Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

Analysis of Digital Bank Customer Protection Against Loss of Funds in Accounts Reviewed According to Indonesian Positive Law

Muhammad Raihan Hakim, Moody Rizqi Syailendra Putra
Faculty of Law, Tarumanagara University, Jakarta, Indonesia
hakimraihan126@gmail.com

Abstract

This research aims to analyze digital bank customer protection regarding cases of fund losses in accounts based on Indonesian positive law, examining the legal framework governing consumer protection in digital banking services. The urgency of this study stems from the rapid advancement of information technology in the banking sector, which is creating new challenges and cases, including instances of customer fund losses from accounts through system failures and cyber attacks. This research employs a qualitative approach with an empirical normative design, analyzing legal provisions, regulations, and their practical implementation in protecting digital bank customers. The findings reveal that digital banks are specifically regulated in POJK No. 12/POJK.03/2021 and must apply consumer protection principles according to POJK No. 6/POJK.07/2022, including transparency, fair treatment, reliability, confidentiality, and data security. The study demonstrates that fund losses due to system failures or hacking constitute violations of electronic system reliability and security principles as regulated in the ITE Law, with consumer protection guaranteed by Law No. 8 of 1999 and Law No. 10 of 1998 on Banking. This research contributes new insights into the intersection of digital banking regulation and consumer protection law, revealing gaps in current enforcement mechanisms, particularly regarding third-party cyber crimes, and proposes enhanced protective measures for Indonesia's growing digital banking sector. This study recommends strengthening regulatory enforcement mechanisms, expanding bank liability frameworks for external cyber crimes, and enhancing cybersecurity infrastructure to ensure comprehensive customer protection in digital banking.
Keywords: *Account; Customer Protection; Digital Bank; Funds; Positive Law*

1. INTRODUCTION

Banks play a vital role in driving Indonesia's economy, serving as the main connector for society in conducting various financial transactions, from payments and fund storage to business capital acquisition.[1] Besides being a place to store money, banks also function as the primary source of credit that helps communities and business actors obtain capital to develop their businesses. Thus, banks become an important key in supporting business activities and national economic growth.[2] With technological advancements, digital banks have emerged in Indonesia, expanding public access to more practical and efficient financial services and encouraging the creation of a new digital-based economic ecosystem.[3]

[1] Bayu Prawira, *Transformasi Digital Bank Di Indonesia, Konsep Dan Praktek Dalam Memimpin Transformasi Total* (Malang: Media Nusa Creative, 2021).
[2] E. Larasati, "Tumbuh Kuat Di Kuartal II, Investasi Jadi Motor Penggerak Pertumbuhan Ekonomi 2021," *Badan Kebijakan Fiskal*, September 2021.
[3] Bank Mega Syariah, "Bank Digital: Pengertian, Manfaat, Dan Tips Memilihnya," 2024.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

The continuity of digital transformation today is extremely rapid while simultaneously impacting all sides of life as a consequence of the Industry 4.0 era.[4] Changes in business models, as well as ecosystem overhauls, are required to be more innovative, complex, and dynamic. The current digital transformation also significantly impacts society, especially in the banking world, creating digital banking systems that are easily accessible without having to visit branch offices directly to conduct transactions.

Recent research has examined various aspects of digital banking regulation and customer protection. Gaib analyzed the reconstruction of legal protection for banking consumers amid technological crime threats, revealing significant gaps in monitoring and enforcement capabilities.[5] While this study provided valuable insights into general banking consumer protection, it did not specifically address the unique challenges posed by digital-only banking platforms or the specific regulatory framework governing them. Chairunnisa, Murwadji, and Harrieti investigated legal protection for customers against phishing and hacking crimes in digital bank services, finding that existing legal frameworks require strengthening to address evolving cyber threats.[6] However, this research focused primarily on criminal law aspects rather than examining the comprehensive regulatory framework for consumer protection in digital banking, and did not address the regulatory gaps regarding bank liability for external cyber crimes.

Another significant study by Fauzadeli examined legal protection for e-wallet customers regarding data breaches and fund losses, highlighting the intersection of financial technology and consumer protection law.[7] While valuable, this research did not address the specific regulatory environment for digital banks or the unique challenges they face in ensuring customer fund security, particularly regarding third-party liability issues.

