JURNAL LITIGASI

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Uncovering Legal Gaps in Digital Banking: Customer Protection and Bank Accountability in Indonesia

Sriono[(1)]
Faculty of Law, Universitas Labuhanbatu
Jl. Sisingamangaraja No. 126 A KM 3.5 Aek Tapa, Balaran Batu, Kec. Rantau Selatan, Labuhanbatu District, North Sumatra, Indonesia.
Email: sriono.mkn@gmail.com

Risdalina[(2)]
Faculty of Law, Universitas Labuhanbatu
Jl. Sisingamangaraja No. 126 A KM 3.5 Aek Tapa, Balaran Batu, Kec. Rantau Selatan, Labuhanbatu District, North Sumatra, Indonesia.
Email: risdalinasiregar@gmail.com

Kusno[(3)]
Faculty of Law, Universitas Labuhanbatu
Jl. Sisingamangaraja No. 126 A KM 3.5 Aek Tapa, Balaran Batu, Kec. Rantau Selatan, Labuhanbatu District, North Sumatra, Indonesia.
Email: Kusno120485@gmail.com

Indra Kumalasari M[(4)]
Faculty of Law, Universitas Labuhanbatu
Jl. Sisingamangaraja No. 126 A KM 3.5 Aek Tapa, Balaran Batu, Kec. Rantau Selatan, Labuhanbatu District, North Sumatra, Indonesia.
Email: Indrakumalasarim@gmail.com

Hengki Syahyunan[(5)]
Faculty of Law, Universitas Labuhanbatu
Jl. Sisingamangaraja No. 126 A KM 3.5 Aek Tapa, Balaran Batu, Kec. Rantau Selatan, Labuhanbatu District, North Sumatra, Indonesia.
Email: hengkihsb31081997@gmail.com

ABSTRACT

Digital bank users in Indonesia are currently so numerous that legal regulations are needed for their users. Writing This will examine the form of legal protection for digital bank customers in Indonesia. The method used in this case is the Normative Juridical Research Method, using library data supported by applicable laws and regulations. The study results indicate that the rules and regulations for protecting the confidentiality of bank customer data in Indonesia are not absolute, and are not subject to one

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

regulation. Still, several regulations are interrelated. The form of legal protection for digital bank customers related to the confidentiality of customer personal data currently does not provide comprehensive legal protection and certainty because the responsibility, both criminal and administrative, is only given to the bank for misuse of data confidentiality.

In contrast, the responsibility for material losses by customers has not been explicitly regulated. Only subject to and bound by the agreement or deal made between the bank and the customer and still requires other efforts in the form of a lawsuit in court. The concept of protecting customer data confidentiality in digital banks can be done responsively, namely by connecting several relevant regulations to provide a sense of justice for customers if customer rights are not protected by banking regulations.

***Keywords**: Bank; Digital Services; Customer Protection; Confidentiality, Personal Data.*

I. INTRODUCTION

A bank is a type of financial organization that serves the community by collecting and distributing money. Banks play a significant part in a nation's development. Funds can be collected from the community through savings by community fund collectors, such as banks. A bank is a financial organization that has been granted the power to disburse monies to the community through banking or credit operations. The primary role of a bank, according to Susilo, Triandaru, and Santoso generally, is to take money from the community and give it back to the community for a variety of uses or as a financial intermediary (Susilo et al., 2006). In Indonesia, the banking sector plays a significant role in economic activity as a financial services industry (Cvijovic et al., 2017). The development of a nation's economy greatly depends on banking services. When there are at least two uses for banking. First, as a service provider, we offer effective payment methods and tools for our clients. The second way that banks can boost cash flow for investment and more productive use is by taking savings from consumers and lending them to parties in need. Banking is a service-oriented industry. Or offerings. The primary functions of banking are to gather community finances (funding), disburse monies to meet community needs (lending and financing), and offer financial services. As the e-commerce industry expands, the banking sector must also be able to keep up with the trend of digital transactions, including the emergence of new fintech sectors and internet-based financial

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

banking services, the number of which is rising in Indonesia (Marlina & Bimo, 2018).

Changes and developments in digital technology are currently taking place very quickly with the launch of the 4.0 revolution especially after the occurrence of Covid-19 (Adiningsih, 2019). Digital transformation has hastened by 5.3 years due to COVID-19 (Ayu, 2021). Digital and the internet have made it difficult for banks, like Bank Indonesia (BI), to stay up with the rate of change. Entering the IT-based industrial era 4.0 is another goal of this endeavor. The enormous potential of digital banking cannot be separated from this. By using information technology to improve customer service, banks are indirectly stepping into a new era known as digital banking (Mbama., 2018). The period of disruption (Industry 4.0) has led to digital transformation, which has altered company models and redesigned current corporate ecosystems into new, more creative, intricate, and dynamic ecosystems. One of the requirements for a bank to provide services financing is the use of information technology (Winasis & Riyanto, 2020). Digital banking services are electronic banking services created by optimizing the use of client data to serve consumers more quickly, easily, and according to their needs (customer experience), according to the Financial Services Authority.

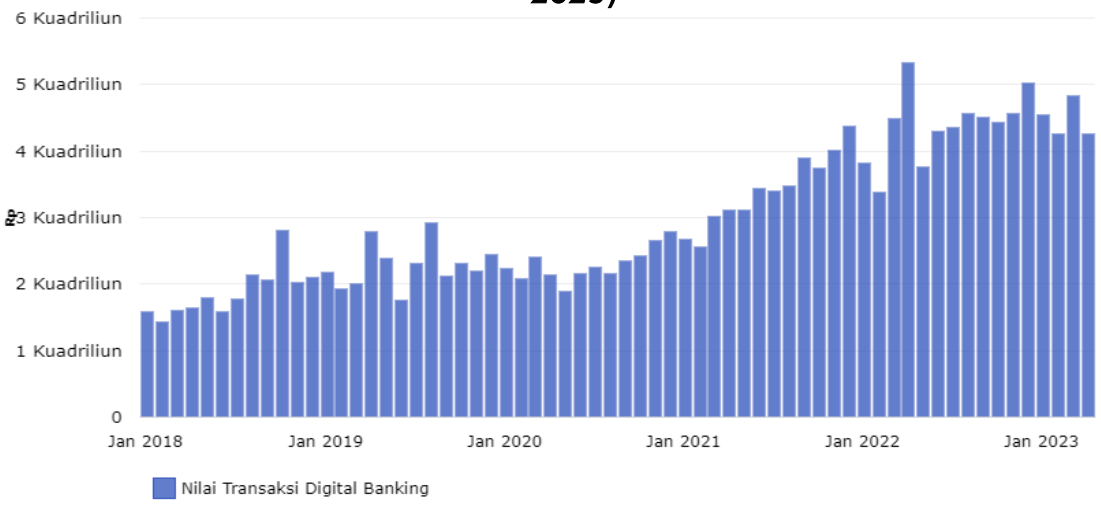
Enhancing the application of risk management in the bank's efficient use of information technology is vital since the provision of digital banking services can increase risk, particularly in operational, strategic, and reputational risk. Compared to current offerings, digital banking is anticipated to offer greater convenience (Kholis, 2020). Customer data misuse is one of the threats that banks face, thus safeguarding customers in digital systems is crucial (Hartono & Atmaja, 2021). To fulfill the principles of confidentiality, integrity, authenticity, cannot be disputed (non-repudiation), and availability, general banks must be prepared to undertake risk management, particularly security control (Edu, 2021).

