

Legal Protection for Depositor Customers in Digital Banks Against Cyber Crimes in the Banking Sector

Agita Justisia Br. Tarigan¹, I Gusti Agung Mas Rwa Jayantiari²

¹ Master of Law, Udayana University, Denpasar, Bali, Indonesia and agitajt@gmail.com

² Master of Law, Udayana University, Denpasar, Bali, Indonesia and mas_jayantiari@unud.ac.id

ABSTRACT

The full use of technology in running a digital bank makes things easier for customers but is vulnerable to cybercrime in the banking sector which can harm customers. This research places the main focus on forms of legal protection efforts for customers who deposit at digital banks against the occurrence of cybercrime in the banking sector. Legal problems, namely regarding the legal relationship between deposit customers and digital banks in banking sector cyber crime issues as well as legal protection efforts for deposit customers in digital banks in banking sector cyber crime issues. The type of research applied is normative legal research using statutory, conceptual and analytical approaches to examine the problems discussed. The research results show that the legal relationship between digital banks and customers who deposit funds is a relationship of trust (fiduciary relationship) contained in the funds deposit agreement. Legal protection for deposit customers in cases of cyber crime includes: 1) Preventive legal protection in the form of preventing losses for deposit customers in accordance with the provisions of the Banking Law, POJK Number 12/POJK.03/2018, as well as related legal instruments; and 2) Repressive legal protection in the form of dispute resolution efforts which can be implemented in 2 (two) ways, namely Non-Litigation and Litigation dispute resolution. Efforts to resolve non-litigation disputes, namely: 1) Making a complaint to PUJK; 2) Make a complaint to the OJK. Meanwhile, the litigation effort is to file a civil lawsuit.

Keywords: Cyber Crime, Deposit Customers, Digital Ban, Legal Protection.

1. INTRODUCTION

The advancement of technology has had an impact on the development of various sectors of society worldwide. The influence of technological progress has significantly affected the economic sector, which is crucial for people's lives. In Indonesia, the government has been actively promoting technological advancements in the economic sector. Regarding this matter, the government must take proactive initiatives to properly structure the realization of the digital economy through an effective legal framework that ensures balance for all parties. According to the paradigm of Indonesia's constitutional economy, the state must be responsive to technological developments to advance the national economy. This means that if the state does not adopt a progressive approach in decision-making, economic digitalization will become increasingly unregulated and difficult to control through legal legitimacy [1].

The government has implemented various innovations to accelerate economic digitalization, such as launching the QRIS payment system as the official QR Code from Bank Indonesia [2]. Additionally, digitalization has been applied to financial institutions, including Financial Technology, commonly known as Online Loans, which still face issues regarding legality and debt collection practices that often involve unlawful and violent methods [3]. Another innovation in the financial sector is the creation of e-Wallets or digital wallets, such as Dana, OVO, Flip, ShopeePay, Gopay, and others, which are frequently used by millennials for transactions due to lower administrative fees compared to conventional bank transactions. This trend is also accompanied by the digitalization of banking institutions through the establishment of Digital Banks [4], [5].

A digital bank is a banking institution that provides digital banking services. The emergence of digital banks necessitates the creation of regulations to govern their operations in Indonesia. Many digital banks have been established in the country, such as SeaBank and others. Therefore, the government must promptly update the Banking Law by enacting Law No. 4 of 2023 on the Development and Strengthening of the Financial Sector, which includes provisions on economic digitalization, particularly regarding Digital Banks [6].