Previous studies have generally focused on conventional banking protection or specific aspects of digital financial services without comprehensively analyzing customer fund protection in digital banks based on Indonesia's positive legal framework. No research has comprehensively analyzed the intersection of digital banking regulation, consumer protection law, and information technology legislation in the context of fund loss protection. This research addresses these gaps by conducting a comprehensive analysis of the legal framework governing digital bank customer protection against fund losses, examining the intersection of banking regulation, consumer protection law, and information technology legislation. The study provides practical insights into regulatory enforcement challenges and

[4] Krisna Wijaya, "Digital Banking VS Digital Bank," *Majalah Info Bank Lppi*, no. 1 (2021): 1–5.
[5] Djuwita N Gaib, "Dinamika Hukum Perbankan Digital Di Indonesia," *Lex Et Societatis* 7, no. 11 (2019), https://doi.org/https://doi.org/10.35796/les.v7i11.27366.
[6] Salsabila Chairunnisa, Tarsisius Murwadji, and Nun Harrieti, "Perlindungan Hukum Terhadap Nasabah Atas Kejahatan Phising Dan Hacking Pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia," *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 1 (2024): 1–16, https://doi.org/https://doi.org/10.51903/hakim.v2i1.1535.
[7] Muhammad Fahri Fauzadeli, "Perlindungan Hukum Terhadap Nasabah E-Wallet Atas Kebocoran Data Dan Kehilangan Sejumlah Dana," *Qistie* 15, no. 2 (2022): 224–38.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

proposes solutions for enhanced customer protection. The research aims to analyze the perspective of digital bank customer protection regarding cases of fund losses in accounts based on Indonesian positive law.

2. METHOD

This research uses normative legal research focusing on the study of legal rules as a system of norms and written principles in legislation, court decisions, legal doctrines, jurisprudence, individual behaviors related to legal contexts, and other legal sources.[8] This research aims to understand, interpret, and describe the content of legal implications from legal sources in terms of protecting the rights of digital bank customers, arranged systematically and logically. Legal materials used in this research include primary legal sources (statutory regulations including POJK, Banking Law, Consumer Protection Law, and ITE Law), secondary legal sources (books, journal articles, and expert opinions related to digital banking and consumer protection), and tertiary legal sources (legal dictionaries and encyclopedias). Data analysis is conducted qualitatively through prescriptive and interpretative methods, employing deductive logic and systematic legal interpretation, aiming to provide legal argumentation and a systematic understanding of customer protection within the digital banking regulatory framework.

The research methodology involves a systematic examination of relevant legal provisions, a comparative analysis of regulatory frameworks, and a critical evaluation of enforcement mechanisms.[9] Data collection focuses on analyzing the effectiveness of current legal protections and identifying regulatory gaps, particularly in cases involving third-party cyber crimes against digital bank customers.

3. RESULTS AND DISCUSSION

3.1 Regulatory Framework for Digital Bank Customer Protection

Digital Bank, as mentioned in Article 1, paragraph 22 of POJK No.12/POJK.03/2021 related to Commercial Banks, is stated as part of BHI Bank that provides and runs main activities, especially through electronic channels without physical office forms other than headquarters or utilizing limited physical offices.[10] In this case, BHI (Indonesian Legal Entity Bank) is marked as a bank party that runs business activities in the banking sector, formed as an Indonesian legal entity that is aligned with provisions of laws and regulations, including in the context of intermediary banks.[11]

---

[8] G. Wala and H. Firmansyah, "Konsep Restorative Justice Untuk Mengurangi Over Capacity Pada Perkara Pidana," *Jurnal Kertha Semaya*, 12, no. 2 (2024): 247–54, https://doi.org/https://doi.org/10.24843/KS.2024.v12.i02.p19.

[9] A Kennedy, "The Role of Indonesian Constitutional Law in Sustaining National Resilience Amid Global Challenges," *Jurnal LemhannasRI* 12, no. 4 (2024): 485–508, https://doi.org/10.55960/jlri.v12i4.957.

[10] Otoritas Jasa Keuangan, "Tanya Jawab Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 Tentang Bank Umum," 2021.

[11] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22/POJK.04/2021 Tentang Penerapan Klasifikasi Saham Dengan Hak Suara Multipel Oleh Emiten Dengan Inovasi Dan Tingkat Pertumbuhan Tinggi Yang Melakukan Penawaran Umum Efek Bersifat Ekuitas Berupa Sa" (Jakarta: Otoritas Jasa Keuangan Republik Indonesia, 2021).