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

According to data from Bank Indonesia (BI), domestic digital banking transactions were IDR 4,264.8 trillion in April 2023, or nearly IDR 4.3 quadrillion. Here is a graph of the value of digital bank transactions in Indonesia in the last 5 years:

Chart 1. Value of Digital Banking Transactions in Indonesia (January 2018- April 2023)



Source: Bank Indonesia (2023)

With such a large transaction value in digital banks, it has the potential to cause problems in both service and data misuse. The availability of digital financial services causes some issues, such as crime. The prevalence of cybercrime is increasing due to the rapid development of data misuse techniques by careless individuals. Particularly in the digital age, cybercrime has emerged as the most prevalent crime in the financial industry (Tarigan & Paulus, 2019). The development of digital technology affects people. The great aspect of middle society is its convenience, but the negative aspect is the rise of several issues throughout time (Pakpahan et al., 2020).

Crimes involving digital technology, such as misuse of data. Given the prevalence of crimes like data misuse, banks that offer digital services need to be mindful of and safeguard the privacy of client information. Customers who utilize digital banking services will feel more secure thanks to customer protection for

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

digital services. The type of protection offered is a defense against banking crimes or bank exploitation of consumer data. Regulations on the confidentiality of customer data in banking are needed to protect its users (Riswandi, 2005).

Legal protection for digital bank customers in Indonesia is currently regulated in Regulation of the Financial Services Authority of the Republic of Indonesia (POJK) No. 38/POJK.03/2016 concerning the Implementation of Risk Management in the Use of Information Technology. However, the regulation on customer protection is limited to personal data protection and requires digital banks to have a risk management analysis of misuse or criminal acts in digital banks. Article 40 of Law Number 10 of 1998 about Amendments to Law Number 7 of 1992 concerning Banking, which mandates that banks maintain confidential information regarding depositors and their deposits, also governs the bank's duty to protect client data. However, because of the lack of consistency in identifying the groups covered by bank secrecy in the rules and regulations, its implementation or execution is still challenging (Zaini, 2018). Trust is frequently the foundation for this need to protect confidentiality (fiduciary duty). However, in some situations, banks are also required to reveal their clients' financial information and conditions (Djumhana, 1996).

Based on the description above, several problem formulations can be put forward as a basis for limitations in conducting the discussion. The problem formulations are:

1. How does the legislation in Indonesia regulate banks' responsibility for customer data confidentiality?
2. What form of legal protection is there for digital bank customers in Indonesia regarding personal data confidentiality?
3. How is the concept of legal protection for digital bank customers in Indonesia a form of legal certainty?

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

II. RESEARCH METHODS

This research is compiled systematically and descriptively to answer the problems that have been determined. This research uses a normative legal approach method, namely a legal research method used by examining library materials or secondary data (library legal research). Specifically, the approach methods in this study are the statute approach, historical approach, and conceptual approach. These approaches are used to answer the identification of problems. In addition, the research specifications in this paper are descriptive and analytical, while the data collection technique is carried out by studying literature on laws and regulations such as Banking Laws, Consumer Protection Laws, Personal Data Protection Laws, Financial Services Authority Regulations relating to customer protection and the use of information technology, books, and other literature in the form of journals and articles that discuss legal protection and the bank's responsibility for protecting the confidentiality of customer data. All of these legal materials are then analyzed and presented using qualitative legal methods.

III. RESULTS OF RESEARCH AND ANALYSIS

1. Legislation in Indonesia governing banks' responsibility for customer data confidentiality

Banks operating in a country must have a legal basis for their operations. This is to provide legality for the bank and also the customers. The legal basis for operations in the banking system must of course be in the form of laws or regulations that exist in a country. In Indonesia, the laws governing banking are Law Number 7 of 1992 which was amended by Law Number 10 of 1998 concerning banking. The implementation or operational system of banks is regulated through either Bank Indonesia regulations or the Financial Services Authority as a supervisory institution and licensing institution for opening banks in Indonesia.

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Banks can use electronic or digital methods to carry out their activities, including service provision. The Regulation of the Financial Services Authority of the Republic of Indonesia Number 12/POJK.03/2018 serves as the legal foundation for the introduction of digital and electronic services in Indonesia. Digital banking services are defined as electronic banking services that are created by optimizing the use of customer data to serve customers more quickly, easily, and according to their needs (customer experience). Customers can complete these services on their own while keeping security considerations in mind. Banks must apply risk management and the prudential principle when providing digital services (OJK, 2018).

Services provided by banks and are the bank's obligations to customers such as protecting customer data from other parties. The protection provided is in the form of maintaining the confidentiality of customer data. Article 1 number 28 of the Banking Law states that all information about depositors and their funds is considered bank confidentiality. So, the Banking Law emphasizes and narrows the definition of bank secrecy compared to its provisions in the Articles of the previous Law, namely Law Number 7 of 1992 concerning Banking, which does not specifically refer banks to depositors only. From the definition given by Article 1 number 28 and other Articles, the elements of bank secrecy itself can be drawn, namely as follows:

a. Information about depositors and their savings is related to bank secrecy.

b. Must be kept private by the bank unless there is an exception based on the rules, laws, and procedures that apply.

c. The bank itself and/or related parties are forbidden from sharing bank secrets. The following are affiliated parties:

    1. Supervisors, directors, members of the board of commissioners, or their representatives, officials, or workers at the relevant bank;

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

2. Employees, bank officials, supervisors, managers, or committee principals, particularly for banks operating as cooperative legal entities, as defined by applicable laws and regulations;
3. Public accountants, legal consultants, and other consultants are among the service providers to the bank in question;
4. Parties that, in the opinion of Bank Indonesia, have an impact on the bank's management include, but are not restricted to, shareholders, the families of directors, and managers.

