**Legal Protection for Customers Against Transaction Security Risks in Digital Banking Services**

**Hassanain Haykal**

Universitas Kristen Maranatha, Bandung, Indonesia

Email: [hassanain.haykal@law.maranatha.edu](mailto:hassanain.haykal@law.maranatha.edu)

**Abstract**

The development of information technology has driven significant transformation in the banking sector through digital banking services. However, this convenience also presents various risks, especially related to transaction security that has the potential to harm customers. This study aims to analyze how legal protection is provided to customers in facing transaction security risks in digital banking services in Indonesia. The research method used is normative juridical with a statutory approach and the concept of consumer protection. Data were obtained through a literature study of related laws and regulations, such as the Consumer Protection Law, the Electronic Information and Transactions Law, and the Financial Services Authority regulations. The results of the study show that legal protection for customers has been regulated in various regulations, but its implementation still faces challenges, especially in terms of customer digital literacy, law enforcement, and dispute resolution mechanisms. This study recommends the need for optimization of supervision by relevant authorities, increased digital literacy education for customers, and strengthening banking cybersecurity standards to minimize risks that can harm customers.

Keywords: Legal Protection, Customers, Transaction Security, Digital Banking.

1. **INTRODUCTION**

Banking is a financial intermediary institution that plays a primary role in collecting funds from the public, which are then redistributed in the form of credit or other financial products. As a trust-based institution, a bank serves as a place for people to deposit their funds and entrust the management of their finances (Park, 2020). In practice, banking is divided into two types, namely conventional banks and sharia banks, each operating based on different principles according to prevailing regulations. The strategic role of banking in the economy is reflected in its function as a provider of liquidity, a driver of investment, and a supporter of financial system stability (Tomasic & Akinbami, 2011). According to Cvijovic et al (2017), the banking industry holds a central position in supporting a country’s economic activities, not only as a provider of funds but also as an institution that ensures the smooth flow of payments and transactions.

Moreover, banking also contributes to improving public welfare by supporting national development. Zhuang et al (2009) emphasize that the existence of banks plays an important role in facilitating the distribution of funds to productive sectors, which ultimately impacts economic growth and improves people's living standards. However, the rapid development of banking services, including product innovations and digitalization, has also intensified competition among banks in attracting customers. The variety of services offered by each bank has become one of the main strategies to gain customer trust and loyalty, while at the same time presenting new challenges for the banking industry to maintain the quality and security of its services amid increasingly tight competition (Balkan, 2021).

Indonesia is a country that heavily depends on the existence of banks, considering that banks function as both a gateway and a bridge for the public in carrying out various economic transactions. Banks play an important role in operating the payment system, are a primary source of credit for business capital needs, and are a key pillar in supporting business activities and national economic growth (Soejachmoen, 2016). In addition, the classic function of banks as a safe place to store public funds remains the main reason why customers entrust their money to these institutions. To ensure the function and sustainability of banking, Indonesia has established a legal framework governing this industry, among others through Law Number 10 of 1998 concerning the Amendment to Law Number 7 of 1992 on Banking, which serves as the main foundation for banking business activities in Indonesia. In addition, Law Number 21 of 2008 on Sharia Banking specifically regulates the existence and activities of banks that operate based on sharia principles (Tabalujan, 2011).

Along with the times and advances in information technology, the banking has undergone significant transformation with the emergence of digital banks. The presence of these digital banks is not merely complementary, but has become an important part in shaping a new digital-based economic ecosystem (Ortino, 2022). As the main pillar of financial institutions, banks are required to be able to adapt and transform in order to remain competitive and relevant. To regulate digital banking services, the Financial Services Authority issued specific regulations, including Regulation of the Financial Services Authority Number 12/POJK.03/2018 on the Implementation of Digital Banking Services by Commercial Banks, which serves as the legal basis for banks in developing digital-based services (Robing et al., 2024).

Behind the convenience and efficiency offered by digital banking services, there are various potential risks that must be anticipated. One of the main risks is the increasing violations of the law related to personal data through the internet. In the digital era, customers’ personal data becomes a very valuable asset and is vulnerable to misuse (Liyanaarachchi et al., 2021). Cybercriminals can easily access, obtain, and even trade personal data without the owner’s knowledge. Data breach cases that occur not only result in violations of privacy rights but also cause public anxiety that can erode the level of trust in digital banking services. This compels the banking industry to continuously strengthen data security systems to protect customers’ personal information in accordance with the principles of prudence and applicable data protection regulations (Wang et al., 2024).

In addition to risks in the aspect of personal data protection, digital banking services also bring significant financial risks to customers. The use of internet banking opens up opportunities for cybercrimes such as phishing, malware, and skimming, which can cause direct financial losses to customers (Al-Surkhi & Maqableh, 2024). This condition pushes banks to prepare various information technology security measures to ensure the safety of electronic transactions, such as the implementation of multi-layer authentication, data encryption, and real-time transaction monitoring. However, strengthening security systems alone is not enough without awareness and digital literacy from the public as users of these services. Thus, protection for customers requires synergy among regulations, banking technology innovations, and continuous education so that these risks can be minimized (Gualdono et al., 2017).