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

The institutional relationship between digital banks' legal entity status (Bank Berbadan Hukum Indonesia) and their legal responsibilities creates a foundation for liability frameworks.[12] Digital banks, despite their technological business model, remain subject to the same fiduciary duties and prudential principles as conventional banks, including the fundamental obligation to safeguard customer deposits. The term "digital bank" does not change the institutional nature of the bank, because whatever business model it runs, a bank is still a bank.[13] Digital banks officially operate if they have complied with requirements as contained in Article 24, including holding business models that are in line with technology use and adhering to risk management. Digital banks in this context have advanced bank products, namely, collecting funds according to information technology.[14] Suppose digital banks are unable to provide protection for customer funds. In that case, the bank is prohibited from running bank products, including connection with fund collection, and pursued termination of bank products. The legal implications of non-compliance with risk management principles are significant. If a digital bank fails to meet prudential requirements or demonstrates an inability to protect customer funds, regulatory authorities can impose sanctions ranging from operational restrictions to complete termination of banking products.[15] This creates a legal framework where customer protection is not merely a regulatory guideline but a fundamental operational requirement with enforceable consequences.

In efforts to collect digital bank customer funds, several types of risks can occur, including loss of deposit funds.[16] In this connection, risk management is needed as a preventive step if such things emerge. The risks that often occur in digital banks are related to risks that befall conventional banks, namely cases of deposit funds being taken or used by banking parties themselves, or cases of loss of funds stored by customers in banking. In the context of this happening, it is possible that third parties take the money through digital media, often referred to as cyberattacks.[17] However, a critical gap exists in the regulatory framework regarding cases where fund losses result from external cyber attacks by unaffiliated third parties. Current regulations primarily address internal mismanagement or affiliated third-party actions, leaving a normative vacuum for purely external cyber crimes.

[12] Anggi Riazti Gitazia and Muhaimin Muhaimin, "Tinjauan Yuridis Bank Digital Dalam Perspektif Bank Indonesia," *Commerce Law* 3, no. 1 (June 2023): 203–17, https://doi.org/10.29303/commercelaw.v3i1.2807.

[13] Ibid. hlm 4.

[14] Davina Dewi, "Perlindungan Hukum Nasabah BTPN Jenius Dalam Kasus Pembobolan Dana Rekening," *Fairness and Justice: Jurnal Ilmiah Ilmu Hukum* 21, no. 1 (2023): 9–20, https://doi.org/https://doi.org/10.32528/faj.v21i1.22959.

[15] Mochammad Su'eb and Yonika Nazla Rohma, "Peran Otoritas Jasa Keuangan (OJK) Dalam Pasar Uang Dan Modal Di Era Digital," *Jurnal Penelitian Ilmu Ekonomi Dan Keuangan Syariah* 3, no. 2 (May 2025): 107–17, https://doi.org/10.59059/jupiekes.v3i2.2386.

[16] Moch P Saputra, Sukono, and Diah Chaerani, "Estimation of Maximum Potential Losses for Digital Banking Transaction Risks Using the Extreme Value-at-Risks Method," *Risks*, 2022, https://doi.org/10.3390/risks10010010.

[17] Alfian Rifqi Aziz, "Perlindungan Hukum Dan Tanggung Jawab Bank Atas Hilangnya Dana Nasabah (Studi Pada: PT Bank Mandiri Tbk, Cabang Ciceri)" (Universitas Islam Indonesia, 2023).

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

3.2 Consumer Protection Principles in Digital Banking

POJK No. 6/POJK.07/2022 explains the mechanism of consumer data protection and the public in the financial services sector, which includes digital banking.[18] The POJK also requires digital banking to communicate with concerned customers regarding risk changes. If customers have not agreed to risk changes, then customers have the right to end legal relationships formed between banks, but there is a notification period of risk and provision of decisions by customers, which states that digital banks can communicate at least 30 working days before implementation of risk changes.[19] If customers have not expressed their opinions, then digital banks consider that customers have really agreed to the terms of such risk changes.[20]

The effectiveness of the 30-day notification requirement raises critical questions in practice. This timeframe may be insufficient for customers to fully understand complex risk implications, particularly in rapidly evolving digital environments where new cyber threats emerge frequently.[21] The principle of presumed consent through silence also contradicts basic consumer protection principles of explicit informed consent. Digital banks are specifically regulated in POJK No. 12/POJK.03/2021, while provisions related to consumer protection are stated in POJK No. 13/POJK.03/2021, especially in Chapter VII concerning Consumer Protection.[22] Based on Article 26, paragraph (1), banks are required to apply consumer protection principles as stipulated in regulations governing consumer protection in the financial services sector. These principles refer to provisions of POJK No. 6/POJK.07/2022 concerning Consumer Protection in the Financial Services Sector, Article 2, which includes principles of transparency, fair treatment, reliability, confidentiality and data security, complaint handling, and dispute resolution.[23]