The bank is already required by civil and criminal law to maintain bank secrecy. The first reason for the civil requirement is that since the customer and the bank have a fiduciary and confidential relationship, it is morally required that the two maintain their trust and confidentiality. The second is found in Article 1 Number 18 of the Banking Law, which essentially states that the bank's confidentiality relationship is a contractual arrangement with the debtor customer that implicitly requires the bank to maintain the confidentiality of information about the debtor customer. This is supported by the agreement principle outlined in Article 1339 of the Civil Code (henceforth referred to as the Civil Code), which essentially says that the agreement is binding not only on matters specifically mentioned in it but also on anything that, given the terms of the agreement, is required by law, propriety, or custom. Article 40 of the Banking Law regulates the need to safeguard bank secrecy.

In Indonesia, bank secrecy is not always maintained. The notion of relative bank secrecy states that it gives banks the authority to divulge information about their clients or secrets in the event of an emergency, including when doing so would benefit the government (Rossana, 2016). This can be found in the provisions of Article 40 paragraph (1) of the Banking Law which states that the provisions on bank secrecy are exempted from the application in cases as referred to in Articles 41, 41 A, 42, 43, Article 44 and Article 44A of the Banking

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Law, the word "except" is interpreted as a limitation on the application of bank secrecy. Regarding the information mentioned in the previous Articles, the bank may not keep it confidential (Agustina, 2017; Muhammad & Murniati, 2004).

For violations in implementing the provisions on maintaining the confidentiality of customer data, criminal sanctions can be imposed. Criminal penalties as stipulated in Law Number 10 of 1998, Article 47, which states that anyone who willfully coerces a bank or affiliated party to provide information as specified in Article 40 without the Head of Bank Indonesia's written consent or order as mentioned in Articles 41, 41A, and 42, shall be punished by a minimum fine of IDR 10,000,000,000.00 (ten billion rupiah) and a maximum fine of IDR 200,000,000,000.00 (two hundred billion rupiah), as well as imprisonment for at least two (two) years and up to four (four) years. Similarly, individuals who knowingly divulge information that Article 40 requires to be kept private, such as directors, bank staff, or other Affiliated Parties, face a minimum of two years in prison and a fine of IDR 4,000,000,000.00 (four billion rupiah) and a maximum of IDR 8,000,000,000.00 (eight billion rupiah).

The confidentiality of consumer data is a critical component of digital banking services. In addressing this, the Financial Services Authority (FSA) aims to safeguard information technology risk management through the ratified legislation. Several requirements must be met by banks when implementing their digital services, as outlined in the Financial Services Authority of the Republic of Indonesia (POJK) Regulation No. 38/POJK.03/2016 Concerning the Implementation of Risk Management in the Use of Information Technology. For banks to have control over banking technology services, they must be able to recognize and manage technology risks about their directors and internal audits. The Financial Services Authority of the Republic of Indonesia's Regulation No. 12/POJK.03/2021 additionally mandates that banks that use digital services put in place safeguards for the security of customer data. Naturally, it also offers initiatives that support data security, and to facilitate digital transactions safely, it

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

needs to have robust and excellent risk management. Similarly, according to Regulation Number 12/PJOK.13/2018 of the Financial Services Authority of the Republic of Indonesia, all banks offering digital or electronic services must apply security control standards for client information and transactions.

Personal data is data that is protected and kept confidential by the bank from other parties (unless otherwise specified by law). Article 1 number 1 of Law Number 27 of 2022 concerning the protection of personal data states that personal data is data about an individual who is identified or can be identified separately or combined with other information either directly or indirectly through an electronic or non-electronic system. Meanwhile, Personal Data Protection is the entire effort to protect Personal Data in the series of Personal Data processing to guarantee the constitutional rights of Personal Data subjects (Article 1 number 2).

Chapter V of the Financial Services Authority of the Republic of Indonesia Number 12/PJOK.03/2018 Regulation concerning the Provision of Digital Banking Services by Commercial Banks governs the confidentiality of customer data in digital banking services. Banks that offer digital services must follow the consumer protection concept. The Financial Services Authority of the Republic of Indonesia's Regulation Number 1/POJK.07/2013 about the protection of financial service consumers is cited in the application of the consumer protection principle. In this regulation, "consumer protection" refers to safeguarding consumers from the range of actions taken by financial service business actors (OJK, 2013).

The following guidelines must be followed in financial services consumer protection:

1. transparency;
2. fair treatment;

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

3. reliability;
4. privacy and protection of customer data and information; and
5. managing grievances and settling customer conflicts in an easy, quick, and economical manner.

Since corporate players are included in consumer protection, financial services Business actors are required to give and/or communicate information about goods and/or services that is truthful, transparent, and not deceptive. Product and/or service-related information must:

1. provided while educating customers about their rights and responsibilities
2. submitted after reaching a consensus with the customer; and
3. loaded when distributed throughout a variety of media, such as print or electronic media ads.

Legal protection, in the words of Satjipto Rahardjo, is the defense of human rights violated by others, and it is provided to society so that it can benefit from all the rights that the law grants (Rahardjo, 2000). Legal protection, according to CST Kansil, is a range of legal measures that law enforcement officials must take to ensure that people feel safe and secure from disruptions and threats from any source (Kansil, 1989). Philipus M. Hadjon, on the other hand, defines legal protection as an activity taken to safeguard or aid legal subjects through the use of legal instruments (Hadjon, 2011).

According to Article 1 Number 1 of the Consumer Protection Law, every endeavor that ensures legal certainty to safeguard customers is considered consumer protection (Setneg, 1999). The phrase "consumer protection" refers to the legal safeguards provided to customers while they work to satisfy their wants and avoid situations that could endanger them (Sidabalok, 2014). Users of digital banking services are consumers of the banking system, so legal

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

protection for bank users is mandatory in the implementation of the digital banking system (Clevalda & Kharisma, 2021). The Consumer Protection Act must be clear and firm so that it can provide privacy rights and balance between personal data and existing information (Rhoen, 2016).

