into concrete operational standards that banks must follow.

The interrelationship between these regulations is therefore hierarchical and functional. The UUPK provides the rights and liability principles. The Banking Law and the PDP Law provide sectoral obligations. The ITE Law provides evidentiary tools. The POJK provides operational standards. No single regulation is sufficient on its own. A customer claiming compensation must rely on the UUPK for the right, the Banking Law for the breach of prudential duty, the ITE Law for evidence, and the POJK for the standard of care expected of the bank. This multidimensional framework reflects the complexity of mobile banking fraud, which involves not only contractual relationships but also data security, electronic evidence, and regulatory supervision.

3.2 Parameters of Liability for Banks and Customers

The second research question concerns the extent to which banks can be held liable for customer fund losses due to online fraud. To answer this question, it is necessary to define the parameters of liability for both banks and customers. This study identifies five parameters: legal obligations, types of violations, fault, causal links, and evidentiary requirements.

The first parameter is legal obligations. Banks are bound by multiple obligations. Under Article 2 of the Banking Law, they must apply the prudential principle. Under Article 7 of the UUPK, they must act in good faith, provide correct information, guarantee service quality, and provide compensation if the service provided causes losses due to their error or negligence. Under the PDP Law, they must protect customer data. Under POJK No. 21 of 2023, they must implement information technology risk management. Customers, on the other hand, are bound by the obligation to maintain the confidentiality of their user ID, password, PIN, and OTP code. This obligation is stipulated in the mobile

banking service agreement and is reflected a contrario in Article 4 of the UUPK, which grants the right to security but also implies a duty of care on the part of the consumer.

The second parameter is the type of violation. A bank violates its obligations when it fails to implement an adequate security system, is negligent in maintaining data confidentiality, fails to monitor suspicious transactions, or fails to handle complaints professionally. A customer violates their obligation when they voluntarily disclose authentication data to a third party, fail to report suspicious activity, or ignore security warnings. The type of violation determines the nature of the legal claim: a bank's failure to provide a secure system may give rise to a claim for unlawful act, while a customer's voluntary disclosure may be treated as contributory negligence.

The third parameter is fault, meaning error or negligence. A bank is at fault if its system does not meet regulator standards under POJK No. 21 of 2023, or if it fails to provide adequate education about phishing risks. A customer is at fault if they voluntarily enter credentials into a fake site or provide an OTP code to a perpetrator. Fault is not presumed; it must be proven through evidence. This is consistent with Article 19 of the UUPK, which requires the loss to arise from the error or negligence of the business actor.

The fourth parameter is the causal link. The customer's loss must be directly caused by the bank's system weakness or omission for bank liability to arise. Conversely, the loss must be directly caused by the customer's disclosure for customer negligence to be established. The causal link is the decisive element that determines the proportion of liability. In practice, this requires a factual investigation into the chronology of events, the security logs, and the communication between the bank and the customer.

The fifth parameter is evidentiary requirements. The bank must rely on its internal investigation report, system logs, audit trails, and compliance reports to OJK. The customer must rely on transaction history, a chronology of events, proof of complaint, and digital forensics such as fake URL records and SMS logs. The ITE Law supports this by recognizing electronic evidence as valid. Without proper evidence, neither party can establish fault or causal link.

Applying these parameters, bank liability under Article 19 of the UUPK is not absolute. Article 19 states that business actors are liable for consumer losses if the loss arises from their error or negligence. In the BRI phishing case documented in Putusan Nomor 3/Pdt.Sus BPSK/2022/PN Lsm, the perpetrator did not hack the BRIimo system directly. Instead, the victim voluntarily entered their user ID, password, PIN, and OTP into a fake site resembling the bank's official site. Under the parameters above, the causal link points to customer negligence, which limits the bank's liability. However, the bank remains obligated to prove that its security system functioned optimally and that it provided adequate education about phishing risks. If the bank fails to provide such proof, the causal link shifts back to the bank. This proportional approach reflects the principle of justice: the bank is not burdened with absolute liability, but it cannot escape liability if its own negligence contributed to the loss.