In Article 26, paragraph (2) POJK No. 13/POJK.03/2021, it is mentioned that digital banks are required to have systems and mechanisms that can respond to any customer questions or complaints operationally 24 hours a day, every day. Based on the explanation of the article, it can be interpreted that if customer funds are lost, then customers can immediately contact digital banks to obtain needed explanations to reduce concerns and ensure their funds remain protected. However, if banks do not provide responses, then in accordance with provisions of Article 28, paragraph (1) and (2), banks can be subject to

[18] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan" (Jakarta: Otoritas Jasa Keuangan Republik Indonesia, 2022).

[19] Pakhry Nugroho Kadari, Saharuddin Saharuddin, and Muh. Akbar Fhad Syahril, "Perlindungan Hukum Nasabah Atas Penggunaan E-Banking," *Jurnal Litigasi Amsir* 10, no. 2 (February 2023): 167–79, https://doi.org/https://journalstih.amsir.ac.id/index.php/julia/article/view/238.

[20] Dita Fitri and Suherman, "Perlindungan Hukum Terhadap Nasabah Perbankan Yang Mengalami Kerugian Atas Pembobolan Rekening," in *Prosiding National Conference on Law Studies (NCOLS)*, vol. 2, 2020, 274–92.

[21] Kadek Adi Putre and Putri Triari Dwijayanthi, "Perlindungan Hukum Dana Nasabah Yang Hilang Pada Bank Digital," *Jurnal Kertha Desa* 10, no. 9 (2023): 934–42.

[22] Keuangan, "Tanya Jawab Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 Tentang Bank Umum."

[23] Keuangan.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

sanctions in the form of written warnings, freezing, or prohibition of the implementation of information technology-based products.[24]

3.3 Legal Framework for Fund Loss Protection

The initial step to secure lost funds is to submit questions or complaints to banks to identify the main causes, whether it comes from bank negligence, customer error, or third-party involvement.[25] In practice, management of digital banks involving individuals with diverse backgrounds creates potential that, from the bank itself, there can be misuse of customer funds for personal purposes. The change of bank management can also affect the effectiveness of customer fund protection, because it is not certain that the new management has the same protection commitment as the previous management.[26] The application of strict liability theory becomes crucial in this context. Under the prudential banking principle, banks should bear responsibility for fund protection regardless of the specific cause, unless customer negligence is clearly proven. However, current regulations create ambiguity regarding the burden of proof in cases involving external cyber crimes.

In line with provisions as stated in Article 22, paragraph (3) letter d POJK No. 6/POJK.07/2022, banks are prohibited from imposing an obligation of proof on customers if banks state that loss of funds is not their responsibility. The explanation of this article can be interpreted that customers do not need to prove the loss themselves if there are strong indications that the causes come from bank systems or employees, and if proven, then Article 29 requires digital banks to replace lost funds.[27] The principle of prudence requires bank employees to safeguard customer funds, but in reality, there are cases where employees themselves misuse customer funds.

Furthermore, including in the context of positive law enforced in Indonesia, protection of digital bank customers against disappearance of these funds should be reviewed based on multi-regulatory perspective, which concerns Law No. 19 of 2016 related to information and electronic transactions, where its existence is able to present crucial juridical foundation, especially as stated in Article 15 which essentially requires electronic system providers, which include digital banks, in efforts to organize secure, reliable, and responsible systems for electronic operational systems used.[28]

---

[24] R Muarief, *Bank Dan Lembaga Keuangan Lainnya: Fondasi Sistem Keuangan* ([Kota tidak disebutkan]: Asadel Liamsindo Teknologi, 2024).

[25] D. Utami and Y. Yennisa, "Faktor-Faktor Mempengaruhi Ketepatan Waktu Pelaporan Keuangan Pada Perusahaan Sub Sektor Bank Di Bursa Efek Indonesia," *AKUNTANSI DEWANTARA* 1, no. 1 (2017): 31–38, https://doi.org/https://doi.org/10.26460/ad.v1i1.22.

[26] Syariah, "Bank Digital: Pengertian, Manfaat, Dan Tips Memilihnya."