Because banks, as trust institutions, are obligated to maintain the confidentiality of all information about depositors and their savings, bank secrecy is crucial. Therefore, to prevent criminal or administrative penalties as well as social sanctions from the community, banks as entities and linked parties, including workers and management of the bank in question, must be aware of this bank secrecy legislation.

Customer data confidentiality is important and plays a role in customer trust in using banking services. Protection of customer data confidentiality if based on banking laws is not absolute because in certain circumstances (state interests) banks can provide customer data information. So in its implementation, banks are required to provide information to prospective customers who will use banking services related to customer data confidentiality. Likewise, banks must pay attention to applicable regulations not only limited to banking regulations but also pay attention to regulations outside banking such as personal data protection laws and consumer protection laws.

2. Forms of legal protection for digital bank customers in Indonesia regarding personal data confidentiality

Bank secrecy is a fundamental requirement in any healthy banking system. It stems from the relationship between a bank and its customers, which requires the bank to keep all information held by its customers confidential. Therefore, a customer cannot trust their funds and financial affairs to a bank if the institution does not guarantee the confidentiality of the data owned by the customer. Therefore, this system plays an important role in protecting the banking confidentiality owned by a particular individual or entity.

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Bank secrecy is implemented anywhere in the world, this means that every bank financial institution has bank secrecy. Bank secrecy is a common ethical principle and almost all countries have legal regulations governing bank secrecy. The relationship between customers and banks is a relationship of trust. Banks certainly do not act ethically if they tell other parties about the wealth of a person or legal entity entrusted to them. The obligation to maintain bank secrecy certainly has limits, because the interests of many customers must be considered.

Financial Services Authority Regulation (POJK) Number 12/POJK.03/2021 concerning Commercial Banks is one of the regulations that protects the confidentiality of customer data. This regulation shows that the implementation of banking in providing digital services has legal challenges. The legal challenges for the implementation of digital banking are visible in Article 24 of POJK Number 12/POJK.03/2021. Article 24 of the regulation states that there are at least six legal and regulatory challenges to the implementation of digital banking (Christian, 2021). The legal challenges are:

1. The lack of consumer losses as a result of the adoption of digital banking is known as transaction security. In this instance, specific rules (lex specialis) that govern the protection of customers using digital banking must be added to the current Financial Services Authority Regulation.
2. Article 24 letter (b) of POJK Number 12/POJK.03/2021, which is a derivative of Article 2 of the Banking Law, regulates the term "prudent" in digital banking. It states that Indonesian banks conduct their operations using the principle of prudence, which is founded on economic democracy.
3. There must be sufficient risk management while using digital banking.
4. Special rules pertaining to the application and passing requirements of fit and appropriate tests for potential directors of digital bank organizers must be issued by the Financial Services Authority, an organization that conducts these exams for banking directors.

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

5. Given that banking client data is still frequently misused, data security is a significant concern for the digital sector today.
6. To achieve a cashless or cardless society, regulations that support the implementation of digital banking and other supporting ecosystems must be created. For instance, the use of digital money and the integration of digital banks into trade practices/real sectors and e-commerce require that the implementation of digital banking be able to contribute to the development of the digital financial ecosystem and/or financial inclusion.

Law Number 10 of 1998's Articles 40 through 47 regulate the bank secrecy principle. This article states that banks are obligated to maintain the privacy of depositors' information. Nonetheless, there are some exceptions to the duty to maintain secrecy in these clauses. The goal of bank secrecy is to safeguard the public's interests so that it can be more strongly upheld as a criminal requirement as well as a contractual commitment between the bank and its customers (Ahmad et al., 2022).

The bank may have an express or implicit duty to protect the privacy of its depositors' and savers' information. Generally speaking, the bank-customer agreement does not specifically express that. The obligation to keep confidentiality is seen, for example, in the agreement for opening a savings and deposit account between the bank and its customer. Therefore, the agreement between the bank and its client is regarded as including a tacit obligation to preserve confidential information about the depositor and its funds, even though it is not specifically regulated in the agreement. This is based on the principle of good faith in implementing the agreement.

This is consistent with Law Number 8 of 1999's Article 7 letter (a) on Consumer Protection, which stipulates that one of the responsibilities of corporate actors is to conduct their operations in good faith. Therefore, the agreement between the bank and its customer is regarded as containing a tacit

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

obligation to maintain confidentiality regarding the deposit and its savings, even though it is not expressly regulated and is instead founded on the idea of good faith in carrying out the agreement. Regarding the matter of bank secrecy, even whether it has been governed by a law or an agreement between a bank and its clients, the terms of the relevant legislation must still put the public interest first.

Every bank is required to uphold the principle of confidentiality. One of the efforts that can be made by banks to maintain bank confidentiality is if someone asks about the identity of a customer, or their activities in the bank other than the three authorized parties, namely the Prosecutor's Office, the Police, and the Court, then the bank does not provide any information. The bank will keep it confidential. By making efforts to maintain the security of bank confidentiality, it also indirectly maintains the security of customer finances because bank confidentiality includes protection for customers and their savings.

Several sorts of rules protect consumer data in Indonesian digital banks, specifically Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law of the Republic of Indonesia Number 8 of 2011 concerning Information and Electronic Transactions, Bank Indonesia Regulation Number 9/15/PBI/2007 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks, and the Financial Services Authority Law in the Consumer Protection section. (Azharuddin, 2019). The Republic of Indonesia Law Number 27 of 2022 respecting Personal Data Protection governs the protection of personal information (State Secretariat, 2022). With this law, the personal protection of banking customers will be protected against misuse of customer data.

Banks and other financial service providers are not allowed to give third parties data and/or information about their customers to safeguard them. If the consumer gives a written agreement or if laws and regulations mandate it, information may be shared with third parties. A Financial Services Business Actor

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

must have a written statement confirming that the other party has obtained written consent from the individual or group of individuals to provide the personal data and/or information in question to any party, including the Financial Services Business Actor if the Financial Services Business Actor requests personal data and/or information from another party and plans to use it to carry out its operations.

The form of protection for the confidentiality of customer data as regulated in the Banking Law states that banks are required to maintain the confidentiality of their storage and savings data. Confidentiality protection is also regulated by the financial services authority regulations that banks are required to have risk mitigation, this shows that banks in carrying out services must pay attention to matters relating to external interference such as cybercrime. While customer protection is equated with consumer protection provisions, this can be seen in the Financial Services Authority regulation 1/POJK.07/2013 concerning the protection of financial service consumers.