3.3 Legal Basis, Authority, and Functions of OJK and BPSK in Dispute Resolution

The third research question concerns the legal remedies available for customers to recover their financial losses. To answer this question, it is necessary to clarify the legal basis, authority, and functions of the two primary dispute resolution institutions: the Financial Services Authority (OJK) and the Consumer Dispute Resolution Agency (BPSK).

The Financial Services Authority (OJK) derives its consumer protection function from Law No. 21 of 2011 on OJK and POJK No. 1/POJK.07/2013 on Consumer Protection in the Financial Services Sector. OJK's authority is supervisory and facilitative. It can set standards for transparency, data security, and complaint handling. It can impose administrative sanctions on banks that violate consumer protection provisions. It can also facilitate mediation between customers and banks. However, OJK cannot issue binding decisions in individual disputes. Its function is preventive through standard setting and repressive through facilitation and sanctions. In the context of mobile banking fraud, OJK

encourages banks to enhance customer education, improve system security, and provide clear information about risks and complaint procedures.

The Consumer Dispute Resolution Agency (BPSK) derives its authority from Articles 49 to 58 of the UUPK. BPSK's authority is adjudicative. It can resolve disputes through mediation, conciliation, or arbitration. In arbitration, BPSK's decision is final and binding on both parties. In mediation and conciliation, the parties may reach a voluntary agreement. BPSK's function is to provide fast, simple, and low cost dispute resolution. In the banking context, BPSK functions as a means of legal protection for customers as consumers who feel disadvantaged by the use of banking services, including mobile banking.

In practice, there is a debate regarding BPSK's authority over financial sector disputes. Some argue that financial service disputes should be resolved through the special mechanisms provided by OJK, as regulated in POJK No. 1/POJK.07/2013, which requires banks to establish internal dispute resolution and allows customers to escalate complaints to OJK. However, BPSK remains a recognized forum under the UUPK. The practical sequence for customers is: first, an internal bank complaint; second, escalation to OJK for facilitation; third, BPSK for binding arbitration if facilitation fails; and fourth, litigation as the last resort.

In addition to OJK and BPSK, customers may also pursue litigation through the courts. A civil lawsuit can be filed against the bank if there is an allegation of default or unlawful act. Default occurs if the bank is considered not to have carried out its obligations as agreed in the mobile banking service agreement. An unlawful act can be filed if the bank's action or negligence is considered contrary to legal provisions and causes losses to the customer, for example due to a weak security system or lack of adequate data protection. A civil lawsuit is filed with the competent district court accompanied by supporting evidence such as transaction history, proof of fund loss, chronology of fraud, and proof of complaints made to the bank. In addition, if there is a criminal element, customers can report the online fraud perpetrator to law enforcement officials. Perpetrators can be sanctioned under the Criminal Code and the ITE Law.

3.4 Requirements and Legal Grounds for Compensation

The legal ground for compensation is Article 19 of the UUPK, which states that business actors must provide compensation for consumer losses arising from their error or negligence. Article 7 huruf a of the UUPK reinforces this by requiring business actors to act in good faith and guarantee service quality. These provisions establish that compensation is not a discretionary gesture but a legal obligation.

The requirements for compensation are fourfold. First, proof of loss, which can take the form of account mutations, transaction history, transaction notifications, and complaint reports. Second, proof of fault, meaning evidence that the loss arose from bank error or negligence such as system weakness, failure to monitor, or failure to educate. Third, proof of causal link, meaning evidence connecting the bank's conduct to the loss. Fourth, proof of complaint, meaning evidence that the customer has exhausted internal complaint mechanisms.

When these requirements are met, compensation can take several forms. The most common is a refund if it is proven that the loss of funds occurred due to system error, service disruption, or bank negligence. Compensation can also be in the form of replacement of additional financial losses arising from the incident, such as administrative costs or account blocking fees. In practice, compensation can also be carried out through an agreement between the bank and the customer, including additional compensation as a form of bank good faith. Conversely, if the loss arises from customer negligence through voluntary disclosure of authentication data, compensation liability may be limited or not borne by the bank. The determination of liability is based on the bank's investigation results regarding the system, account access history, and transaction patterns.

