JCS Journal of Comprehensive Science
JOURNAL OF COMPREHENSIVE SCIENCE
Published by Green Publisher
Crossref Google Scholar GARUDA PKP|INDEX

Journal of Comprehensive Science
p-ISSN: 2962-4738 e-ISSN: 2962-4584
Vol. 3. No. 12 December 2024

Transformation of Consumer Protection Against Loss of Customer Funds in Digital Banking

Miftakul Azis[1], Faisal Santiago[2]
Universitas Borobudur, Indonesia[1,2]
Email: azizmoeda@gmail.com[1], faisalsantiago@borobudur.ac.id[2]

Abstract

Digital banking has become a major trend in the global financial sector, offering ease of access and efficiency for customers. However, this development also brings new risks, particularly related to the loss of funds due to cyber attacks. This research analyzes the legal vacuum in the regulations protecting customers of digital banking in Indonesia, particularly as regulated by POJK No. 12/POJK.03/2021 and POJK No. 13/POJK.03/2021. Despite the existing legal framework, this study identifies the weak legal protection for customers regarding the risk of losing funds due to cyber attacks, as well as the lack of clarity regarding the bank's responsibility in such situations. By examining national and international case studies and providing recommendations for regulatory enhancement and security standards, this study aims to contribute to the ongoing efforts to protect consumers in the increasingly complex context of digital banking.

Kata kunci: digital banking, consumer protection, loss of funds, cyber attacks, legal vacuum

INTRODUCTION

Digital banking refers to the use of information and communication technology in the delivery of banking services. This includes all transactions and banking services conducted through digital platforms, such as mobile applications, internet banking, and other technology-based banking services. The main characteristics of digital banking include high accessibility, efficiency in executing transactions, and convenience for users (Barkatullah, 2019). Customers can perform various activities, such as fund transfers, bill payments, account opening, and investments, without needing to visit a physical branch. In addition, digital banking typically offers 24-hour services, allowing customers to transact anytime and anywhere (Gultom & Rokan, 2022). Security is a major concern in digital banking, with the implementation of various technologies such as encryption, two-factor authentication, and advanced security systems to protect customer data and funds (Basoeky et al., 2021).

The growth of digital banking has increased rapidly in recent years, both in Indonesia and around the world. In Indonesia, the adoption of digital banking has been driven by high smartphone penetration, the expanding access to the internet, and changes in consumer behavior that favor convenience and speed in transactions (Christiani, 2016). According to data from the Indonesian Internet Service Providers Association (APJII), the number of internet users in Indonesia has surpassed 200 million, creating a large market for digital banking services. Globalization has also contributed to this development, with many large banks and fintech companies introducing innovative banking solutions to meet the ever-evolving needs of consumers. For example, services such as digital wallets, online loans, and app-based

investments are increasingly available and gaining popularity among the public (Hermansyah, 2020).

At the global level, digital banking has become a major trend that is changing the way banks operate and interact with customers. Many traditional banks are beginning to transform into more digitally-centric institutions to remain competitive. The presence of fintech has also provided a significant boost, introducing more flexible and innovative business models (Ngamal & Perajaka, 2022). According to a report by McKinsey, digital banking is expected to reach a market value of trillions of dollars in the coming years, with growth driven by increased technology adoption among customers and changes in regulations that support innovation. Digital banking offers a range of significant benefits for customers and the banking industry as a whole (Putera & SH, 2020). For customers, one of the main benefits is the ease of access and time efficiency. Customers no longer need to wait in line at bank branches to carry out transactions, which can often be time-consuming. Additionally, with features such as transaction notifications and expense tracking, customers can more easily manage their finances. Digital banking also often offers lower service fees compared to traditional banking services, making it a more economical choice for many people (Roberto, 2020).

Activities conducted through electronic systems, known as cyberspace, despite being virtual, can be considered as real legal actions (Mastur, 2016). Cyberspace is an environment not bound to any physical location, but within it, electronic communication, access to websites, and fund transfers can take place (Maskun, 2022). In this digital world, individuals have the freedom to express themselves, acquire knowledge, and engage in various activities in different ways (Setiawan, 2017). This freedom encompasses a range of actions, including the enforcement of laws and regulations that were once applicable only in the physical world, now also applied in the digital realm. Although the freedom to act in cyberspace is appealing, challenges arise when the regulating laws tend to feel coercive. If existing laws are not balanced with agreements between the parties involved, the essence of the freedom that individuals possess in cyberspace may become irrelevant (Aji, 2016).