Legal protection for customers is a very important aspect in the conduct of business activities, especially in the banking sector. With the guarantee of legal protection, customers will feel safer and more comfortable in carrying out various financial transactions, including in using digital banking services (Chellappa & Pavlou, 2002). This legal protection should essentially be directed at creating a sense of security, minimizing the risk of losses, and ensuring that customers’ rights are fulfilled. According to Hurley et al (2014), the relationship between banks and customers is the key to the banking world, because through sufficient trust and protection, customers can continue to grow and ultimately provide broader benefits to the economy. Without the presence of customers, banks would not be able to perform their function as financial intermediary institutions that sustain the wheels of the economy.

However, in the context of digital banking, the issue of legal protection for customers has become increasingly complex. The rapid development of technology is not always accompanied by adequate regulatory readiness. The lack of specific rules that comprehensively regulate the protection of customers in digital banking services makes this topic important to be further studied (Giannakoudi, 1999). This concerns the relationship between the public as service users and financial service providers that have greater resources and bargaining positions. Therefore, efforts are needed to strengthen regulations that not only protect customers from the contractual side but also from the side of personal data protection and transaction security, so that a balance of interests between banks and customers can be created in a healthy and fair digital banking ecosystem (Sasea & Sakmaf, 2023).

Several previous studies have discussed the issue of legal protection in digital banking services from various perspectives. Van de Meulen (2013), through her research on customer legal protection in electronic transactions of digital banking, focused on the civil liability of banks in cases of fraud that harm customers, emphasizing dispute resolution and compensation for losses. Meanwhile, Ilmih (2020) examined the protection of customers’ personal data in digital banking transactions by reviewing the bank’s obligation to maintain data confidentiality based on the Law on Information and Electronic Transactions as well as Financial Services Authority regulations, although they were more focused on privacy protection without elaborating on transaction risks comprehensively.

The study by Khattak et al (2021) is also relevant, which analyzed the security risks of internet banking services on consumer protection, but the discussion was more on identifying types of security risks, without delving into a comprehensive legal protection framework. On the other hand, Maladi (2016) examined the effectiveness of consumer protection regulations in digital financial services, but this research was general to digital financial services and did not specifically explore the legal protection of digital bank customers who have their own operational characteristics.

From these studies, it is apparent that there is an important research gap that needs to be addressed. Most previous studies were still limited to discussing personal data protection, civil liability of banks in cases of fraud, or the effectiveness of consumer protection regulations in digital financial services broadly, without specifically examining the legal protection of customers against transaction security risks in digital banking services in Indonesia in an integrated manner. Therefore, this research is important to be conducted to provide scientific contributions in filling that gap, by focusing on the legal protection of digital bank customers in facing electronic transaction risks, including the urgency of strengthening regulations to provide a sense of security for customers in the digital era.

1. **METHOD**

The research method used in this study is a normative legal approach. This approach combines a study of legal norms contained in laws and regulations (normative aspect) with an analysis of how these norms work in practice in society (empirical aspect) (Negara, 2023). Thus, this study does not only stop at the textual or theoretical level, but also explores the social reality related to the application of legal rules. In the context of this research, a normative study is conducted by examining banking regulations in Indonesia such as Law Number 10 of 1998 concerning Banking, the Consumer Protection Law, the ITE Law, the Personal Data Protection Law, OJK Regulation Number 12/POJK.03/2021 concerning Commercial Banks, and other relevant regulations. This normative analysis will identify the extent to which the existing legal framework provides protection for digital bank customers in facing transaction security risks. In addition, this study also analyzes how these laws and regulations provide legal certainty, justice, and protection of customer rights in the context of digital banking services. By using normative legal methods, this research is expected to provide an in-depth understanding of the legal construction of digital bank customer protection, as well as identifying weaknesses or legal gaps that may exist, so that it can contribute to improving regulations in the future.

1. **RESULT AND DISCUSSION**

**Analysis of Transaction Security Risks in Digital Banking Services**

The development of digital banks in Indonesia has shown a significant increase, driven by the shift in community activities from conventional patterns toward digitalization. This phenomenon cannot be separated from the tendency of society to increasingly prioritize digital activities because they are considered more practical and efficient. As a response to this dynamic, the Financial Services Authority of Indonesia issued Financial Services Authority Regulation Number 12/POJK.03/2021 concerning Commercial Banks, which serves as the legal basis for conducting digital banking activities in Indonesia. This regulation was formulated with the aim of supporting economic growth and maintaining national stability through the strengthening of a competitive banking industry that is also adaptive to technological developments and banking business trends.