Furthermore, a specific regulation governing digital banking services has been established through Financial Services Authority Regulation (POJK) No. 12/POJK.03/2018 on the Implementation of Digital Banking Services by Commercial Banks. Article 1, point 4 of this regulation defines Digital Banking Services as "Electronic Banking Services developed by optimizing customer data utilization to serve customers more quickly, conveniently, and in accordance with their needs (customer experience), allowing customers to conduct transactions independently while ensuring security aspects are maintained." The regulation also defines Electronic Banking Services as services designed for users (customers) to access information, interact, and conduct banking transactions using electronic platforms. Article 10, paragraph (1) of POJK No. 12/POJK.03/2018 states: "The Digital Banking Services provided by banks, as referred to in Article 8, paragraph (1), letter a, include: (a) account administration; (b) transaction authorization; (c) financial management; and/or (d) other financial product services as approved by the Financial Services Authority" [7]. These regulations indicate that digital banks focus on meeting customer needs through the full use of digital technology, employing both hardware and software as service delivery channels. The sophistication of digital banking services allows customers to access them anytime and anywhere. Additionally, the full implementation of digital technology minimizes direct interactions between customers and bank employees. The ease of accessing digital banking services supports more efficient operational activities and service quality [8], [9].

While the full use of technology in digital banking provides convenience for customers, it also poses risks that may harm them. Cybercrime in the banking sector has become a significant threat to digital bank customers. The banking sector is highly vulnerable to cyberattacks such as skimming, hacking, and malware. These crimes primarily affect customers who conduct transactions or use other financial services via the internet. In addition to digital banking crimes, traditional banking fraud also poses risks to digital bank customer [10].

Several previous studies have explored digital banking, including research by Denis Megel Putra, titled "Legal Protection for Customers in Digital Banking," which examines a Sharia financing application in relation to the legal framework governing digital banks and consumer protection efforts under the Consumer Protection Law. This study highlights the state-of-the-art aspect where the researcher provides a detailed explanation of digital banking regulations in Indonesia and customer protection efforts based on the Consumer Protection Law [11], [12]. Another study conducted by Michelle Jefelyn Hardinata and colleagues, titled "Dissemination of Digital Banking Policies: Legal Protection of Customer Data from Cyberattack Risks," discusses regulations on digital banks and the threat of cyberattacks, particularly in Samarinda. The state-of-the-art aspect of this study lies in its discussion of real-life cases of cybercrime affecting digital bank customers.

Based on previous research, this article formulates two main research questions: (1) What is the legal relationship between deposit customers and digital banks concerning cybercrime in the banking sector? (2) What are the legal protection measures for deposit customers in digital banks

against cybercrime in the banking sector? To address the key issue of deposit customer protection in digital banking, which has been identified through these research questions, this article will conduct an in-depth and detailed analysis of the legal protection issues faced by digital bank customers, who are highly vulnerable to digital banking crimes. The analysis will be based on the Indonesian Civil Code (KUHPPerdata) and other relevant legal provisions concerning this issue.

2. METHODS

This journal article applies normative legal research, which involves studying and analyzing written sources or secondary information. Therefore, it is often referred to as library research or theoretical/dogmatic legal research. As a result, the sources examined in normative legal research consist of written materials or secondary information [13]. The researcher focuses on analyzing legal protection for depositors in digital banks due to cybercrime in the banking sector. To analyze and discuss this research topic, the study employs various legal instruments, including regulations and laws governing legal protection for depositors in banks, as well as expert opinions from civil law scholars relevant to the research theme.

The researcher utilizes three types of approaches: the statute approach, the conceptual approach, and the analytical approach. This study relies on primary legal materials, including the Civil Code and other legal provisions related to the research topic. Additionally, secondary legal sources such as books on banking law, cybersecurity law, and relevant academic journals or scientific papers are used. To support the research, tertiary legal sources, including dictionaries and other legal references related to the journal's topic, are also utilized. The research method involves document studies by analyzing various legal documents. Once the legal materials are collected, they will be examined using a qualitative descriptive analysis method. Therefore, all legal findings will be presented and analyzed through discussion, review, and data processing to be structured into information that is understandable for readers.