3.5 Discussion: Balancing Protection and Liability

The analysis above demonstrates that legal protection for mobile banking customers requires a balance between customer rights and bank obligations. On the one hand, customers as consumers of financial services have the right to obtain security, correct information, personal data protection, and compensation if they suffer losses due to bank error or negligence. On the other hand, banks as business actors have the obligation to apply the prudential principle, provide a secure system, and handle complaints professionally. However, banks cannot be burdened with absolute liability for every loss suffered by customers, especially if the loss occurs due to the customer's own negligence.

The BRI phishing case illustrates that perpetrators increasingly exploit social engineering rather than system vulnerabilities. This shifts the factual basis of liability. The loss is not always caused by bank negligence. Therefore, the determination of liability must be based on proof of the cause of the loss and the proportion of fault of each party. This approach reflects the principle of justice because it provides protection for customer rights without ignoring the bank's obligations as a banking service operator and the customer's obligation to use mobile banking services carefully.

This study contributes to the literature by constructing a proportional liability framework that distinguishes between system negligence, which triggers bank liability, and voluntary disclosure, which triggers customer negligence. Unlike previous studies that focus only on criminal law (Putri et al., 2024) or on a single court decision (Oping & Gunadi, 2025), this study integrates the UUPK, Banking Law, ITE Law, PDP Law, and POJK into a single analytical framework. It also goes beyond the existing literature by explicitly defining the five parameters of liability and by mapping the legal remedies available to customers, from internal complaints to litigation.

The practical implication is twofold. First, banks must continuously improve system security, implement unusual transaction detection, and provide ongoing education about phishing and OTP misuse. Second, customers must improve digital literacy and maintain the confidentiality of authentication data. OJK and BPSK must also strengthen their coordination to ensure that dispute resolution is fast, simple, and low cost. Legal certainty in digital banking thus depends not only on the existence of regulations but on their consistent application and enforcement.

From a theoretical perspective, this study reinforces the view that consumer protection in digital banking is not a matter of absolute liability but of proportional liability. The principle of justice requires that liability be apportioned according to fault and causal link. This is consistent with the doctrine of contributory negligence and with the principle of balance between rights and obligations. From a practical perspective, this study provides a framework that can be used by banks, regulators, and customers to assess liability in mobile banking fraud cases.

4. Conclusions

Based on the research results and discussion, this study draws three conclusions that correspond directly to the three research questions. First, regarding the construction of legal protection (Research Question 1). Legal protection for mobile banking customers in Indonesia is both preventive and repressive, and it rests on a layered and interconnected regulatory framework rather than a single statute. Preventive protection operates through regulation and supervision under the UUPK, the Banking Law, the ITE Law, the PDP Law, POJK No. 1/POJK.07/2013, and POJK No. 21 of 2023. Repressive protection operates through complaint mechanisms, dispute resolution, and compensation. The interrelationship between these regulations is hierarchical and functional: the UUPK supplies the rights and liability principles, the Banking Law and PDP Law supply sectoral obligations, the ITE Law supplies evidentiary tools, and the POJK supplies operational standards. Customers therefore have the right to security, correct information, personal data protection, and compensation if they suffer losses due to bank error or negligence.

Second, regarding the basis and limits of bank liability (Research Question 2). Bank liability for loss of funds due to online fraud is not absolute. It is determined by five parameters: legal obligations, types of violations, fault, causal links, and evidentiary requirements. Under Article 2 and Article 29 paragraph (2) of the Banking Law, banks must apply the prudential principle and maintain bank secrecy. Articles 4, 7 huruf a, and 19 of the UUPK require business actors to act in good faith, provide correct information, and provide compensation if consumer losses arise from their error or negligence. However, a bank's liability cannot be established solely on the ground that a customer's credentials were used by a perpetrator of fraud. It must be determined based on three elements: whether the bank breached its legal obligations, whether there is sufficient evidence to prove the breach, and whether there is a causal link between the breach and the loss. If the loss is caused by a weakness in the security system, a failure to monitor suspicious transactions, or a failure to provide adequate education, the bank can be held liable. Conversely, if the loss occurs because the customer voluntarily provided authentication data to the phishing perpetrator, the element of customer negligence becomes a decisive consideration in determining the proportion of liability. The burden of proof is shared: the customer must prove the loss and the complaint, while the bank must prove that its security system functioned optimally and that it provided adequate education. This proportional approach reflects the principle of justice and balance between customer rights and bank obligations.