[27] Eveline Ivanca and Hery Firmansyah, "Perlindungan Hukum Pengguna Mobile Banking Sebagai Korban Kejahatan Melalui Internet Ditinjau Dari Hukum Positif," *UNES Law Review* 6, no. 2 (2023): 6166–74, https://doi.org/10.31933/unesrev.v6i2.1137.

[28] T Tasman and U Ulfanora, "Perlindungan Hukum Terhadap Nasabah Bank Digital," *UNES Law Review* 6, no. 1 (2023): 1624–35, https://doi.org/10.31933/unesrev.v6i1.962.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

In relation to the context of fund loss faced by customers, system failures or weak data security can be assessed as forms of violations of security and reliability principles of electronic systems mandated by the ITE Law, especially if there is a leak or misuse of personal data protected through Article 26 of the same Law. Protection of consumers is also regulated in Law Number 8 of 1999 concerning Consumer Protection, which affirms that consumers have the right to safety, comfort, and security in using services (Article 4), and provides the right to compensation if experiencing losses due to these services (Article 19).[29] In this case, digital bank customers are positioned as financial service consumers who have the right to demand accountability for losses due to loss of funds in accounts that are not caused by personal error.

Furthermore, Law Number 10 of 1998 concerning Banking also presents a fundamental foundation for banks in maintaining and preserving public trust, where that trust is primarily reflected in a bank's ability to protect public deposit funds.[30] These rules also emphasize the importance of the prudence principle (prudential banking principle), and violations of this principle in the context of digital banking can result in the failure of oversight functions and risk management, which then harms customers.

The relevance of PBI No. 14/2/PBI/2012, which talks about electronic money, cannot be ignored, considering that in practice, digital bank payment systems are often integrated with e-money instruments or digital wallets that are marked as capable of bringing risks of fund loss due to hacking or data misuse. The regulation essentially requires electronic money providers to adopt strong security systems and risk management, while emphasizing the importance of service provider responsibility in ensuring guarantees for consumer protection.

3.4 Digital Bank's Responsibility Towards Customer Data Protection

Customers as owners of funds stored in digital banking besides also become causes of fund loss, precisely as a result of customer carelessness itself.[31] Customers unconsciously leak data such as private passwords to unknown parties, which can occur because customers receive electronic message information through phones or computers containing access links to certain websites from third parties, but on behalf of digital banks. When customers click on links, it results in the leakage of username and password data being breached. Digital banks in this context will only replace losses if caused by negligence of banking systems.[32]

[29] "Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen" (1999).
[30] "Undang-Undang Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan" (1998).
[31] Hetty Karunia Tunjungsari, Rahmat Aji Nuryakin, and Romi Ilham, *Customer Experience 5.0: Meningkatkan Loyalitas Di Era Digital* (Padang: Takaza Innovatix Labs, 2025).
[32] Revalina Annisa Antoine et al., "Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia)," *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 316–27, https://doi.org/10.61722/jmia.v2i1.3147.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

The existence of digital banks that are closely related to cyberspace triggers separate concerns, especially those related to the potential for system misuse by unauthorized individuals or groups.[33] In this case, parties with certain technical expertise can infiltrate digital bank systems and access deposit funds that are not their rights. Similar phenomena like this only emerge in digital worlds, which are marked as part of hacking techniques, where hackers can break into systems and steal customer data and funds.[34]

According to what is stated in Article 29 POJK No. 6/POJK.07/2022, the responsibility of digital banks for loss of customer funds is limited only to situations where harmful actions are carried out by internal bank parties, namely related to management or employees, or by third parties acting for and on behalf of digital banks.[35] In other words, if hacking actions are carried out by third parties that have no affiliation or interest relationship with digital banks, then provisions do not explicitly require banks to compensate for losses, which creates normative voids and has implications for legal protection that have not fully touched external cybercrime cases.[36]

This limitation in bank responsibility creates a significant legal loophole. The current regulatory framework fails to address the reality that digital banks, by choosing to operate in cyberspace, inherently expose their customers to cyber risks that do not exist in traditional banking. The question arises whether banks should bear responsibility for losses resulting from their choice of operating environment, even when perpetrated by unaffiliated third parties. Nevertheless, customers still have rights to submit complaints about fund losses that are possibly caused by third parties, as regulated in Article 35 POJK No. 6/POJK.07/2022 which stipulates that digital banks are obliged to follow up on each customer complaint within periods of no later than 20 working days, and can be extended up to 20 working days if there are special circumstances such as needs for in-depth investigation or events beyond bank control, including hacking attacks.