3. RESULTS AND DISCUSSION

3.1 Legal Relationship Between Depositor Customers and Digital Banks in Cybercrime Issues in the Banking Sector

A legal relationship (*rechtsbetrekkingen*) is a relationship formed between two or more parties that hold legal subject status, which may include individuals, communities, or other legal entities. Essentially, the interaction between these legal subjects results in rights and obligations that vary for each involved party. A legal relationship also exists between depositor customers and digital banks [14]. Law No. 10 of 1998, which amends Law No. 7 of 1992 on Banking (the Banking Law), defines a customer as a party utilizing banking services. Under the Banking Law, customers are categorized into Depositor Customers and Debtor Customers [15]. According to these provisions, a Depositor Customer is defined as a customer who deposits funds in a bank under an agreement between the bank and the customer. Meanwhile, a Debtor Customer is a customer who utilizes credit or financing services based on either Islamic banking principles or their conventional equivalent, also established through an agreement involving both the bank and the customer.

Furthermore, Article 1, Clause 2 of the Banking Law states: "A bank is a business entity that collects funds from the public in the form of deposits and distributes them to the public in the form of credit and/or other forms in order to improve the living standards of the people." Banks are also classified into Commercial Banks and Rural Banks (previously known as People's Credit Banks). Over time, commercial banks have been permitted to provide digital banking services, commonly referred to as Digital Banks. This is stipulated in Article 4 of the Financial Services Authority Regulation (POJK) No. 12/POJK.03/2018, which mandates that banks offering Electronic Banking Services must be classified as Commercial Banks in accordance with Financial Services Authority

(OJK) regulations governing their business activities. Digital Banking Services are facilities within the banking sector that utilize electronic systems to optimize customer information, enabling faster, more convenient, and customer-oriented banking services. Digital banking services are specifically designed for customers to independently access banking services while still being protected by the bank's security measures. Digital banking services offered by Digital Banks include:

1. Account Administration

Account administration services include account creation, customer information updates, and account closure, all conducted through electronic media.

2. Transaction Authorization

Transaction authorization services provide facilities for both financial and non-financial transactions.

3. Financial Management

Financial management services are among the financial facilities provided by banks to help customers analyze and plan their funds according to their needs, allowing them to make wise financial decisions. These services include financial planning, financial transactions, and financial advisory related to banking services. One example of financial management services is a bank's offer to help customers manage and plan their savings according to their financial goals, such as structured savings plans. Through this service, the bank assesses the customer's financial situation and recommends relevant financial products via its banking application. If the customer is interested, they can apply for the desired product directly through the application, following a tailored authorization process. Additionally, the bank provides periodic reports and notifications to ensure customers maximize the benefits of the products they have chosen.

4. Other Financial Services Approved by the OJK

Based on the services provided by digital banks, financial management services are the services used by deposit customers. As previously explained, a deposit customer is an individual who entrusts their funds to a bank in accordance with an agreement between both parties. The funds deposited by customers are referred to as deposits, which are funds entrusted to the bank according to the terms of a deposit agreement, such as savings accounts or their equivalents. The previously described fund deposit process is similar to the financial management services provided by digital banks, as outlined above. Thus, it is evident that conventional and digital banks share similarities in providing services to deposit customers, although there are differences in the operational and implementation methods.

Fundamentally, there is a legal relationship between the bank and the deposit customer, based on the customer's trust in the bank, known as a fiduciary relationship. In this context, the bank acts as the entity that receives and holds public funds based on the trust of the public in conducting its banking business activities. Due to this public trust, every bank is required to maintain financial stability while simultaneously preserving public confidence. However, a customer's trust in the bank is still based on an agreement or contract. Therefore, it can be stated that, aside from a customer's trust in the bank regarding their deposits, the legal relationship between the bank and the customer is also based on a contract or agreement [16].

When a customer enters into an agreement with a bank, it creates a binding relationship based on a contract. However, if one examines the provisions of the Civil Code (KUH Perdata) and the Commercial Code (KUH Dagang), there is no specific regulation governing the contractual

relationship between a bank and a deposit customer in the form of a deposit agreement. Additionally, there is no clear explanation of the contractual legal relationship between these two parties. Nevertheless, if the established legal relationship is a contractual relationship in the form of a deposit agreement, then the deposit agreement must adhere to the Civil Code, which governs binding agreements. Article 1319 of the Civil Code states: "All agreements, whether specifically named or not recognized by a particular name, are subject to the general provisions contained in this chapter and other chapters." [17] This legal provision indicates that, as a type of agreement, a deposit agreement must refer to the Civil Code. Therefore, it is understood that a deposit agreement cannot be equated with other types of agreements. Additionally, it differs from interest-bearing loan agreements because the bank is not a borrower, the deposit customer is not a lender or creditor, and they do not act as mere custodians of funds at the bank.