Freedom to engage in activities in the digital world, however, can become excessive and potentially infringe upon the rights of others (Prima & Kamaluddin, 2024). In many cases, individuals or groups with specific experience and skills can launch cyberattacks with the intent to harm others for personal gain (Kumalasari, 2021). These attacks often aim to gain unauthorized access to someone else's computer systems or phones, particularly in financial contexts, with the goal of taking over or stealing valuable information stored on those devices. This illustrates that although cyberspace offers freedom, the risks and legal violations also increase with the growing use of technology.

With the advancement of technology, society now has new alternatives for storing valuable assets, especially money (Wiwoho, 2014). Previously, people tended to keep their money in physical places deemed safe or convert it into other forms of value, such as vehicles or technological devices. However, human errors often lead to negligence in safeguarding valuable assets, allowing others to steal or seize them. In this context, the law serves as a reminder to society that taking someone else's property without permission is an illegal act that can lead to imprisonment (Ayuni, 2024).

Nonetheless, some individuals still ignore these legal warnings, continuing illegal practices for various reasons, such as urgent financial needs. They exploit the negligence of others who are not vigilant about their asset security. In this case, banks, as institutions managing public funds, become vulnerable targets for criminal activities. With the shift toward digital banking, although banks strive to keep up with the times and strengthen their systems protecting customer funds, there are still loopholes that can be exploited by irresponsible parties to access and steal valuable items stored in digital form (Rahmawati & Rahmawati, 2020).

Legal vacuums refer to situations or issues that are not explicitly regulated by existing legislation (Pratama, 2024). In the rapidly evolving digital era, legal vacuums often arise because current regulations have not been able to accommodate changes triggered by technological advancements. For example, many activities in the digital world are not yet detailed in laws, such as certain forms of digital transactions, personal data protection, and evolving cybercrimes. This creates gaps that certain parties can exploit to operate outside the bounds of legality without fearing clear legal consequences. In the context of digital banking, these legal vacuums also pose risks for customers, as regulations related to fund protection and the security of digital transactions may not adequately address emerging threats like cyberattacks or fraud.

On the other hand, legal vacuums can also create legal uncertainty for parties involved in digital activities. Customers and banking institutions may feel confused about their rights and obligations within the context of digital banking, especially when disputes or issues regarding fund security arise. Moreover, as the law has not explicitly regulated several new aspects of digital technology, the legal resolution process could be slow or even misdirected. This vacuum requires a response from policymakers to urgently formulate relevant, adaptive regulations that encompass various aspects of evolving technology. Thus, addressing legal vacuums in the digital field becomes essential to ensure that the rights of all parties are protected and that digital activities can proceed safely and orderly.

RESEARCH METHOD

The normative juridical research method focuses on studying the legal norms found in legislation, legal doctrines, and judicial decisions (Masidin, 2023). This research aims to identify, analyze, and understand the applicable legal rules and how these rules should be applied in specific situations. In normative juridical research, the primary sources used are primary legal materials, such as laws, government regulations, and court decisions, along with secondary legal materials, including legal literature, academic journals, and opinions from legal experts. This research is often employed to answer theoretical or normative legal questions, which concern what should be done based on the applicable law and to evaluate the alignment between legal norms and their implementation in society.

One of the approaches used in normative juridical research is the statute approach, which emphasizes the study of various laws and regulations relevant to the legal issue being investigated. Researchers analyze the content and structure of the laws and how these laws are applied in practice. In addition, a conceptual approach is also commonly used in normative juridical research. This approach involves studying the legal concepts underlying specific rules or norms, for instance, the concepts of legal protection, justice, or human rights. Through this approach, researchers strive to understand the foundational ideas or legal principles, allowing for an examination of the alignment between legal concepts and their practical application. Both of these approaches assist in deepening the understanding of law not only from a textual perspective but also philosophically and conceptually.