Furthermore, Article 38 letter c in the same POJK requires digital banks to convey apologies and offer forms of recovery (redress or remedy), either in the form of compensation for losses or repairs to products or services that cause losses, if it is proven that customer complaints have a strong basis. This provides normative guarantees that lost

[33] Ana Irawati et al., "Urgensi Cyber Law Dalam Kehidupan Masyarakat Indonesia Di Era Digital," in *Proceeding of Conference on Law and Social Studies* (Madiun: Fakultas Hukum Universitas PGRI Madiun, 2021), 1–13.

[34] Farrel Ardan Rinaldi and Bintang Kusuma Wijaya, "Efektivitas Penegakan Hukum Terhadap Tindak Pidana Perbankan: Studi Kasus Pembobolan Dana Nasabah," *PENG: Jurnal Ekonomi Dan Manajemen* 2, no. 2 (2025): 3437–47, https://doi.org/https://doi.org/10.62710/9pwz7812.

[35] Keuangan, "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan."

[36] Miftah Arifin, Zaenal Arifin, and Mac Thi Hoai Thuong, "The Principle of Proportionality on Digital Business Agreements: Between Mitigation and Orientation," *Indonesia Private Law Review* 4, no. 1 (2023): 47–56, https://doi.org/10.25041/iplr.v4i1.2954.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

customer funds can be returned, and regulates maximum time limits of 40 working days to complete processes thoroughly.[37]

Cases of fund loss in digital bank accounts that tend to involve hacking processes face obstacles in relation to evidence processes, especially if the digital forensic infrastructure owned by banks is limited.[38] Therefore, it is important for digital banks to take appropriate steps and efforts to integrate security technology based on artificial intelligence (AI), biometric authentication, as well as real-time transaction anomaly detection systems to prevent similar incidents.

The inadequacy of current provisions regarding external cyber crimes necessitates regulatory updates. There is an urgent need for explicit regulation of bank responsibility for external cyber crimes that directly impact consumer losses, to create legal certainty and comprehensive protection guarantees for digital bank customers in Indonesia. Such regulations should establish a framework where banks cannot simply disclaim responsibility for losses resulting from the inherent risks of their chosen operating environment.

Besides strengthening legal positions of consumers, these regulations can also provide encouragement for digital banking not only to meet legal formality aspects, but also to internalize risk-based compliance principles in their operational systems. The proposed framework should require banks to implement mandatory minimum security standards and establish shared responsibility mechanisms for losses resulting from external cyber attacks, similar to models implemented in Singapore and Japan, where banks bear greater responsibility for cybersecurity failures.

4. CONCLUSION

Based on the discussion that has been presented, it can be concluded that digital banks are specifically regulated in POJK No. 12/POJK.03/2021, with consumer protection principles referring to provisions of POJK No. 6/POJK.07/2022 concerning Consumer Protection in the Financial Services Sector, including principles of transparency, fair treatment, reliability, confidentiality and data security, complaint handling, and dispute resolution. System failures or weak data security constitute violations of security and reliability principles of electronic systems mandated by the ITE Law, while consumer protection is guaranteed by Law Number 8 of 1999 concerning Consumer Protection and Law Number 10 of 1998 concerning Banking, emphasizing banks' fundamental responsibility to maintain public trust and protect deposit funds. This legal framework is supported by PBI No. 14/2/PBI/2012 concerning electronic money to protect customers from the risks of fund loss due to hacking or data misuse. Article 35 POJK No.

[37] Fuad Nur, "Penegakan Hukum Terhadap Kejahatan Digital Perbankan," *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 3234–49, https://doi.org/https://j-innovative.org/index.php/Innovative/article/view/6617.

[38] Delvyan Putri Surya Ningrum and Jamiatur Robekha, "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia," *Journal Evidence Of Law* 1, no. 1 (2022): 112–28, https://doi.org/https://doi.org/10.56799/peshum.v2i4.2115.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

6/POJK.07/2022 requires digital banks to follow up on customer complaints within 20 working days (extendable to 40 working days), while Article 38 letter c requires banks to provide apologies and recovery forms if complaints are proven valid. This research contributes new insights into the comprehensive regulatory framework governing digital bank customer protection, revealing both strengths and gaps in current enforcement mechanisms while proposing enhanced measures for Indonesia's evolving digital banking sector.