In addition, the Financial Services Authority also more specifically regulates digital services through Financial Services Authority Regulation Number 12/POJK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks. In this regulation, digital banking services are defined as electronic services designed to maximize the use of customer data so as to provide faster, easier services that suit customer needs (customer experience). These services enable customers to carry out transactions entirely independently, while still paying attention to security aspects in every implementation. The analysis of transaction security risks in digital banking services includes the identification, evaluation, and mitigation of various potential threats that could endanger customer data and transactions. Below are some of the main security risks in digital banking transactions:

1. **Identity Theft**

Identity theft is one of the serious risks faced by customers in using digital banking services. This risk arises when customers’ personal data, such as identification numbers, biometric data, or account information, is unlawfully obtained by irresponsible parties. The stolen data is then used to carry out various illegal actions, such as making transactions without the data owner’s permission, applying for loans in the customer's name, or even opening fake accounts used for money laundering or financing other crimes. This phenomenon of identity theft not only causes financial losses but can also reduce public trust in the digital banking system. Therefore, the protection of customers’ personal data becomes a crucial aspect that must be seriously addressed by banks through the implementation of strict security standards, as well as by regulators through strengthening regulations and continuous supervision.

1. **Deceptive Attempts to Obtain Personal Information (Phishing)**

Deceptive attempts to obtain personal information, commonly referred to as phishing, are one type of cybercrime that often occurs in digital banking services, where perpetrators impersonate banks or official financial institutions with the aim of tricking customers into voluntarily providing sensitive information. This mode is usually carried out via email, text messages, or fake links that appear convincing, making victims unaware that they are interacting with unauthorized parties. The requested information, such as usernames, passwords, or one-time passwords, is then used by the perpetrators to access the customer’s account and perform transactions without permission. These phishing attacks are very detrimental because they are often not detected until the customer’s funds have been drained. Therefore, educating customers as well as implementing strong verification and detection systems are important steps in preventing this crime.

1. **Malicious Software (Malware)**

Malicious software, or malware, is one of the main threats in digital banking security that can secretly infect customers’ devices, such as smartphones or computers. This malware usually infiltrates through downloading unauthorized applications, suspicious links, or harmful email attachments. Once it infects the device, the malware can work to steal important customer information, including login credentials, card data, as well as personal identification numbers and one-time passwords, without the owner realizing it. Furthermore, some sophisticated types of malware are capable of directly modifying transaction instructions, so that funds that should be transferred to legitimate accounts can be diverted to the accounts of the perpetrators. This condition certainly causes significant financial losses and undermines customer trust in digital banking services. Therefore, layered protection both from the banking technology side and customer vigilance is needed to mitigate the risk of malware attacks.

1. **Technical Risks**

Technical risks in digital banking services include various problems arising from failures or weaknesses in the information technology systems used by banks. These can be errors in mobile banking applications, disruptions on servers, or interruptions in data communication networks that cause transactions to stop or be delayed. Although these risks are not always caused by criminal acts, their impact remains significant because they can hinder transaction processes, cause errors in balance records, and even open opportunities for cybercriminals to exploit system weaknesses. Such technical issues also have the potential to cause financial losses for customers and damage the bank’s reputation if not promptly addressed. Therefore, strengthening technological infrastructure, conducting regular testing, and implementing reliable recovery systems are important steps in mitigating technical risks in digital banking services.

1. **Compliance Risks**

Compliance risks in digital banking services arise when banks fail to fulfill legal obligations related to the protection of customers’ personal data, which have been regulated in various regulations such as the General Data Protection Regulation at the international level as well as the Law on Personal Data Protection in Indonesia. Non-compliance can occur in various forms, such as weak privacy policies, negligence in obtaining consent for data processing, or failures in securing data that result in information leaks. If violations occur, banks not only face the risk of administrative sanctions and large fines but also a decline in public trust that can have long-term impacts on business sustainability. Therefore, banks are required to apply the principle of prudence by ensuring every operational procedure complies with the prevailing regulations, conducting regular compliance audits, and building a culture of data protection in every operational line to minimize this compliance risk.

Banks in Indonesia have undertaken various risk mitigation measures for digital banking services, yet challenges and risks continue to evolve alongside technological advancements. The following are several risk mitigation steps that have been implemented by banks:

1. **Enhancement of System Security**

Enhancing system security is a primary focus for banks in addressing various risks associated with digital banking services. This effort is carried out through several strategies, one of which is strengthening cybersecurity by building more robust digital infrastructure. Banks utilize technologies such as data encryption, firewalls, and intrusion detection systems to protect sensitive data from hacker attacks and prevent the theft of customer information. In addition, banks implement two-factor authentication, which combines something known by the user (for example, a password) with something owned (such as a one-time password code sent to a mobile phone) to ensure that only legitimate customers can access their accounts. Not only that, banks also proactively monitor customer activities in real time to identify unusual transaction patterns or suspicious activities that may indicate attempted fraud or identity theft. This multi-layered approach is expected to increase customer trust and minimize the risk of losses due to cybercrime.