RESULT AND DISCUSSION

Forms of Legal Protection Provided to Customers of Digital Banking Against the Risk of Loss of Funds Due to Cyber Attacks

Legal protection for customers who lose funds in digital banks is a crucial issue in the era of modern banking, which increasingly relies on technology. According to Article 1 number 22 POJK No. 12/POJK.03/2021 concerning Conventional Banks, digital banks are defined as Indonesian Legal Entities (BHI) that conduct their business primarily through electronic channels without physical branches other than the Head Office or with limited physical offices. Although this distinction emphasizes the digital aspect, institutionally, digital banks remain

banks, whereby their business model does not alter their operational essence. Digital banks are required to meet the requirements set out in Article 24 of the aforementioned POJK, including technology usage and risk management. In raising funds through technology, digital banks have the obligation to protect customer funds. If a bank fails to perform this duty, it may be prohibited from collecting funds and subject to sanctions, including a ban on operating the banking products it runs.

The risk of loss of funds in digital banking is similar to the risks faced in traditional banking, such as the theft of funds or abuse by bank insiders. Additionally, funds may also be lost due to cyber attacks (cyber attacks), which are the primary risk in the digital era. Therefore, risk management becomes an essential element in digital banking to anticipate potential fund loss. It is also important for customers to understand these risks when storing funds with digital banks. Article 12 of POJK No. 1/07/2013 requires banks to inform customers about any changing risks that may occur. If customers disagree with such changes, they have the right to terminate the legal relationship with the bank.

Loss of customer funds becomes one of the main concerns when dealing with digital banks, particularly as cases of theft or loss of funds through banking systems continue to occur. Nevertheless, legal protections for customers have been specifically formulated in POJK No. 12/POJK.03/2021 and further elaborated in POJK No. 13/POJK.03/2021 concerning Consumer Protection. Digital banks are required to apply consumer protection principles, including transparency, data security, complaints handling, and dispute resolution. Banks are also required to have a complaint mechanism that operates 24 hours a day, allowing customers to report incidents and obtain appropriate information and handling when a loss occurs.

Furthermore, if a digital bank fails to respond to customer complaints, the POJK stipulates that the bank may be subject to sanctions ranging from written warnings to freezing or prohibiting the operation of technology information-based products. Although these sanctions are intended to have a deterrent effect, the primary focus remains on efforts to restore lost customer funds to their original condition. If negligence on the bank's part is proven, Article 29 POJK No. 1/07/2013 obliges digital banks to compensate for customers' lost funds. Customers are also not required to prove the loss of funds if there is indication that the fault lies with the bank, including if bank employees were involved in the misuse of customer funds.

Although regulations concerning digital banking have begun to be introduced through various rules, legal protection for customers regarding the risk of losing funds due to cyber attacks is still considered inadequate. In this context, the rapid development of technology has led to legal gaps that have not been fully addressed by the existing regulations. The articles in POJK No. 12/POJK.03/2021 and POJK No. 13/POJK.03/2021 concerning consumer protection, for instance, have provided some general protection mechanisms for customers, but do not detail specific protections against the risks facing digital bank customers, particularly risks associated with cyber attacks.

To this day, cases continue to occur where customers lose funds due to cyber attacks or hacking schemes involving third parties, such as skimming or hacking. When customers lose funds, the dispute resolution process between banks and customers often drags on, and customers frequently have to bear losses without any clear legal certainty regarding compensation or accountability. In many instances, banks claim that the attacks were beyond their control, making it difficult for customers to obtain adequate protection or reimbursement for losses. This illustrates that there is still no comprehensive and firm legal mechanism in place to protect customers from cyber crime risks in the digital banking sector.

Moreover, despite existing regulations emphasizing the importance of risk management and banks' obligations to ensure system security, the established standards and guidelines are still not sufficiently detailed to anticipate the losses customers might suffer. A primary shortcoming is the lack of specific rules regarding banks' responsibilities towards cyber attacks

that successfully breach their systems. While digital banks are required to implement preventive measures, there is no definite obligation regarding compensation if such preventive actions fail. This leaves customers in a vulnerable position, especially if they do not possess adequate technical knowledge regarding digital risks.