Depositing funds is a facility provided by banks that is widely used by the public, including digital savings accounts, digital deposits, digital wallets, and many other services. When using these services, customers or users act as depositors, while service providers act as recipients and managers of the entrusted funds. As the party responsible for managing depositors' funds, service providers must avoid actions that could harm depositors, such as unauthorized electronic transactions in e-commerce, QRIS-based payments, or other electronic payments made from depositors' accounts.

The trust of deposit customers in banks forms the basis for placing their funds in a bank. The deposited funds become the bank's assets, giving the bank full rights to utilize these funds in its banking operations without needing prior approval from the deposit customer. In this context, the bank is obliged to return the customer's deposit in the agreed amount along with any agreed-upon compensation [18].

The operation of digital banks, in addition to being related to Banking Law and Civil Law, is also linked to Information Technology Law or Cyber Law, as outlined in the Electronic Information and Transactions Law (UU ITE). This is because the entire business operation of a digital bank relies on electronic systems. Under the UU ITE, the bank functions as an electronic system provider, commonly referred to as a digital bank. Article 1, point 6a of Law No. 19 of 2016 states: "An Electronic System Provider is any individual, government entity, business entity, or community organization that provides, manages, and/or operates an Electronic System, either independently or jointly, for its own purposes and/or for the purposes of other parties."

As previously explained, the relationship between a deposit customer and a digital bank is considered a contractual relationship. Once a customer enters into an agreement with the bank, the relationship established is based on a contract. The contract between the customer and the digital bank is an electronic contract. The UU ITE regulates this in Article 1, point 16, which states: "An Electronic Contract is an agreement between parties made through an Electronic System." Therefore, the electronic contract formed between deposit customers and digital banks is directly related to the customers' deposited funds.

Regulations concerning electronic contracts (e-contracts) are further detailed in Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions [19]. An electronic transaction is a type of transaction that can be conducted based on an electronic contract or other contractual forms that establish a legally binding agreement between the parties. The conditions for an electronic contract to be considered valid are fundamentally similar to the validity requirements of agreements under Article 1320 of the Civil Code, which include:

1. The emergence of an agreement between the parties;
2. Execution by legal subjects with the capacity and authority to act on their behalf or for related parties in accordance with applicable legal regulations;
3. The presence of a clear object;
4. The transaction object must align with legal regulations, moral values, and public order, and must not contradict any of these principles.

An electronic contract is categorized as an "unnamed contract," meaning it is a type of agreement not specifically regulated in the Civil Code but widely used in society due to advancements in technology and business needs. Contracts conducted over the internet generally adhere to contract law principles as determined by civil law. However, there are key differences: electronic contracts are highly specific and heavily influenced by digital media and electronic devices [20].

Essentially, an electronic contract is similar to a conventional contract in that it carries the same legal force as a law for the parties involved (Article 1338 of the Civil Code). Contracts formed in electronic commerce transactions are considered valid as long as their contents comply with the provisions of the Civil Code. Although an electronic contract is a non-written contract, this does not automatically render it legally invalid. This is because the Civil Code does not require a contract to be in written form to be legally binding. With the increasing prevalence of electronic commercial transactions using electronic contracts, business transaction practices should adapt to technological advancements, including the use of electronic contracts in electronic transactions. Since electronic contracts are becoming widely used in business, they are considered legally valid [21].