1. **Protection of Personal Data**

In efforts to strengthen legal protection and maintain customer trust, banks also emphasize compliance with data protection regulations, such as the General Data Protection Regulation, which has become a global standard in the management of personal data. This compliance is realized through the implementation of strict data protection policies and continuous internal supervision. Moreover, banks ensure that customer data is stored in secure and encrypted systems, so that only authorized parties can access this information, thereby minimizing the risk of data leaks or misuse. Equally important, banks apply the principle of transparency in data usage by providing clear and easily understood explanations to customers regarding how their personal data is collected, used, and kept confidential. These measures are expected not only to fulfill legal obligations but also to strengthen customers’ sense of security and loyalty toward digital banking services.

1. **Policies and Procedures**

To ensure the security of digital banking services remains maintained, banks implement comprehensive risk management to identify, assess, and control various potential risks, ranging from operational risks to cyber risks. This system helps banks map out potential threats early and formulate appropriate mitigation measures. Additionally, banks place significant attention on the capacity of their human resources by providing special training to employees so they can recognize, prevent, and handle various forms of cybersecurity threats as well as continuously evolving fraud schemes. Furthermore, to anticipate the worst-case scenarios, banks have prepared systematic emergency response procedures as guidelines when security incidents or system failures occur. With these procedures, banks can respond quickly and effectively, minimize the impact on operations and customers, and ensure that service recovery can be carried out as promptly as possible. This holistic approach serves as an essential foundation in maintaining the sustainability and reliability of digital banking services in an era increasingly vulnerable to technological attacks.

1. **Supervision and Regulation**

Supervision and regulation are crucial pillars in safeguarding the security of digital banking services in Indonesia. In this regard, the Financial Services Authority plays a strategic role as an institution that supervises and ensures that every bank complies with security standards and implements adequate risk mitigation measures. The Financial Services Authority not only conducts direct supervision but also establishes various regulations and guidelines, such as regulations concerning the provision of digital banking services, which are designed to protect customers while maintaining the stability of the national financial sector. Through these regulations, banks are required to implement reliable security systems, safeguard the confidentiality of customer data, and be prepared to face operational and technological risks. These efforts are expected to enhance public trust in digital banking services and create a healthy and sustainable financial ecosystem.

**Legal Protection of Customers from Security Risks in Digital Banking Transactions**

Strong legal protection plays an essential role in maintaining and increasing customers’ trust in digital banking services. In today’s digital era, financial transactions are no longer limited to face-to-face interactions or the use of physical documents, but have shifted to online platforms that heavily rely on information technology systems. This opens up opportunities for various risks to emerge, such as theft of personal data, misuse of accounts, and other cybercrimes. With the existence of a clear and binding legal framework, customers obtain assurance that their rights are protected by the state, and if a violation occurs, there is a legal resolution mechanism that can be pursued to obtain justice.

Furthermore, comprehensive legal protection does not only provide a sense of security for customers but also directly contributes to the growth of a healthy and sustainable digital economy. When people feel confident in using digital banking services, transaction activities increase, financial inclusion expands, and economic circulation becomes more dynamic. This situation will ultimately create a stable and competitive digital ecosystem, while also driving innovation in the financial services sector. Therefore, it is important for regulators and banking service providers to continuously strengthen regulations and increase legal awareness so that they can accommodate technological developments while protecting the interests of customers.

There are several regulations governing consumer protection in digital transactions, particularly in the context of digital banking services in Indonesia:

1. **Law Number 10 of 1998 concerning Banking**

Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking is the main legal foundation for the implementation of banking activities in Indonesia. This law regulates various matters ranging from the definition of banking business, prudential principles, bank secrecy, to supervision by the relevant authorities. Although this law was enacted before the digital era developed rapidly, its provisions remain the legal umbrella that underpins all banking activities, including the transformation of services towards digitalization. This demonstrates the flexibility of banking law in accommodating innovation and technological developments.

In a relevant manner, the Banking Law contains several provisions that form the basis for the use of information technology in banking services. For example, in Article 6 letter c, it is stated that the business activities of commercial banks include “carrying out payment traffic.” In its development, payment traffic is carried out not only conventionally but also through electronic and digital means, such as internet banking, mobile banking, and application-based digital banking services. This normatively provides space for the practice of digitalization of transactions carried out by banks.

In addition, the prudential banking principle affirmed in Article 2 of the Banking Law becomes an important foundation in the implementation of technology in banking activities. Banks are required to conduct their business based on the prudential principle to maintain public trust, including in the use of information technology that may pose new risks such as data security risks and digital operational risks. Therefore, even though it does not explicitly mention the term “digital,” this article mandates banks to ensure that the digital systems implemented can mitigate these risks for the protection of customers.