Education for customers concerning digital financial risks has also not been clearly regulated. Although regulations require digital banks to provide information about changes in risks, many customers feel inadequately educated about the potential digital threats that could result in the loss of their funds. This lack of understanding may hinder customers' ability to protect themselves against potential cyber attacks, simultaneously making them vulnerable to exploitation. In other words, the existing legal protections remain predominantly general and do not address the specifics of protection related to digital technologies and the increasingly complex cyber threats.

Robust and clear legal protections are urgently needed to balance technology advancements with customer rights. The existence of more detailed and specific regulations regarding cyber risks, banks' responsibilities, and dispute resolution mechanisms must be adopted to provide better guarantees for customers. Digital banks must be required to implement stricter security standards and be held legally accountable when attacks occur resulting in losses to customers. Without these regulations in place, legal protection for customers in digital banking against cyber threats will remain limited, allowing for greater potential violations of consumer rights in the future.

Legal Vacuum in Regulations Protecting Digital Banking Customers Against Loss of Funds Due to Cyber Attacks

Customers who own funds stored in digital banks run the risk of losing funds, particularly in cases of negligence on their part. Often, customers unknowingly disclose personal data, such as passwords, to unauthorized parties. This can happen when customers receive electronic messages containing suspicious links from third parties pretending to act on behalf of the digital bank. When customers click such links, sensitive data like their username and password can be exposed, opening the door for others to breach the customer’s account. However, digital banks typically only assume responsibility for compensating losses when those damages are caused by faults or negligence within the banking system itself.

Alongside risks stemming from customer error, the presence of digital banks operating in a digital space also poses specific threats, such as attacks from hackers. An individual or group can hack a digital bank’s system and illegally withdraw funds that do not belong to them. This activity is known as "hacking" in the digital domain, where hackers exploit security gaps to illegally access customer funds. This scenario mirrors the real-world scenario of bank heists, where criminals seek opportunities for criminal acts. According to Article 29 POJK No. 1/07/2013, digital banks are obliged to compensate customers for losses caused by offenses perpetrated by insiders, such as bank managers or employees. However, this regulation does not clearly specify the bank's responsibility for offenses committed by third parties, like hackers, who have no affiliation with the bank.

In cases of fund loss due to hacking, customers still have the right to file complaints. Under Article 35 POJK No. 1/07/2013, digital banks are required to address customer complaints within 20 working days, with a possibility of an extension of up to 20 additional days if further investigation is necessary or if there are issues outside the bank's control, such as a hacking incident. Moreover, in Article 38 letter c POJK No. 1/07/2013, it is stipulated that if a customer's complaint is proven valid, the digital bank must issue an apology and offer solutions for compensation or service improvements. In this case, customers are assured of having their lost funds restored, provided that the reimbursement must be completed within a maximum of 40 working days.

If the resolution of complaints between customers and digital banks does not reach an agreement, customers have the option to take the matter to the legal route. Resolution can be conducted through courts, alternative dispute resolution agencies, or the Financial Services Authority (OJK) for mediation. While resolution through both judicial and non-judicial processes has its advantages and disadvantages, both offer customers the opportunity to seek justice if they feel wronged by the digital bank. Nevertheless, the existence of grievance resolution pathways aims to ensure that customers receive adequate legal protection.

Digital banking has rapidly developed in recent years, supported by regulations designed to align with the demands of the digital era. However, despite the existence of regulations such as POJK No. 12/POJK.03/2021 concerning Conventional Banks and POJK No. 13/POJK.03/2021 concerning Consumer Protection, there are significant legal vacuums related to customer protection against the risk of losing funds due to cyber attacks. These regulations primarily focus on general consumer protection but are insufficient in addressing specific technical aspects of cybersecurity that are critical in the digital banking ecosystem.

Nevertheless, the Consumer Protection Law in the Financial Services Sector plays an important role as the legal foundation for customer protection. This law emphasizes principles such as transparency, data security, and fair treatment. However, the increasingly complex threats, such as cyber attacks that can result in financial losses for customers, indicate that existing regulations have not completely encompassed effective protection against these risks. In cases of cyber attacks, regulations often do not explicitly mention the bank's responsibility when external hackers successfully breach banking systems.