Third, regarding legal remedies and the right to compensation (Research Question 3). Customers who suffer loss of funds due to online fraud have the right to compensation, which is grounded in Article 19 of the UUPK. This right can be pursued through non litigation and litigation channels. Non litigation channels include internal complaints to the bank, escalation to OJK for facilitation, and resolution through BPSK for binding arbitration. Litigation channels include civil lawsuits against the bank on the grounds of default or unlawful act, and criminal reports against fraud perpetrators under the Criminal Code and the ITE Law. Compensation may take the form of a refund, replacement of other financial losses, or compensation based on agreement as a form of bank good faith. The requirements for compensation are fourfold: proof of loss, proof of fault, proof of causal link, and proof of complaint. The determination of liability is based on the bank's investigation results regarding the system, account access history, and transaction patterns.

Recommendations. Based on these conclusions, this study proposes several concrete recommendations. First, banks should establish clear internal criteria for investigating mobile banking fraud, including mandatory system log audits, transaction pattern analysis, and a documented assessment of whether the customer voluntarily disclosed authentication data. Second, banks should develop a standardized mechanism for assessing compensation claims, including a checklist of required evidence, a timeframe for investigation, and a written decision that can be reviewed by OJK or BPSK. Third, OJK and BPSK should strengthen their coordination by issuing joint guidelines on the sequence of dispute resolution, clarifying which forum has jurisdiction over which type of claim, and setting maximum time limits for each stage. Fourth, the government should clarify regulations regarding the burden of proof in mobile banking fraud, so that customers are not required to prove technical matters beyond their access and banks are not able to escape liability by simply asserting customer negligence. Fifth, customers should improve digital literacy and maintain the confidentiality of authentication data. Future researchers are expected to develop this study through normative and empirical approaches, particularly by examining court decisions and BPSK rulings to test the proportional liability framework proposed in this study.

References

- Ali, Z. (2021). *Metode penelitian hukum*. Sinar Grafika.
- Antara News. (2025). *OJK mencatat peningkatan laporan penipuan dan scam yang masuk ke Indonesia Anti Scam Centre (IASC)*. Antara News.