This law also emphasizes bank secrecy in Article 40, which regulates the obligation of banks to keep confidential information regarding their depositors, except under certain circumstances regulated by law. In the context of banking digitalization, this provision is very important to ensure that customer data, which is now also stored in electronic systems, remains protected with the same confidentiality standards as manual data. This becomes the legal basis for banks to ensure the protection of customer data both physically and in digital form.

Thus, although Law Number 10 of 1998 concerning Banking does not specifically formulate digital services, the substance of its articles remains highly relevant and becomes the legal framework for the digital transformation of banking. Derivative regulations such as regulations of the Financial Services Authority concerning digital services were later issued to more technically regulate how the digitalization of banking services can be carried out in accordance with the prudential principle, data protection, and public trust mandated by this law. This shows that the Banking Law serves as the main foundation supporting the development of digital banking services in Indonesia.

1. **Law Number 8 of 1999 concerning Consumer Protection**

Although the Consumer Protection Law does not specifically regulate digital transactions, this law remains a very important legal foundation in providing protection to consumers, including bank customers who conduct digital transactions. As a general regulation regarding the relationship between business actors and consumers, this law establishes basic principles that must be implemented by every business actor to protect the rights of consumers from harmful practices. In the context of digital banking, this protection becomes increasingly relevant given the increasing risks of fraud, data misuse, and service disruptions due to technological transformation.

The Consumer Protection Law regulates several provisions that form the foundation of legal protection for consumers. One of these is contained in Article 4, which explicitly states the rights of consumers, including the right to comfort, security, and safety in consuming goods and/or services. This means that customers of digital banks have the legal right to obtain banking services that are safe from the risks of data leakage and unauthorized transactions. In addition, Article 4 also includes the right of consumers to obtain true, clear, and honest information regarding the conditions and guarantees of the services offered. This requires digital banks to disclose their data usage policies and security procedures transparently.

Furthermore, Article 7 of the Consumer Protection Law regulates the obligations of business actors, which in this case include digital banking service providers. Business actors are obliged to act in good faith in conducting their business activities, provide true, clear, and honest information, and ensure the quality of goods and/or services produced and traded. For digital banks, this obligation includes providing adequate security systems to protect customer data and ensuring that transaction services run smoothly as promised. Thus, if there is a violation of these obligations that causes losses to customers, consumers have a legal basis to demand compensation.

In addition, Article 19 also strengthens the legal position of consumers by stipulating that business actors are responsible for providing compensation for damage, pollution, or losses suffered by consumers due to consuming goods and/or services produced or traded. In the context of digital banking, this may include financial losses due to weak bank security systems that result in data breaches or illegal transactions. This article also opens the way for customers to claim their rights through dispute resolution mechanisms.

Thus, although the Consumer Protection Law has not yet specifically regulated digital transactions, this law still provides a legal protection framework that can be used by digital bank customers to claim their rights and obtain a sense of security in every electronic transaction. In the future, this law can be integrated or used as an important reference in drafting more specific regulations related to consumer protection in the digital ecosystem, including the ever-growing digital banking sector.

1. **Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016**

The Law concerning Electronic Information and Transactions is the main regulation that governs activities in the electronic realm in Indonesia. This law contains provisions regarding the operation of electronic systems, electronic transactions, as well as the protection of electronic data and information used in various digital activities. In today’s era of banking digitalization, this law becomes an important legal foundation because it provides a regulatory framework on how electronic systems must be operated reliably, securely, and responsibly. At the same time, it serves as a legal instrument to protect customers of digital banks from the risks of misuse of personal data and increasingly complex cyber-attacks.

The Law concerning Electronic Information and Transactions specifically contains provisions on the obligations of electronic system operators to ensure that the systems they use are secure and reliable. This is regulated in Article 15, which states that electronic system operators are obliged to operate electronic systems in a reliable, secure, and responsible manner and ensure the continuity of the operation of such electronic systems. For digital banking, this article serves as the legal basis that obligates banks to ensure that the applications and information technology infrastructure they use are protected from various security vulnerabilities that can be exploited for data theft or fraud.

In addition, this law also provides legal protection for personal data processed within electronic systems. Although it is not regulated in detail as in the newer Law concerning Personal Data Protection, Article 26 paragraph (1) of this law has already emphasized that the use of any information through electronic media concerning a person’s personal data must be done with the consent of the person concerned. This grants digital bank customers the right to have their personal data not misused by the bank or by third parties without lawful consent.

This law also regulates criminal sanctions for misuse of data or cybercrime. For instance, Article 30 paragraph (1) prohibits any person from accessing another person’s computer and/or electronic system by any means without rights. The sanctions are regulated in Article 46, which stipulates imprisonment of up to six years and/or a fine of up to six hundred million rupiah for violators. In the context of digital banking, this can serve as the legal basis for prosecution if there are parties who illegally access banking systems to steal data or conduct unauthorized transactions.