All provisions in Chapter III of the UU ITE serve as the foundation for establishing legal relationships between prospective deposit customers and digital banks. At the initial stage of this legal relationship, there is usually an offer process to the other party. In this context, digital banks offer deposit services in the form of savings or deposits to prospective deposit customers. Once the information exchange process has been conducted properly and is legally recognized, it can proceed to the formation of a deposit agreement, which is then formalized through an electronic contract.

3.2 Legal Protection Efforts for Depositor Customers in Digital Banks Against Cybercrime in the Banking Sector

Efforts to strengthen and regulate the legal protection concept for depositor customers who fall victim to cybercrime in the banking sector must first consider the types of losses suffered by these customers. These losses are not limited to material or physical damages but also include immaterial or psychological harm. In addition to legal or juridical protection efforts, customer protection can also be accompanied by non-juridical measures aimed at preventing such losses from occurring [22].

Fundamentally, there are two forms of direct legal protection for individuals who have suffered harm or become victims of crime: preventive legal protection, which seeks to avoid the possibility of becoming a victim (essentially a form of human rights protection or legal interest protection), and repressive legal protection, which ensures compensation for losses suffered due to criminal acts. Preventive protection is related to actions taken by individuals and whether those actions pose risks and how to mitigate them. Meanwhile, repressive legal protection includes cases where a bank customer entrusts their funds to the bank in a personal account, granting them the right to protection regarding the security and confidentiality of their personal data and savings amount, as agreed by all parties. If a crime such as account hacking occurs, affecting the funds deposited in a bank, the depositor has the right to seek compensation or assurances regarding the confidentiality of their data [23].

Legal protection guarantees are crucial for depositors in light of the rising cybercrime cases in the banking sector. Cybercriminals employ various methods and techniques. In digital banking, multiple forms of cybercrime cause losses, particularly to depositors, including [24]:

1. Card Skimming

A crime involving the unauthorized copying of data from an ATM or debit card's magnetic strip to steal sensitive information. This strip contains essential customer details, such as the card number, expiration date, and cardholder name.

2. Phishing

An attempt to deceive computer users into providing confidential information through fraudulent messages, such as emails, websites, or other electronic communications.

3. Carding

The unauthorized use of stolen debit or credit card data for online transactions. This crime is relatively easy to commit as it does not require a physical card, only the card's details.

Beyond these cybercrime tactics, other methods include unauthorized data or software modifications, such as altering program instructions to prevent the program from performing its intended functions (Trojan Horse). Another example is Data Diddling, where legitimate data is unlawfully modified, altering input or output information. In the banking sector, these crimes may involve manipulating banking software to divert interest payments from customer accounts to unauthorized accounts. Additionally, cybercriminals may embezzle or reduce customers' deposited funds and transfer them to private accounts [1].

Given that digital banking relies entirely on electronic information systems, it is highly vulnerable to such cybercrimes. These crimes can severely harm depositors who have entrusted their funds to a digital bank for safekeeping and management. Therefore, depositors must be provided with legal protection regarding their rights over the funds entrusted to digital banks.

POJK No.12/POJK.03/2018 Article 21(1) states: *"Banks providing Electronic Banking Services or Digital Banking Services must implement consumer protection principles as stipulated in financial service consumer protection regulations."*

Additionally, POJK No.6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector defines [25]:

1. Financial Service Providers (PUJK) as institutions or entities engaged in fund collection, fund distribution, and/or fund management in the financial services sector.
2. Consumers as individuals who place funds and/or use services offered by financial institutions, including banking customers, capital market investors, insurance policyholders, and pension fund participants, based on financial service regulations.