REFERENCES

Antoine, Revalina Annisa, Najalya Siti Farizqa, Alifia Hafizha Hasna, and Masta Pasaribu. "Penyalahgunaan Data Pribadi Dalam Teknologi Transaksi Digital Di Industri Perbankan Digital (Studi Kasus PT. Bank Syariah Indonesia)." *Jurnal Multidisiplin Ilmu Akademik* 2, no. 1 (2025): 316–27. https://doi.org/10.61722/jmia.v2i1.3147.

Arifin, Miftah, Zaenal Arifin, and Mac Thi Hoai Thuong. "The Principle of Proportionality on Digital Business Agreements: Between Mitigation and Orientation." *Indonesia Private Law Review* 4, no. 1 (2023): 47–56. https://doi.org/10.25041/iplr.v4i1.2954.

Aziz, Alfian Rifqi. "Perlindungan Hukum Dan Tanggung Jawab Bank Atas Hilangnya Dana Nasabah (Studi Pada: PT Bank Mandiri Tbk, Cabang Ciceri)." Universitas Islam Indonesia, 2023.

Chairunnisa, Salsabila, Tarsisius Murwadji, and Nun Harrieti. "Perlindungan Hukum Terhadap Nasabah Atas Kejahatan Phising Dan Hacking Pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia." *Hakim: Jurnal Ilmu Hukum Dan Sosial* 2, no. 1 (2024): 1–16. https://doi.org/https://doi.org/10.51903/hakim.v2i1.1535.

Dewi, Davina. "Perlindungan Hukum Nasabah BTPN Jenius Dalam Kasus Pembobolan Dana Rekening." *Fairness and Justice: Jurnal Ilmiah Ilmu Hukum* 21, no. 1 (2023): 9–20. https://doi.org/https://doi.org/10.32528/faj.v21i1.22959.

Fauzadeli, Muhammad Fahri. "Perlindungan Hukum Terhadap Nasabah E-Wallet Atas Kebocoran Data Dan Kehilangan Sejumlah Dana." *Qistie* 15, no. 2 (2022): 224–38.

Fitri, Dita, and Suherman. "Perlindungan Hukum Terhadap Nasabah Perbankan Yang Mengalami Kerugian Atas Pembobolan Rekening." In *Prosiding National Conference on Law Studies (NCOLS)*, 2:274–92, 2020.

Gaib, Djuwita N. "Dinamika Hukum Perbankan Digital Di Indonesia." *Lex Et Societatis* 7, no. 11 (2019). https://doi.org/https://doi.org/10.35796/les.v7i11.27366.

Irawati, Ana, Hasan Bachtiar Fadholi, Alfarozi Nur Alamsyah, Dimas Pramodya Dwipayana, and Moh Muslih. "Urgensi Cyber Law Dalam Kehidupan Masyarakat Indonesia Di Era Digital." In *Proceeding of Conference on Law and Social Studies*, 1–13. Madiun: Fakultas Hukum Universitas PGRI Madiun, 2021.

Ivanca, Eveline, and Hery Firmansyah. "Perlindungan Hukum Pengguna Mobile Banking Sebagai Korban Kejahatan Melalui Internet Ditinjau Dari Hukum Positif." *UNES Law Review* 6, no. 2 (2023): 6166–74. https://doi.org/10.31933/unesrev.v6i2.1137.

Kadari, Pakhry Nugroho, Saharuddin Saharuddin, and Muh. Akbar Fhad Syahril. "Perlindungan Hukum Nasabah Atas Penggunaan E-Banking." *Jurnal Litigasi Amsir* 10, no. 2 (February 2023): 167–79.

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

https://doi.org/https://journalstih.amsir.ac.id/index.php/julia/article/view/238.

Kennedy, A. "The Role of Indonesian Constitutional Law in Sustaining National Resilience Amid Global Challenges." *Jurnal LemhannasRI* 12, no. 4 (2024): 485–508. https://doi.org/10.55960/jlri.v12i4.957.

Keuangan, Otoritas Jasa. "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22/POJK.04/2021 Tentang Penerapan Klasifikasi Saham Dengan Hak Suara Multipel Oleh Emiten Dengan Inovasi Dan Tingkat Pertumbuhan Tinggi Yang Melakukan Penawaran Umum Efek Bersifat Ekuitas Berupa Sa." Jakarta: Otoritas Jasa Keuangan Republik Indonesia, 2021.

———. "Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 6/POJK.07/2022 tentang Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan." Jakarta: Otoritas Jasa Keuangan Republik Indonesia, 2022.

———. "Tanya Jawab Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2021 Tentang Bank Umum," 2021.