Furthermore, this law strengthens the government’s efforts to secure the digital ecosystem, including digital banking services. With this regulation in place, customers have a strong legal basis to demand accountability if their personal data is stolen or used without rights, and it ensures that electronic system operators such as banks are obliged to provide systems that are secure and meet proper data protection standards. Thus, this law not only serves as a technical regulatory instrument but also directly protects the rights of digital bank customers in Indonesia.

1. **Law Number 27 of 2022 concerning Personal Data Protection**

Law Number 27 of 2022 concerning Personal Data Protection is a significant milestone in data protection regulations in Indonesia. This law was established as a response to the increasingly urgent legal needs arising from the development of information technology, including in the digital banking sector. This law comprehensively regulates how personal data must be managed, protected, and the rights of individuals (data subjects) as well as the obligations of parties processing the data (data controllers and data processors). In the context of digital banking, this law is crucial to ensure the security and confidentiality of customer data, which is the main foundation of public trust in digital services.

This law explicitly grants rights to data subjects (in this case, customers) over their personal data. Articles 5 through 13 regulate various rights of data subjects, among others: the right to obtain information regarding the processing of their personal data (Article 6), the right to complete and update their personal data (Article 8), the right to delete personal data (Article 9), and the right to withdraw consent to the processing of personal data (Article 10). In digital banking practices, this means customers have full rights to know how their data is used, to request updates if the data is inaccurate, and even to withdraw consent for the use of certain data.

On the other hand, this law establishes very strict obligations for parties processing personal data, including digital banks as data controllers and third parties (such as information technology vendors or cloud service providers) as data processors. Article 39 emphasizes that data controllers are obliged to maintain the accuracy, completeness, and consistency of personal data in accordance with its purpose. Article 40 stipulates that data controllers must implement personal data protection measures against risks of misuse, hacking, or data loss. Furthermore, if there is a failure to protect data, data controllers are obliged to notify the data subjects and the data protection supervisory authority in writing, as stipulated in Article 46.

This law also regulates the lawful grounds for processing personal data as stated in Article 20, such as requiring explicit consent from the data subject or fulfilling contractual obligations, which often becomes the basis for banks to request permission to process customer data. This underscores the need for transparency and documented consent in every digital banking service activity. Thus, the existence of this law provides a legal framework that ensures customers that their personal data is managed securely and responsibly by digital banks. At the same time, this law provides clear guidelines for the digital banking industry to build a strong personal data protection system. In a digital ecosystem that is vulnerable to data breaches and cyber-attacks, compliance with this law is not only a legal obligation but also an essential instrument to maintain reputation and customer trust.

1. **Regulation of the Financial Services Authority Number 12/POJK.03/2021 concerning Commercial Banks**

Regulation of the Financial Services Authority Number 12/POJK.03/2021 concerning Commercial Banks is an important regulation issued by the Financial Services Authority to adjust banking business activities to the development of information technology and the needs of the community, which are increasingly moving toward digitalization. In this regulation, the Financial Services Authority explicitly provides a legal basis for the implementation of digital banking services organized by commercial banks. This regulation replaces the previous regulation of the Financial Services Authority to strengthen the regulatory framework of banking, so that Indonesia’s banking industry remains competitive, is able to adapt to changes, and continues to uphold the principle of prudence.

In the context of providing digital banking services, this regulation stipulates that banks may offer products and activities of digital banking services as part of the adopted business model. This regulation not only opens space for innovation by banks to utilize technology but also obliges the application of adequate risk management principles. One important point is contained in Article 39, which emphasizes the obligation of banks to implement risk management for all of their products and activities, including digital-based services, to ensure the stability and soundness of the bank.

From the perspective of consumer protection, this regulation also emphasizes the importance of fair and transparent treatment of customers. In Article 71, it is regulated that banks must provide sufficient education and information to customers regarding the characteristics of products or services, including the risks inherent in them. This is highly relevant in digital banking services that often utilize electronic platforms, thereby requiring customer understanding regarding the security of using such services.

1. **Regulation of the Financial Services Authority Number 6/POJK.07/2022 concerning** Consumer and Community Protection in the Financial Services Sector

Regulation of the Financial Services Authority Number 6/POJK.07/2022 was issued as an improvement from the previous regulation, with the aim of strengthening consumer protection in the financial services sector, including in digital services that are now growing rapidly. This regulation governs the obligations of financial services business actors—including digital banks—to prioritize the principles of transparency, fairness, reliability, data confidentiality, and effective complaint handling. This is very important given the many financial services that are now digital-based, so the risks to personal data and potential fraud are increasing.

In the aspect of information transparency, this regulation mandates that financial services business actors must provide clear, accurate, and non-misleading information regarding the products and services offered. This is regulated in articles that require the existence of contracts or product information documents that are easy for consumers to understand, including explanations regarding benefits, costs, and risks. For digital services, this includes how personal data will be used as well as the available security features.