Based on these regulations, digital banks act as Financial Service Providers (PUJK), while depositors are classified as consumers. As a PUJK, digital banks are obligated to ensure legal certainty for their customers by protecting their rights and obligations as consumers in the financial services sector. Following these legal provisions, digital banks must implement preventive legal protection measures to safeguard customers from potential losses due to cybercrime in the banking sector. Preventive customer protection is generally regulated under banking laws, including [12]:

1. Law No.10 of 1998 on Banking

The provisions in the Banking Law also include regulations regarding legal protection provided to customers concerning digital banking services, which include [1]:

- a. Providing information to customers regarding the potential risks associated with digital banking services. This ensures that customers can easily access and gather information about commercial activities and banking conditions while ensuring transparency in the banking sector (Article 29 paragraph (4) of the Banking Law);
- b. Enhancing banking security to strengthen public trust by ensuring that personal data of digital banking users, deposit information, and customer financial position data cannot be misused (Article 40 of the Banking Law); and
- c. Guaranteeing customer deposits by establishing a Deposit Insurance Corporation and receiving funds from digital banking customers stored in banks (Article 37B of the Banking Law).

2. POJK No. 6/POJK.07/2022 on Consumer and Public Protection in the Financial Services Sector

The provisions in Articles 4-38 of POJK No. 6/POJK.07/2022 also cover preventive legal protection efforts for customers, including:

- a. Banks, as Financial Services Business Actors (PUJK), are required to conduct their business in good faith and are not allowed to provide discriminatory services to customers;
- b. Banks must establish and implement written policies and procedures related to consumer protection efforts. Additionally, banks are required to implement the Consumer and Public Protection Code of Ethics;
- c. Banks are prohibited from distributing and misusing customers' personal data;
- d. Banks must conduct trials for newly developed products and services to prevent potential losses for customers;
- e. Banks are required to inform prospective customers about the products and services offered before they decide to place their money in the bank and/or use the services provided;
- f. Banks are prohibited from offering products and services that could harm potential customers;
- g. Banks must inform consumers about funds, assets, or liabilities based on agreements between PUJK and consumers.

3. POJK No.12/POJK.03/2018 on the Implementation of Digital Banking Services by Commercial Banks

Specifically, regarding preventive legal protection for digital bank customers, it has been explicitly stipulated in POJK No.12/POJK.03/2018. This regulation mandates that banks offering digital banking facilities must implement consumer protection principles in the financial services sector. Additionally, digital banking service providers must perform their duties by handling customer inquiries and/or complaints 24 hours a day. This customer protection is carried out based on principles of transparency, fairness, security, privacy, and reliability of customer information, while dispute resolution must be conducted efficiently [12].

In addition to preventive legal protection, there is also repressive legal protection aimed at safeguarding customers through dispute resolution. In the event of a dispute, the available resolution methods include Non-Litigation and Litigation dispute resolution. Non-litigation dispute resolution involves negotiation (deliberation), mediation, arbitration, and conciliation. Meanwhile, litigation dispute resolution refers to resolving disputes through the judicial system [26].

1. Non-Litigation Dispute Resolution Efforts

Repressive legal protection categorized as non-litigation dispute resolution is stipulated in Article 36 of POJK No.6/POJK.07/2022, which requires Financial Service Providers (PUJK) to ensure the security of funds and/or assets entrusted by consumers. If customers, as consumers, seek accountability from the bank as a PUJK, they can do so through the procedures outlined in POJK No.6/POJK.07/2022, namely:

A. Filing a Complaint with the Financial Service Provider (PUJK)

Complaints to PUJK are regulated in Article 6 of POJK No.6/POJK.07/2022, which mandates that PUJK must establish and implement written policies and procedures related to consumer protection. The provisions regarding consumer complaint services to PUJK are further detailed in POJK No.6/POJK.07/2022. If the consumer complaint facilities provided by PUJK fail to yield satisfactory results, consumers are allowed to

pursue resolution through legal channels or alternative dispute resolution mechanisms in the Financial Services Sector.