Banking services in digital form are not free from errors or mistakes that result in data leaks so customer data confidentiality is violated. These errors can cause losses to customers, so a form of bank accountability is needed if losses occur due to these errors or mistakes. Errors occur either intentionally or unintentionally, one of the intentional errors is Fraud and/or cybercrime (a crime that occurs through or on a computer network on the internet) in electronic services from this digitalization in the Financial Services Authority Regulation Number 39 of 2019 defines fraud as follows: Fraud is defined as an intentional act of deviation or omission that is carried out in the Bank's environment and/or while using Bank facilities to deceive, manipulate, or deceive the Bank, customers, or other parties. The goal of fraud is to cause losses for the Bank, customers, or other parties, and/or to provide the perpetrator with direct or indirect financial benefits (Tasman & Ulfanora, 2023).

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

The form of customer data confidentiality protection also indirectly applies to the existence of an agreement (contract) that has been signed by both parties or is bound by civil law. The contractual relationship is both from the application as a customer to the diversion of customer funds to a digital bank that already legally has legal force. Article 1338 of the Civil Code (KUHPerdata) explains that; All agreements made by the law apply as laws for those who make them must be implemented in good faith.

Misuse of customer data that occurs can cause material losses. Losses suffered by customers can sue the bank by taking legal action, this is based on Article 1365 of the Civil Code, namely that every unlawful act that causes losses to others, requires the person whose fault is to issue the loss to compensate for the loss. The return of the value of losses to digital bank customers still refers to the provisions of Article 7 Letter f of Law Number 8 of 1999 which explains that "business actors are obliged to provide compensation, compensation, and/or reimbursement for losses due to the use, use, and utilization of goods and/or services traded". In the elements contained in Article 7 letter f, where consumers who have used digital services in digital banking that result in losses caused by the operational services are not by the traded value or are detrimental, the bank is obliged to provide such compensation.

Legal liability for losses to bank customers can be carried out through civil law for the value of the losses experienced as long as the agreement is not in good faith at the beginning by the parties. Such as the digital wallet service policy regulated through Bank Indonesia Regulation Number 20/6/PBI/2018 concerning Electronic Money, which regulates consumer or customer protection in the implementation of the system. The Bank Indonesia Regulation concerning Consumer Protection contains matters that must be complied with by the Organizer, specifically that the organizer is not allowed to create or include standard clauses, that the organizer must provide a dependable system for payment system service activities, that the organizer must be accountable to

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

customers for any losses resulting from mistakes on the organizer's part, and that the organizer must inform customers about the advantages, risks, and repercussions of using payment system services, The organizer must have and implement a complaint handling mechanism, maintain the confidentiality of consumer data and/or information, provide facilities that make it easy for consumers to obtain information, and conduct socialization and education activities related to the implementation of consumer protection (Utama, 2021).

Based on the aforementioned, the author believes that bank duties for the confidentiality of client data remain the exclusive source of liability; nevertheless, in civil cases, the customer must still make additional steps if there is a serious loss. Compensation can be given by the bank directly only for operational reasons, while the form of responsibility related to losses due to misuse of customer data confidentiality cannot be done directly and has not been regulated, especially because of banking crimes in Banking Regulations, so that other efforts are needed by the customer. These efforts are in the form of filing a civil lawsuit with the District Court (Ida Bagus Putu Sutama., I Gusti Ayu Puspawati., 2013) And it can be proven that the loss occurred not due to the customer's negligence or error (Denisya et al., 2024).

3. The concept of legal protection for digital bank customers in Indonesia as a form of legal certainty

Based on Finder data, Indonesia has huge potential in the digital banking industry. About 47 million adults in Indonesia, or 25% of the population, had digital bank accounts in 2021; by 2026, that figure is predicted to rise to 39%, or roughly 75 million. Given Indonesia's enormous potential for digital bank users, regulations governing consumer legal protection are necessary to ensure legal certainty. For banks, having legal protection is crucial, particularly when conducting business (Sriono et al., 2021).

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Legal protection to provide legal certainty requires regulations or rules that govern it. A regulatory and conceptual approach is required because changes or the creation of regulations are predicated on an incident that demonstrates the shortcomings in their application (Christiani, 2021). Customers of banking in general and digital banking in particular are in a particularly challenging situation because their rights and protection as consumers (services) are frequently violated. Examples include instances of bank money misappropriation, credit card fraud, the trading of private information, including personal identification numbers (PINs), which ought to be kept private, and more. Customers are then protected from the aforementioned unfavorable situations that have happened and are harmful to them; therefore, efforts must be made to address these issues. Repressive protection is protection intended to settle disagreements or issues that come up (Jahri, 2017). Cases or operational risks that can occur in digital banking services such as (Yusuf et al., 2022):

a. The User ID which is the customer's identity is locked because they do not remember the Personal Identification Number (PIN) they created themselves or they do not remember the user's User ID.
b. Password criteria that are difficult and unusual for the general public,
c. Customer errors when entering data due to a lack of information from the bank regarding the correct procedure,
d. Theft of bank data information carried out by internal and external parties,
e. There is no Internet network so customers cannot access transactions online,
f. Virus Or Malware On Bank Systems Which Is Very Vulnerable,
g. Customers do not receive proof of notification from the bank because it was not sent via SMS or email.

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

h. External parties can steal customer User IDs and key codes or passwords,

i. The customer's key code or password and User ID can be accessed illegally by perpetrators of fraudulent acts in the name of the customer,

j. The customer's key code or password and User ID are requested by an external bank by a criminal who is acting on behalf of the Bank,

k. Employees collaborate with criminals to link ATM cards to customer account numbers,

l. Domains used to access bank systems are used by perpetrators of fraudulent crimes.

m. External parties to the bank hijack the existing system in the bank,

n. Customers provide false data with real but fake identities that are submitted to the bank to commit crimes.