This regulation also provides detailed arrangements regarding consumer complaint handling, where banks or financial services business actors are required to provide complaint channels that are easily accessible and to resolve each complaint within the stipulated timeframe. In addition, there is an obligation to carry out risk mitigation of digital services, such as the application of security technologies and systems for monitoring activities that have the potential to harm consumers. Thus, this regulation strengthens the position of consumers in the digital era by ensuring that business actors do not only focus on product innovation but also on protecting consumer interests.

1. **Regulation of Bank Indonesia Number 22/23/PBI/2020 concerning Payment Systems**

Regulation of Bank Indonesia Number 22/23/PBI/2020 concerning Payment Systems was issued as a response to the rapid development of financial technology and transaction digitalization. This regulation governs the organization of payment systems, including the obligation to apply the principles of prudence, security, efficiency, and consumer protection in every activity of payment system operation. This covers services such as digital wallets (electronic wallets), online transfers, Quick Response Code Indonesian Standard (QRIS), to clearing and settlement systems that are all digitally integrated.

One important aspect of this regulation is the provision regarding the management of operational risk and cybersecurity risk. Bank Indonesia requires every payment system operator to ensure that its systems have integrity, reliability, and resilience against disturbances or cyber attacks. This includes the obligation to conduct periodic tests, information technology system audits, and to have incident response plans to ensure service continuity. The main purpose of these provisions is to protect public funds and maintain public trust in digital payment systems.

In addition, this regulation also emphasizes the need to protect consumer rights, including the right to accurate information and effective complaint services. Thus, besides encouraging innovation and efficiency, this regulation functions to ensure that consumers as end users still receive adequate protection, especially related to transaction security and data confidentiality. The existence of this regulation is very important in maintaining the stability of Indonesia’s digital financial system, which continues to develop.

The rapid development of digital technology has had a significant impact on the banking industry, giving rise to increasingly sophisticated and diverse digital banking services. This condition demands adaptive regulations to anticipate technological dynamics while protecting the interests of all parties involved, especially in digital financial transactions. Laws and sectoral regulations continue to be updated, as seen in regulatory updates by the Financial Services Authority, Bank Indonesia, and the emergence of the Personal Data Protection Law. All of these form an important legal foundation to ensure that digital transactions run safely, transparently, and fairly.

On the other hand, digital banking service providers have a major responsibility to ensure that the systems they operate are secure and reliable. They are obliged to implement the latest security technologies, maintain the confidentiality and integrity of customer data, and provide clear information about products and services so that customers can make appropriate decisions. Obligations regarding transparency, complaint handling procedures, as well as risk mitigation efforts must also become the main commitment of the providers so that public trust in digital banking services is maintained.

Equally important, customers as end users also need to improve their digital literacy and legal awareness in using digital banking services. Customers must understand their rights, including the right to personal data protection and the right to obtain complete information, while also being obliged to keep confidential data such as Personal Identification Numbers, passwords, and One Time Password codes so that they are not easily misused by irresponsible parties. With good collaboration among regulators, business actors, and the community, it is hoped that the digital banking ecosystem can grow in a healthy, safe, and sustainable manner, while at the same time driving the growth of Indonesia’s digital economy in the future.

1. **CONCLUSION**

The development of digital technology has brought significant changes to Indonesia’s banking sector. Banking services that were once conventional are now increasingly shifting to a digital model that leverages information technology to provide convenience, speed, and efficiency to customers. However, this progress also opens up new potential risks such as identity theft, phishing, malware, technical risks, and risks related to compliance with data protection regulations. Therefore, legal protection becomes a very important aspect in maintaining public trust in digital banking services. To address these challenges, Indonesia has established various regulations that serve as the legal foundation for the implementation of digital banking services. Among them is Law Number 10 of 1998 concerning Banking, which forms the basis for national banking activities including the utilization of information technology; Law Number 8 of 1999 concerning Consumer Protection, which guarantees the rights of consumers including bank customers; as well as Law Number 11 of 2008 in conjunction with Law Number 19 of 2016 concerning Electronic Information and Transactions, which specifically regulates electronic transactions, the operation of electronic systems, and data protection in digital activities. In addition, there is Law Number 27 of 2022 concerning Personal Data Protection, which is a major milestone in safeguarding customers’ rights to their personal data, obligating banks as data controllers to maintain the security and confidentiality of customer data.