While POJK No. 12/POJK.03/2021 and POJK No. 13/POJK.03/2021 focus on digital banking regulations and consumer protection in the financial services sector, Article 26 of POJK No. 13/POJK.03/2021 requires banks to implement consumer protection principles, including data security and customer complaint handling. However, there are no special regulations regarding the measures banks must take in response to cyber attacks that involve the theft of customer data and loss of funds as a result of hacking. These regulations are also lacking in clearly explaining the bank's responsibilities in cases where third parties like hackers are the primary cause of customer losses. Conversely, while POJK No. 12/POJK.03/2021 regulates the business model of digital banks with mandatory risk management, this regulation has yet to encompass technical measures that can mitigate hacking risks. Another major flaw is the lack of emphasis on the bank's obligation to provide compensation to customers if a cyber attack occurs due to vulnerabilities in the security systems managed by the banks themselves.

Digital banking regulations in Indonesia are still inadequate in addressing the risks posed by cyber attacks. Hacking or "cyber attacks" are becoming more frequent as digital financial activities increase; however, there is still no clear regulation that imposes firm responsibilities on digital banks for loss of funds due to such attacks. This weakness creates a situation where customers often lack legal certainty regarding the protection of their funds in cases of cyber attacks, particularly if there is no evidence of direct responsibility from the bank. Furthermore, while some regulations mention banks' obligations to address customer complaints, these rules do not explicitly cover guaranteed recovery of funds when hackers are external parties not affiliated with the bank. This indicates that current regulations remain weak in providing concrete legal protection against risks stemming from the digital space.

Various national and international cases demonstrate the vulnerability of digital banks to cyber attacks. One example is the case of card skimming and personal data theft in Indonesia resulting in customer fund loss. In some cases, customers successfully received compensation, but on many other occasions, customers find themselves caught up in complicated and prolonged processes. At the international level, cyber attacks such as hacking against major financial institutions in Europe and the United States indicate similar vulnerabilities. Digital banks often face difficulties in detecting or preventing cyber attacks promptly, particularly due

to the complexity of systems and the evolving nature of the attacks. The legal responsibilities of banks in cases of loss resulting from cyber attacks are often debated, and customers do not always receive adequate protection from existing regulations.

The legal vacuum in protecting digital banking customers is very evident when considering the risks posed by cyber attacks. Although existing regulations encompass general consumer protection, they have not fully responded to increasingly sophisticated cyber threats. This vacuum leads to legal uncertainty for customers who lose their funds due to hacking. Additionally, this legal vacuum also impacts customers' trust in the security of their funds in digital banks. If not addressed, this vacuum could lower public confidence in digital banks and slow the adoption of digital banking in the future. Therefore, the role of the Financial Services Authority (OJK) and the government is essential in closing this legal gap by strengthening regulations governing the responsibilities of digital banks related to cyber attacks.

To address the legal vacuum and protect customers of digital banks from cyber attacks, stricter security standards are needed. Digital banks must reinforce their systems by implementing advanced security measures, such as better data encryption, early detection of attacks, and more effective monitoring of suspicious activities. Additionally, developing specific regulations addressing the risks of cyber attacks should be prioritized. These regulations must include the obligation for banks to provide full compensation to customers if the loss of funds occurs due to hacking, as well as requiring banks to transparently report incidents of cyber attacks to OJK. The legal responsibilities of banks in protecting customer funds must also be strengthened with the obligation to update security systems regularly and educate customers on digital security risks. Consumer protection in the digital financial system not only encompasses technical security aspects but also information transparency and the prompt resolution of disputes. Banks must guarantee that customers will be protected from the risk of losing funds, whether due to internal bank negligence or external attacks. Therefore, stronger regulations and a more robust protection system will enhance customer trust in digital banks in the future.

CONCLUSION

The development of digital banking has opened significant opportunities for advancing technology-based financial services but has also heightened new risks, particularly related to cyber attacks. Although regulations such as POJK No. 12/POJK.03/2021 and POJK No. 13/POJK.03/2021 provide a legal foundation for the operation and consumer protection in the digital banking sector, there exists a significant legal vacuum concerning the protection of customers from the risk of losing funds due to cyber attacks. The existing regulations primarily focus on general consumer protection but do not specifically regulate the mechanisms for handling cyber attack incidents or the obligations of banks in cases of losses caused by external hackers. This creates legal uncertainty for customers who lose funds due to hacking, where the responsibility of banks towards the risks of cyber attacks from third parties has yet to be clearly regulated.