- Atsari, A. W., Sulatri, K., & Mashuri, M. (2023). Perlindungan hukum bagi nasabah perbankan terhadap kesalahan layanan mobile banking dari sistem teknologi informasi perbankan. *Yurijaya: Jurnal Ilmiah Hukum*, 5(1).
- Candra, A., Arista, W., Cayo, P. S. N., Husnaini, & Afriani, K. (2024). *Hukum perbankan Indonesia*. Prenada Media.
- Dewi, R., & Fitri, D. N. (2025). Perlindungan hukum terhadap nasabah bank pengguna m banking sebagai korban kejahatan tindak pidana penipuan di Indonesia. *Cerdika: Jurnal Ilmiah Indonesia*, 5(9), 3.
- Fazriah, D. (2023). Tanggung jawab atas terjadinya wanprestasi yang dilakukan oleh debitur pada saat pelaksanaan perjanjian. *Das Sollen: Jurnal Kajian Kontemporer Hukum dan Masyarakat*, 1(2).
- Firmanto, T., Sufiarina, S., Reumi, F., & Saleh, I. N. S. (2024). *Metodologi penelitian hukum: Panduan komprehensif penulisan ilmiah bidang hukum*. PT. Sonpedia Publishing Indonesia.
- Handayani, S., & Anitasari, M. (2022). Karakteristik pengguna mobile banking di Kota Bengkulu. *Ekombis Review: Jurnal Ilmiah Ekonomi dan Bisnis*, 10(1), 66.
- Hanum, A., Fithriyatirrizqoh, F., & Baidhowi, B. (2025). Analisis yuridis pengawasan Otoritas Jasa Keuangan terhadap penerapan asas kehati hatian oleh lembaga perbankan digital. *Jurnal Ilmiah Penelitian Mahasiswa*, 3(3).
- Huda, K. (2022). Fungsi dan tugas Otoritas Jasa Keuangan (OJK) dalam penyelesaian sengketa nasabah perbankan syariah di Indonesia. *Malia*, 14(1), 18.
- Ismayani, A. (2019). *Metodologi penelitian*. Syiah Kuala University Press.
- Justin Thenata, P. D., Susanto, R. J., Kurniawati, J. O., & Lee, J. C. (2025). Analisis tanggung jawab hukum terhadap keamanan perbankan dan nasabah dalam kasus phishing. *Cerdika: Jurnal Ilmiah Indonesia*, 5(4).
- Lestari, P. A., & Fasa, M. I. (2025). Transformasi digital banking: Manfaat dan risiko transaksi online modern (internet banking dan mobile banking). *Jurnal Media Akademik (JMA)*, 3(4).
- Oping, T. F., & Gunadi, A. (2025). Tanggung jawab bank atas hilangnya dana nasabah melalui layanan aplikasi mobile banking (Studi kasus Putusan Nomor 3/Pdt.Sus BPSK/2022/PN Lsm). *Journal of Syntax Literate*, 10(1).
- Otoritas Jasa Keuangan. (2013). *Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan*.
- Otoritas Jasa Keuangan. (2023). *Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 tentang Layanan Bank Digital oleh Bank Umum*.
- Putri, D. E., Sudarti, E., & Siregar, E. (2024). Tindak pidana penipuan melalui aplikasi digital (Gagasan pemikiran pertanggungjawaban oleh bank). *PAMPAS: Journal of Criminal Law*, 5(1), 72.
- Rahmah, A. T., & Fasa, M. I. (2024). Pengaruh transformasi digital dan pengembangan financial technology (fintech) terhadap inovasi layanan perbankan syariah. *Jurnal Media Akademik (JMA)*, 2(10).
- Republik Indonesia. (1998). *Undang Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang Undang Nomor 7 Tahun 1992 tentang Perbankan*.
- Republik Indonesia. (1999). *Undang Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*. Lembaran Negara RI Tahun 1999 Nomor 42.
- Republik Indonesia. (2022). *Undang Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.
- Republik Indonesia. (2024). *Undang Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*.
- Sari, N., Tanjung, J. H. S., & Amalia, A. (2025). Perlindungan hukum terhadap reseller akibat penjual melakukan wanprestasi dalam jual beli online: (Studi Putusan Nomor: 629/Pdt.G/2022/PN.Jkt.Sel). *Politika Progresif: Jurnal Hukum, Politik dan Humaniora*, 2(1), 85.
- Suwiknyo, F. B. (2021). Tindak kejahatan siber di sektor jasa keuangan dan perbankan. *Lex Privatum*, 9(4).
- Suyanto, S. H. (2023). *Metode penelitian hukum pengantar penelitian normatif, empiris dan gabungan*. Unigres Press.
- Syamsiah, D., Nugroho, A. S., & Damayanti, E. E. (2026). Digitalisasi pembuktian elektronik dalam sengketa wanprestasi transaksi fintech. *JOSH: Journal of Sharia*, 5(1).
- Usanti, T. P., & Shomad, A. (2017). *Hukum perbankan*. Kencana.
- Widarto, J., & Runekawati, M. (2025). Perlindungan hukum dalam melindungi kerahasiaan data pribadi nasabah di era digital: (Studi pada PT. BPR Prima Sejahtera berdasarkan Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023). *Arus Jurnal Sosial dan Humaniora*, 5(2), 79.