Larasati, E. "Tumbuh Kuat Di Kuartal II, Investasi Jadi Motor Penggerak Pertumbuhan Ekonomi 2021." *Badan Kebijakan Fiskal*, September 2021.

Mochammad Su'eb, and Yonika Nazla Rohma. "Peran Otoritas Jasa Keuangan (OJK) Dalam Pasar Uang Dan Modal Di Era Digital." *Jurnal Penelitian Ilmu Ekonomi Dan Keuangan Syariah* 3, no. 2 (May 2025): 107–17. https://doi.org/10.59059/jupiekes.v3i2.2386.

Muarief, R. *Bank Dan Lembaga Keuangan Lainnya: Fondasi Sistem Keuangan*. [Kota tidak disebutkan]: Asadel Liamsindo Teknologi, 2024.

Ningrum, Delvyan Putri Surya, and Jamiatur Robekha. "Analisa Yuridis Dalam Kasus Kejahatan Siber Terhadap Internet Banking Di Indonesia." *Journal Evidence Of Law* 1, no. 1 (2022): 112–28. https://doi.org/https://doi.org/10.56799/peshum.v2i4.2115.

Nur, Fuad. "Penegakan Hukum Terhadap Kejahatan Digital Perbankan." *Innovative: Journal Of Social Science Research* 3, no. 6 (2023): 3234–49. https://doi.org/https://j-innovative.org/index.php/Innovative/article/view/6617.

Prawira, Bayu. *Transformasi Digital Bank Di Indonesia, Konsep Dan Praktek Dalam Memimpin Transformasi Total*. Malang: Media Nusa Creative, 2021.

Putre, Kadek Adi, and Putri Triari Dwijayanthi. "Perlindungan Hukum Dana Nasabah Yang Hilang Pada Bank Digital." *Jurnal Kertha Desa* 10, no. 9 (2023): 934–42.

Riazti Gitazia, Anggi, and Muhaimin Muhaimin. "Tinjauan Yuridis Bank Digital Dalam Perspektif Bank Indonesia." *Commerce Law* 3, no. 1 (June 2023): 203–17. https://doi.org/10.29303/commercelaw.v3i1.2807.

Rinaldi, Farrel Ardan, and Bintang Kusuma Wijaya. "Efektivitas Penegakan Hukum Terhadap Tindak Pidana Perbankan: Studi Kasus Pembobolan Dana Nasabah." *PENG: Jurnal Ekonomi Dan Manajemen* 2, no. 2 (2025): 3437–47. https://doi.org/https://doi.org/10.62710/9pwz7812.

Saputra, Moch P, Sukono, and Diah Chaerani. "Estimation of Maximum Potential Losses for Digital Banking Transaction Risks Using the Extreme Value-at-Risks Method." *Risks*, 2022. https://doi.org/10.3390/risks10010010.

Syariah, Bank Mega. "Bank Digital: Pengertian, Manfaat, Dan Tips Memilihnya," 2024.

Tasman, T, and U Ulfanora. "Perlindungan Hukum Terhadap Nasabah Bank Digital."

Received: 15-5-2025
Revised: 22-5-2025
Accepted: 9-6-2025
e-ISSN: 2621-4105

UNES Law Review 6, no. 1 (2023): 1624–35. https://doi.org/10.31933/unesrev.v6i1.962.

Tunjungsari, Hetty Karunia, Rahmat Aji Nuryakin, and Romi Ilham. *Customer Experience 5.0: Meningkatkan Loyalitas Di Era Digital*. Padang: Takaza Innovatix Labs, 2025.

Undang-Undang Nomor 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang perbankan (1998).

Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen (1999).

Utami, D., and Y. Yennisa. "Faktor-Faktor Mempengaruhi Ketepatan Waktu Pelaporan Keuangan Pada Perusahaan Sub Sektor Bank Di Bursa Efek Indonesia." *Akuntansi Dewantara* 1, no. 1 (2017): 31–38. https://doi.org/https://doi.org/10.26460/ad.v1i1.22.

Wala, G., and H. Firmansyah. "Konsep Restorative Justice Untuk Mengurangi Over Capacity Pada Perkara Pidana." *Jurnal Kertha Semaya*, 12, no. 2 (2024): 247–54. https://doi.org/https://doi.org/10.24843/KS.2024.v12.i02.p19.

Wijaya, Krisna. "Digital Banking VS Digital Bank." *Majalah Info Bank Lppi*, no. 1 (2021): 1–5.