B. Filing a Complaint with the Financial Services Authority (OJK)

In addition to the complaint services provided by PUJK, consumers are also permitted to utilize complaint services facilitated by OJK in accordance with Article 51 of POJK No.6/POJK.07/2022. This service provision follows POJK No.31/POJK.07/2020. The OJK service aims to provide consumers and the public with an avenue for addressing complaints related to financial services, ensuring better consumer protection. OJK accommodates consumer demands at several stages, including:

- 1) Complaint Indicating a Dispute (Articles 10 - 18 of POJK No.31/POJK.07/2020)
At this stage, consumers or their representatives may file a Complaint Indicating a Dispute, which will then be resolved through: (1) Facilitated resolution and (2) Limited facilitated resolution. This type of complaint primarily concerns civil disputes and can be filed if prior attempts at resolution through PUJK have been conducted but were rejected or deemed unsatisfactory by the consumer.
- 2) Complaint Indicating a Violation of Financial Services Regulations (Articles 19 - 21 of POJK No.31/POJK.07/2020)
At this stage, consumers can submit a Complaint Indicating a Violation to OJK regarding actions taken by PUJK in relation to the implementation of financial sector regulations.
- 3) Complaint through the Integrated Consumer Service System in the Financial Services Sector (Article 22 of POJK No.31/POJK.07/2020)
At this stage, consumers may submit their complaints using the services provided by the Financial Services Sector. PUJK is required to take into account all complaints received through this system. If a complaint involving PUJK is identified through monitoring, PUJK must provide information regarding the complaint and update OJK on the progress of the complaint resolution. If the consumer is dissatisfied with PUJK's response, they have the right to escalate the complaint to litigation or non-litigation channels through the Alternative Dispute Resolution Institution in the Financial Services Sector.

2. Litigation Dispute Resolution Efforts

If non-litigation efforts through complaints to PUJK, OJK, and LAPS SJK fail, depositors may pursue dispute resolution through litigation by filing a civil lawsuit in court regarding an Unlawful Act. As stated in Article 1365 of the Indonesian Civil Code (KUH Perdata): *"Every act that violates the law and causes harm to another person obligates the party responsible for the harm to compensate for the loss."*

This provision serves as the legal basis for depositors to file lawsuits if they have suffered losses due to cybercrime affecting their savings. During court proceedings, the involved parties (customers and banks) will present their arguments and evidence before the judge. The judge will issue a verdict based on the evidence presented during the trial. Once a ruling is issued, both the customer and the bank must comply with the decision. If the bank fails to comply, the customer can request court enforcement to ensure their rights are upheld [27].

One case related to this issue is case number 155/Pdt.G/2022/PN Ptk at the Pontianak District Court, which involved an individual plaintiff against a bank (Defendant I) and a telecommunications service provider (Defendant II). The plaintiff held a savings account at the bank (Defendant I), which was illegally accessed, resulting in the withdrawal of the plaintiff's funds without their knowledge. This was facilitated by a fraudulent identity used to obtain a replacement SIM card issued by

Defendant II. Based on the presented evidence and legal facts, the panel of judges ruled that Defendant I, as a banking institution operating on a trust basis, failed to adequately safeguard the plaintiff's funds, constituting an Unlawful Act. Meanwhile, Defendant II was found negligent for allowing the plaintiff's SIM card to be replaced by an unauthorized party, leading to financial losses. Consequently, both defendants were jointly obligated to return the lost funds and compensate the plaintiff [28].

This case serves as a precedent for digital bank customers who suffer financial losses due to cybercrime to file civil lawsuits for Unlawful Acts in the appropriate district court. The legal protection efforts outlined in the prevailing regulations, as described above, are subject to oversight by Bank Indonesia. According to Law No. 23 of 1999 concerning Bank Indonesia and its amendment, Law No. 3 of 2004, Bank Indonesia is designated as the authority responsible for supervising and regulating the banking sector in Indonesia. In this regard, Bank Indonesia holds the authority, responsibility, and obligation to supervise banks through various preventive and corrective measures.

CONCLUSION

Referring to the discussion presented earlier, the conclusions drawn are as follows. The legal relationship formed between a digital bank and a deposit customer is based on the customer's trust in the bank, commonly known as a fiduciary relationship. This trust remains grounded in an agreement or contract in the form of a fund deposit agreement that adheres to the provisions of the Indonesian Civil Code (KUH Perdata).