In social and economic activities, banking is a type of organization that serves as a middleman between parties in need of finance or financing and those with excess long-term funds (Alwahidin, 2020). The Financial Services Authority of the Republic of Indonesia Number 77 of 2016 regulates risk mitigation, data confidentiality, audit trail records, and security systems as outlined in Articles 21 to 28. This regulation protects the interests of customers in electronic transactions. To raise the caliber of services, organizers can collaborate and share information with IT-based support service providers. It is anticipated that risk mitigation will result in responsible, secure, consumer-protected, and risk-managed digital financial technologies. Implementing the Regulatory Sandbox, a testing platform used by the Financial Services Authority to evaluate the dependability of business processes, business models, financial products, and organizer governance, can help with these efforts. Regarding Digital Financial Innovation in the Financial Services Sector, refer to Article 1 Point 4 of Regulation Number 13/POJK.02/2018 of the Financial Services Authority of

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

the Republic of Indonesia. The Regulatory Sandbox was created as a way to connect regulators and industry participants. This forum will be used by the authorities to identify and monitor the dangers and dynamics of digital financial services. The authorities can decide on mitigation measures to preserve the stability of the financial system after they have a better grasp of the new business model. Fintech enterprises use the Regulatory Sandbox as a sort of testing ground before releasing their goods onto the market. Following their observation in the regulatory sandbox, Fintech companies can be classified into one of three categories. It is advised that all three statuses register with the OJK. To evaluate the dependability of business procedures, business models, financial instruments, and the organizer's governance, the status must then be improved in terms of business model, governance, and transparency. Finally, the status cannot be documented efficiently and sustainably (Sugeng & Fitria, 2020). By preventing or resolving unforeseen situations later on, clients can be protected from the deployment of digital banking services by legislative laws; this protection is referred to as preventive protection (Candrawati, 2014).

Policies in the banking world must be accompanied by providing information to potential users that the current banking system is very stable and more efficient (Ayomi et al., 2021). With the socialization of potential customers' trust will increase to use digital-based banks. But if the opposite is true, it will hurt the development of digital banks in Indonesia. A study conducted by Bank Indonesia shows that no bank in Indonesia can be categorized as a digital native. The majority of digital banking businesses are ad hoc or modified from conventional businesses. This is confirmed by a study conducted by the Financial Services Authority of the Republic of Indonesia in 2021 which evaluated various dimensions of digital banking such as data, technology, risk management, collaboration, institutional arrangements, and customers which gave a value of around 53 on a scale of 0-100 (Ariefianto, 2022). Based on these data, legal

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

protection is needed for digital bank customers, so that customers can feel that their rights are protected (there is protection of customer data confidentiality).

Commercial banks that provide services as Digital Banks, in developing financial ecosystems and/or financial inclusion, must adhere to the guidelines of sound banking management and be implemented carefully. Prospective clients will feel more at ease and have legal assurance if the duty to implement carefully and adhere to the principles of sound banking management is fulfilled. So that potential clients are highly assured and trusting while using the digital bank service to open an account or access financial services.

Providing legal certainty must be the first step in protecting consumer data as part of upholding the right to privacy. Because the Basic Law or Constitution is the highest legal document in a nation, the guarantee of privacy data protection must be enshrined in the document with the greatest authority, which is the Constitution. In the framework of any nation's law enforcement, legal certainty—the legality principle—is essential and cannot be disregarded. By creating and securing these rights in the constitution, the state provides legal certainty. As a result, a nation's priorities, legal system, and governmental structure can all be observed through this document (Natamiharja & Mindoria, 2019).

It is anticipated that the clause in the consumer protection statute that states "all efforts to guarantee legal certainty" will serve as a safeguard against capricious acts that injure business actors solely to protect consumers (Miru & Yodo, 2004). The advantages, fairness, balance, safety, and security of consumers, as well as legal certainty, are the foundations of consumer protection, as stipulated in Article 2 of the Consumer Protection Law. Consumer protection is structured as a collaborative endeavor grounded in pertinent national development principles. For this reason, the state ensures the certainty of the law, and both business actors and consumers follow the law and receive justice in

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

its application. Education, information services, grievances, and the facilitation of dispute resolution for consumers in the financial services industry and the community that uses financial services are all part of consumer protection policies and initiatives. There are 3 (three) obstacles in implementing consumer protection, namely laws or regulations, enforcement or implementing agencies, and the culture of the community itself which does not yet understand or understand the importance of consumer protection (Mashdurohatun et al., 2020).

Customers of digital banks are protected by data confidentiality, and banking business players must establish and put in place a consumer complaint resolution and service mechanism. Banking actors are not allowed to charge fees of any kind to provide services and complaint procedures. For digital service users who are not satisfied with the problems faced, they can use higher regulations, namely the Law on Consumer Protection (Clevalda & Kharisma, 2021). So providing good service by the bank will influence customer confidence in using digital banking services (Hoang, 2018).

Protecting the confidentiality of digital bank customer data requires a regulation that shows legal certainty. In providing legal certainty, a responsive legal regulation is needed. Legal products with a responsive character require something more than just procedural justice but can recognize the desires of the community. To better represent a sense of fairness in society, legal products with a responsive character are those whose character reflects the satisfaction of the demands of individuals and diverse social groups in society (Sanusi et al., 2020).

The implementation of customer data confidentiality protection can be carried out with a responsive legal concept, this is necessary to provide a sense of justice and comfort for customer deposits. The regulation of customer data confidentiality in banking laws is still general and has not been explicitly regulated about material losses so other regulations are needed so that customer rights can

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

be protected. In providing customer protection, banks are equated with consumers. So customer protection also applies to the provisions as regulated in consumer protection regulations. Likewise, the use of digital banking applications/services (electronically) regarding customer protection is bound by the Law on Information and Electronic Transactions (Law Number 11 of 2008). As regulated in Article 38 of the ITE Law, it states that: (1) Everyone who uses electronic devices or information technology has the right to file a compensation claim. (2) Members of the public can file a lawsuit on behalf of electronic network operators or people who use technology in a way that has a detrimental impact on the community by statutory regulations.

Based on the descriptions above, it can be seen that providing legal protection for the confidentiality of customer data for users of the Digital bank, can be done responsively, namely if customer rights are not fulfilled, it can be done by connecting other relevant regulations so that customers who are harmed can fulfill their sense of justice. Fulfilling the sense of justice for customer protection, especially data confidentiality, requires a role for law enforcers in this case, court judges if it is not regulated in banking regulations. As regulated in the Civil Code, the Consumer Protection Law, and the Electronic Information and Transactions Law, those who are harmed can file a lawsuit or lawsuit in court.

Based on the above, the author argues that in protecting the confidentiality of digital bank customer data, customers and banks must have better knowledge of the risks they will face. The provisions governing banking do not fully regulate protection against losses due to leaks of customer data confidentiality. Leaks of customer data are not always due to deliberate actions by the bank, but can also occur unintentionally, such as cybercrime. So that the losses experienced by customers need to be accounted for by the bank. As stipulated in the financial services authority regulations, banks must have risk management so that if cybercrime occurs, the bank can be sued civilly for the losses experienced by customers.