To close this legal gap, there is a need for enhanced and more comprehensive regulations aimed at addressing the risks posed by cyber attacks in digital banking. In addition to strengthening regulations, digital banks should also implement stricter security standards to protect customer data and funds, as well as provide adequate education to consumers regarding the risks present in the digital space. More stringent regulations on banks' responsibilities in cases of cyber attacks, together with efficient dispute resolution systems, will enhance customer protection, increase public trust, and encourage the stability and sustainability of digital banking in Indonesia.

BIBLIOGHRAPHY

Aji, R. (2016). Digitalization, the Era of Media Challenges (Critical Analysis of the Readiness of the Faculty of Da'wah and Communication to Welcome the Digital Era). *Islamic Communication Journal*, *1*(1).

Ayuni, Q. (2024). *The Conception of Emergency Constitutional Law in the Perspective of the 1945 Constitution*. Universitas Indonesia Publishing.

Barkatullah, A. H. (2019). *Electronic Transaction Law in Indonesia: as a guideline in facing the digital era E-commerce business in Indonesia*. Nusamedia.

Basoeky, U., Panggabean, S., Manu, G. A., Wardhana, A., Hoeronis, I., Adnan, Y., & Sudirman, A. (2021). *The Utilization of Digital Technology in Various Aspects of People's Lives*. Indonesian Science Media.

Christiani, T. A. (2016). *Bank Indonesia and the Financial Services Authority in a Legal Perspective*. Cahaya Atma Pustaka Publishing Group of Atma Jaya University Yogyakarta.

Gultom, M. S. D., & Rokan, M. K. (2022). Sharia Banking Problems: Digitalization Solutions and Strategies in Improving the Quality of Banking Products and Services at Bank Sumut Medan Sharia Branch Office. *ALEXANDRIA (Journal of Economics, Business, & Entrepreneurship)*, *3*(1), 14–20.

Hermansyah, S. H. (2020). *Indonesian National Banking Law: 3rd Edition*. Prenada Media.

Kumalasari, V. (2021). PROFESSIONAL ETHICS, in the field of Information Technology. *Publisher of Yayasan Prima Agus Teknik*, 1–75.

Masidin, S. H. (2023). *Normative Legal Research: Analysis of Judges' Decisions*. Prenada Media.

Maskun, S. H. (2022). *Cyber Crime: An Introduction*. Prenada Media.

Mastur, M. (2016). Implementation of Law Number 11 of 2008 concerning Information and Electronic Transactions as Non-Conventional Crimes. *Cosmic Law*, *16*(2).

Ngamal, Y., & Perajaka, M. A. (2022). The application of the digital technology risk management model in banking institutions reflects on the blueprint for digital transformation of Indonesian banking. *Journal of Risk Management*, *2*(2), 59–74.

Pratama, A. (2024). Legal Construction of the Granting of Isbat Marriage to Minors in the Decision of the Tegal Religious Court Number 614/Pdt. G/2022/Pa. Tg. *The Indonesian Journal of Islamic Law and Civil Law*, *5*(1), 109–127.

Prima, J., & Kamaluddin, M. (2024). Constitutional law and social media regulation: maintaining a balance between freedom and order. *J-CEKI: Journal of Scientific Scholars*, *3*(6), 5874–5881.

Putera, A. P., & S.H., M. (2020). *Banking law: Analysis of principles, products, risks and risk management in banking*. Scopindo Media Library.

Rahmawati, I., & Rahmawati, I. (2020). Juridical-normative analysis of the role and actions of telemarketing in digital transactions. *Journal of Legal Horizons*, *11*(1), 60–70.

Roberto, A. (2020). *Get to Know More About Digital Banking Benefits, Opportunities, and Challenges*. http://pasca. UGM. air conditioning. id/.

Setiawan, R. (2017). Individual Freedom of Expression in Human Development in the Digital Era. *Proceedings of the FKIP National Seminar on Education*, *1*(2).

Wiwoho, J. (2014). The role of bank financial institutions and non-bank financial institutions in providing fair distribution for the community. *Legal Matters*, *43*(1), 87–97.

This work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.