Not only at the level of laws, technical regulations have also been formulated through regulations by the Financial Services Authority and Bank Indonesia. For example, the Regulation of the Financial Services Authority Number 12 of 2021 concerning Commercial Banks provides a legal framework for the implementation of digital banking services, including risk management and consumer protection. Likewise, the Regulation of the Financial Services Authority Number 6 of 2022 concerning the Protection of Consumers and the Public in the Financial Services Sector emphasizes the obligations of financial service business actors to provide information transparency, handle complaints, and mitigate risks. On the other hand, the Regulation of Bank Indonesia Number 22 of 2020 concerning Payment Systems ensures the principles of prudence, security, and protection of consumer rights in digital payment transactions. With this comprehensive legal framework, it is expected that all parties, both providers of digital banking services and customers, can exercise their rights and fulfill their obligations optimally. Banks are required to implement reliable security systems, ensure compliance with data protection, and act transparently in managing customer data. Meanwhile, customers are required to be more vigilant and understand their rights when conducting digital transactions. With adaptive regulatory synergy and compliance by all parties, Indonesia’s digital banking ecosystem can continue to develop in a healthy and secure manner, and make a real contribution to the growth of the national digital economy.

**REFERENCES**

Al-Surkhi, W. A., & Maqableh, M. (2024). The Impact of Cybercrime on Internet Banking Adoption. In *Current and Future Trends on Intelligent Technology Adoption: Volume 2* (pp. 231-245). Cham: Springer Nature Switzerland.

Balkan, B. (2021). Impacts of digitalization on banks and banking. In *The Impact of Artificial Intelligence on Governance, Economics and Finance, Volume I* (pp. 33-50). Singapore: Springer Nature Singapore.

Chellappa, R. K., & Pavlou, P. A. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management*, *15*(5/6), 358-368.

Cvijović, J., Kostić-Stanković, M., & Reljić, M. (2017). Customer relationship management in banking industry: Modern approach. *Industrija*, *45*(3).

Giannakoudi, S. (1999). Internet banking: the digital voyage of banking and money in cyberspace. *Information and Communications Technology Law*, *8*(3), 205-243.

Gualdoni, J., Kurtz, A., Myzyri, I., Wheeler, M., & Rizvi, S. (2017, July). Multi-layer defense model for securing online financial transactions. In *2017 International Conference on Software Security and Assurance (ICSSA)* (pp. 75-79). IEEE.

Hurley, R., Gong, X., & Waqar, A. (2014). Understanding the loss of trust in large banks. *International Journal of Bank Marketing*, *32*(5), 348-366.

Ilmih, A. A. (2020). Legal protection of personal data based on electronic transactions in the era of the digital economy. In *The 2nd International Conference And Call Paper* (Vol. 1, No. 1).

Khattak, S., Jan, S., Ahmad, I., Wadud, Z., & Khan, F. Q. (2021). An effective security assessment approach for Internet banking services via deep analysis of multimedia data. *Multimedia Systems*, *27*, 733-751.

Kitch, E. W. (1980). The law and economics of rights in valuable information. *The Journal of Legal Studies*, *9*(4), 683-723.

Liyanaarachchi, G., Deshpande, S., & Weaven, S. (2021). Market-oriented corporate digital responsibility to manage data vulnerability in online banking. *International Journal of Bank Marketing*, *39*(4), 571-591.

Malady, L. (2016). Consumer protection issues for digital financial services in emerging markets. *Banking & Finance Law Review*, *31*(2), 389-401.

Negara, T. A. S. (2023). Normative legal research in Indonesia: Its originis and approaches. *Audito Comparative Law Journal (ACLJ)*, *4*(1), 1-9.

Ortino, M. (2022). The Functions of Law and of Digital Platforms in the Payment System. *European Business Law Review*, *33*(7).

Park, N. Y. (2020). Trust and trusting behavior in financial institutions: Evidence from South Korea. *International Review of Economics & Finance*, *67*, 408-419.

Sasea, E. M., & Sakmaf, M. S. (2023). Digital Bank Legal Challenges: Security Protection and Leakage of Customer Personal Data. *Awang Long Law Review*, *6*(1), 245-250.

Soejachmoen, M. P. (2016). Financial inclusion in Indonesia: Moving towards a digital payment system. In *Financial Inclusion in Asia: Issues and Policy Concerns* (pp. 131-186). London: Palgrave Macmillan UK.

Tabalujan, B. S. (2001). Corporate governance of Indonesian banks-the legal and business contexts. *Available at SSRN 268569*.

Tobing, C. I., Marwan, A., Wardani, D., Febriana, E., Pasya, P. C., revalinda alfianti Raisah, R., ... & Gunawan, Z. I. (2024). Juridical Review of Indonesian Banking Consumer Services (Commercial Banks and BPR) in the Digitalization Era. *Jurnal Hukum Sasana*, *10*(2), 152-170.

Tomasic, R., & Akinbami, F. (2011). The role of trust in maintaining the resilience of financial markets. *Journal of corporate law studies*, *11*(2), 369-394.

van der Meulen, N. S. (2013). You've been warned: Consumer liability in Internet banking fraud. *Computer law & security review*, *29*(6), 713-718.

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers & security*, *147*, 104051.

Zhuang, J., Gunatilake, H., Niimi, Y., Ehsan Khan, M., Jiang, Y., Hasan, R., ... & Huang, B. (2009). Financial sector development, economic growth, and poverty reduction: A literature review.