Available online at: https://journal.unpas.ac.id/index.php/litigasi

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

IV. CONCLUSIONS AND SUGGESTIONS

A. Conclusions

Based on the description and discussion that has been carried out, it can be concluded that:

1. The regulations relating to banking responsibilities regarding the confidentiality of bank data in Indonesia are regulated by several regulations, including Law Number 10 of 1999, Law Number 27 of 2022 concerning personal data protection, Law Number 8 of 1999 concerning Consumer Protection, Bank Indonesia Regulation Number 9/15/PBI/2007 concerning the Implementation of Risk Management in the Use of Information Technology by Commercial Banks. The regulation on protecting the confidentiality of customer data based on the regulation is not absolute, because in certain circumstances such as indications of criminal acts, banks are allowed to provide customer data to law enforcement.

2. The form of legal protection for the confidentiality of customer data provided by banks is currently still not comprehensive because the form of protection for the confidentiality of customer data provided is still in the form of a prohibition on providing information to other parties without permission (except for legal purposes), while legal protection for the confidentiality of customer data against cybercrimes that can result in material losses for customers has not been regulated clearly and firmly, only subject to and bound by agreements or agreements made between the bank and the customer and requires other efforts by filing a civil lawsuit with the District Court.

3. The concept of legal protection for the confidentiality of digital bank customer data in Indonesia in providing legal certainty can be done responsively. The implementation of providing responsive protection is carried out by using or connecting other regulations outside the regulations governing banking if customer rights are not fulfilled in banking regulations such as material losses caused by cybercrime.

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

B. Suggestions

Based on the results of the analysis that has been carried out, the following suggestions are needed:

1. Strong supervision is needed by authorized institutions (internal or financial services authorities) regarding the implementation of providing confidentiality of customer data to other parties because providing confidentiality of customer data will increase customer trust in using digital banking services in Indonesia and can result in material losses for customers;

2. As a form of legal protection in maintaining confidentiality, the Bank should provide information to customers regarding the provision of customer information to other parties when signing the contract agreement;

3. The formulation of regulations on the legal protection of customer data confidentiality in banking regulations is urgently needed so that they are no longer linked to other regulations or are special.

REFERENCES

Adiningsih, S. (2019). *Transformasi Ekonomi Berbasis Digital di Indonesia*. Gramedia Pustaka Utama, Jakarta.

Ahmad, H., Anggraini, S., & Iswahyudi, G. (2022). Perlindungan Hukum Terhadap Keamanan Rahasia Bank dalam Menjaga Kepentingan Nasabah Perbankan. *AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam*, *4*(2), 337–350. https://doi.org/10.37680/almanhaj.v4i2.1800

Alwahidin. (2020). Kejahatan Kerah Putih Dalam Industri Perbankan. In Sumitro, B. A. Pramuka, & N. Lukviarman (Eds.), *Perbankan (Hasil Pemikiran Para Dosen)* (cetakan 1, pp. 26–44). Sihsawit.

Ariefianto, D. (2022). *Gambaran Bank Digital dan Tantangan di Indonesia*. https://www.cnbcindonesia.com/opini/20220629140704-14-351414/gambaran-bank-digital-dan-tantangan-di-indonesia

Ayomi, S., Sofilda, E., Hamzah, M. Z., & Ginting, A. M. (2021). The impact of monetary policy and bank competition on banking industry risk: A default analysis. *Banks and Bank Systems*, *16*(1), 205–215. https://doi.org/10.21511/bbs.16(1).2021.18

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Ayu, M. G. (2021). *Bank Indonesia: Digitalisasi Menjadi Kunci Pendukung Pemulihan Ekonomi*. https://www.cloudcomputing.id/acara/bank-indonesia-digitalisasi-kunci-pemulihan-ekonomi

Azharuddin. (2019). Legal Protection For User Of Internet Banking Customers Following Changes In Information And Electronic Transaction Law. In *Jurnal Pembaharuan Hukum* (Vol. 6, Issue 1). https://doi.org/10.26532/jph.v6i1.4674

Candrawati, N. N. A. (2014). Perlindungan Hukum Terhadap Pemegang Kartu E-Money Sebagai Alat Pembayaran Dalam Transaksi Komersial. *Jurnal Magister Hukum Udayana (Udayana Master Law Journal)*, *3*(1), 1--16. https://doi.org/10.24843/JMHU.2014.v03.i01.p03

Christiani, T. A. (2021). Proposed changes to the Bank Indonesia law as a solution to the impact of the COVID-19 spread on banking in Indonesia. *Banks and Bank Systems*, *16*(2), 127–136. https://doi.org/10.21511/bbs.16(2).2021.12

Christiawan, R. (2021). *Tantangan Hukum Bank Digital*. Https://Www.Hukumonline.Com/Berita/a/Tantangan-Hukum-Bank-Digital-Lt61308a5a9a319?Page=2 Retrieved November 20, 2022.

Clevalda, D. K., & Kharisma, D. B. (2021). Perlindungan Hukum Terhadap Nasabah Dompet Digital Oleh Bank Indonesia. *Privat Law*, *9*(1), 1–9. https://doi.org/10.20961/privat.v9i1.41483

Cvijovic, J., Stankovic, M. K., & Marija, R. (2017). Customer Relationship Management In Banking Industry: Modern Approach. *Industrija Journal, 45*(3), 151–165.

Denisya, N. P., Budiartha, I. N. P., & Putra, I. M. A. M. (2024). Perlindungan Hukum Terhadap Data Pribadi Nasabah Oleh Bank Dalam Transaksi Melalui Internet Banking. *Jurnal Preferensi Hukum*, *5*(2), 246–252. https://doi.org/10.22225/jph.5.2.8088.246-252

Djumhana, M. (1996). *Rahasia Bank (Ketentuan Dan Penerapannya di Indonesia)*. PT. Citra Aditya, Bakti, Bandung.

Edu, H. (2021). *Menjawab Kepastian Keamanan Data Nasabah Bank Digital, OJK Keluarkan POJK 12 /POJK.03/2021*. https://heylawedu.id/blog/keamanan-data-nasabah-bank-digital

Hadjon, P. M. (2011). *Pengantar Hukum Administrasi Indonesia,* (p. 10). Gajah Mada University Press, Yogyakarta.

Hartono, B., & Atmaja, H. E. (2021). SDM Digital : Strategi Tranformasi Bank Menjadi Bank Digital. *Jurnal Administrasi Kantor*, *9*(1), 49–60.

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

https://doi.org/10.51211/jak.v9i1.1481

Hoang, T. P. (2018). Factors affecting service quality at Vietnamese retail banks. *Banks and Bank Systems*, *13*(2), 39–48. https://doi.org/10.21511/bbs.13(2).2018.04

Ida Bagus Putu Sutama., I Gusti Ayu Puspawati., D. (2013). Kerahasiaan Bank Sebagai Wujud Perlindungan Hukum Terhadap Nasabah Penyimpan Dana Dikaitkan Dengan Money Laundering. *Kertha Negara*, *1*(1), 3. https://ojs.unud.ac.id/index.php/Kerthanegara/article/view/4780/3590

Jahri, A. (2017). Perlindungan Nasabah Debitur Terhadap Perjanjian Baku Yang Mengandung Klausula Eksonerasi Pada Bank Umum Di Bandarlampung. *FIAT JUSTISIA:Jurnal Ilmu Hukum*, *10*(1), 125–148. https://doi.org/10.25041/fiatjustisia.v10no1.651

Kansil, C. S. T. (1989). *Pengantar Ilmu Hukum dan Tata Hukum Indonesia*. Balai Pustaka, Jakarta.

Kholis, N. (2020). Perbankan Dalam Era Baru Digital. *Economicus*, *12*(1), 80–88. https://doi.org/10.47860/economicus.v12i1.149

Marlina, A., & Bimo, W. A. (2018). Digitalisasasi Bank Terhadap Peningkatan Pelayanan Dan Kepuasan Nasabah Bank. *Innovator*, *7*(1), 14. https://doi.org/10.32832/inovator.v7i1.1458

Mashdurohatun, A., Lestari, F., & Tukinah, U. (2020). Consumer protection of the listing of standard clauses in e-commerce transactions based on the value of Pancasila justice. *International Journal of Advanced Science and Technology*, *29*(6), 1520–1531.

Miru, A. dan, & Yodo, S. (2004). *Hukum Perlindungan Konsumen*. PT. Raja Grafindo Persada, Jakarta.

Natamiharja, R., & Mindoria, S. (2019). Perlindungan Data Privasi dalam Konstitusi Negara Anggota ASEAN. In *Hak Konstitusional: Tebaran Pemikiran dan Gagasan*.

OJK. (2013). *Regulation of the Financial Services Authority of the Republic of Indonesia Number 1/POJK.07/2013 concerning protection for consumers of financial services*.

OJK. (2018). *Republic of Indonesia Financial Authority Services Regulation No. 12/PJOK.03/2018 concerning the Implementation of Digital Banking Services by Commercial Banks*.

Pakpahan, E. F., Chandra, L. R., & Dewa, A. A. (2020). Perlindungan Hukum Terhadap Data Pribadi Dalam Industri Financial Technology. *Veritas et*

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Justitia, *6*(2), 298–323. https://doi.org/10.25123/vej.3778

Rahardjo, S. (2000). *Ilmu Hukum*. PT. Citra Aditya Bakti, Bandung.

Rhoen, M. (2016). Beyond consent : improving data protection through consumer protection law. *Internet Policy Review*, *5*(1), 1–15. https://doi.org/10.14763/2016.1.404

Riswandi, B. A. (2005). *Aspek Hukum Internet Banking*. PT. Raja Grafindo Persada, Jakarta.

Rossana, G. (2016). Penafsiran Pasal 40 Undang-Undang Nomor 10 Tahun 1998 Mengenai Kerahasiaan Bank. *LamLaj*, *1*(2), 121.

Sanusi, S., Idayanti, S., & Widyastuti, T. V. (2020). Demokratisasi dalam Rangka Pembangunan Hukum Responsif. *Diktum: Jurnal Ilmu Hukum*, *8*(2), 182–191. https://doi.org/10.24905/diktum.v8i2.84

Setneg. (1999). *Law of the Republic of Indonesia Number 8 of 1999 concerning Consumer Protection*.

Setneg. (2022). *Law of the Republic of Indonesia Number 27 of 2022 concerning the Protection of Personal Data*.

Sidabalok, J. (2014). *Hukum Perlindungan Konsumen di Indonesia*. PT Citra Aditya Bhakti, Bandung.

Sriono, Kusno, Sagala, E., Risdalina, & Tampubolon, W. S. (2021). Dissenters vs debtors bank promise: A review of normative juridical. *Journal of Legal, Ethical and Regulatory Issues*, *24*(Special Issue 1), 1–11.

Sugeng, & Fitria, A. (2020). Aspek Hukum Digital Lending Di Indonesia. *Jurnal Legalisasi Indonesia*, *17*(4), 437–450.

Susilo, Y. S., Triandaru, S., & Santoso, A. T. B. (2006). *Bank dan Lembaga Keuangan Lain*. Salemba Empat.

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia*, *1*(3), 294–307. https://doi.org/10.14710/jphi.v1i3.294-307

Tasman, & Ulfanora. (2023). Perlindungan Hukum Terhadap Nasabah Bank Digital. *Unes Law Review*, *6*(1), 1624–1635. https://doi.org/https://doi.org/10.31933/unesrev.v6i1

Utama, A. S. (2021). Digitalisasi Bank Konvensional dan Bank Syariah Di Indonesia. *Jurnal Ilmu Hukum Perundang-Undangan Dan Pranata Sosial*, *6*(2), 113–126.

Jurnal LITIGASI, Vol. 25 (2) October, 2024, p. 301-330
dx.doi.org/10.23969/litigasi.v25i2. 18538

Winasis, S., & Riyanto, S. (2020). Transformasi Digital di Industri Perbankan Indonesia: Impak pada Stress Kerja Karyawan. *IQTISHADIA: Jurnal Ekonomi Dan Perbankan Syariah*, *7*(1), 55–64. https://doi.org/10.1905/iqtishadia.v7i1.3162

Yusuf, M., Sumarno, & Komarudin, P. (2022). Bank Digital Syariah Di Indonesia : Telaah Regulasi Dan Perlindungan Nasabah. *Jurnal Ekonomi Islam*, *13*(2), 2579–6453.

Zaini, Z. D. (2018). Analisis Yurisdis Perlindungan Hukum Nasabah Bank terhadap Kerahasiaan Bank di Indonesia. *Recital Review*, *1*(1), 32–49. https://doi.org/10.22437/rr.v1i1.6066