Furthermore, deposit customers must receive legal protection against cyber crimes in the banking sector, such as Card Skimming, Phishing, Carding, and other data manipulation efforts that may harm them. Legal protection for deposit customers consists of preventive and repressive legal protections. Preventive legal protection generally involves efforts to prevent potential losses for deposit customers, as outlined in Law No. 10 of 1998, POJK Number 6/POJK.07/2022, and POJK No. 12/POJK.03/2018.

On the other hand, repressive legal protection focuses on dispute resolution efforts. This dispute resolution process is generally conducted through two methods: non-litigation mechanisms (outside the judicial institution) and litigation processes in court. Repressive legal protection categorized as non-litigation dispute resolution is stipulated in Article 36 of POJK Number 6/POJK.07/2022, which includes:

1. Filing a complaint with the Financial Services Business Actor (PUJK);
2. Filing a complaint with the Financial Services Authority (OJK).

If non-litigation efforts through complaints to PUJK, OJK, or LAPS SJK do not succeed, the deposit customer may pursue litigation dispute resolution by filing a civil lawsuit in court for Unlawful Acts, as referred to in Article 1365 of the Indonesian Civil Code (KUH Perdata).

ACKNOWLEDGEMENTS


The author thanks all parties who contributed to this research. Special appreciation goes to the sponsors and financial supporters who provided the necessary resources to complete this study.

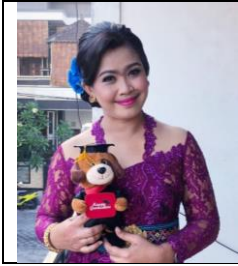
REFERENCES

- [1] A. P. Supriyadi, "Dekonstruksi hukum social commerce Indonesia: Perspektif demokrasi ekonomi di era digitalisasi," *J. Penelit. Huk. Jure*, 2024.
- [2] InterActive QRIS, "Tentang Open API QRIS." <https://qris.online/homepage/open-api>. QRIS Open API Platform.
- [3] S. Nurhaliza, "Analisis Mekanisme Penagihan Pinjaman Online (Pinjol) Ditinjau Dari Peraturan Otoritas Jasa Keuangan Ri Nomor 10/Pojk. 05/2022 Tentang Layanan Pendanaan Bersama Berbasis Teknologi Informasi," *J. Cakrawala Ilm.*, vol. 3, no. 9, pp. 2533–2550, 2024.

- [4] N. Hidayah, "Tinjauan Yuridis Perlindungan Hukum Terhadap Penggunaan Dompot Digital (E-Wallet) Dalam Sistem Pembayaran Di Indonesia," *J. Pustaka Cendekia Huk. dan Ilmu Sos.*, vol. 2, no. 1, pp. 40–56, 2024.
- [5] M. J. Hardinata, S. Shanty, Y. Y. Sitohang, I. A. Rahma, S. Utomo, and S. R. Ramadoni, "Sosialisasi Kebijakan Bank Digital: Perlindungan Hukum Terhadap Data Nasabah Dari Risiko Serangan Siber," *RENATA J. Pengabd. Masy. Kita Semua*, vol. 2, no. 2, pp. 165–172, 2024.
- [6] Republik Indonesia, "Undang-Undang Republik Indonesia Nomor 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan," *Negara Republik Indones.*, vol. 1, no. 163979, pp. 1–527, 2023.
- [7] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 Tentang Penyelenggaraan Layanan Perbankan Digital Oleh Bank Umum," *ojk RI*, no. 1, pp. 1–55, 2018.
- [8] O. J. Keuangan, "Panduan penyelenggaraan digital branch oleh Bank Umum," *Jakarta Otoritas Jasa Keuang.*, 2016.
- [9] J. Tarantang, S. Syawaliah, N. N. A. Astiti, and D. G. G. Kasenda, "PERLINDUNGAN HUKUM NASABAH DALAM PENYELENGGARAN LAYANAN PERBANKAN DIGITAL," *Belom Bahadat*, vol. 13, no. 1, pp. 21–40, 2023.
- [10] M. K. Faridi, "Kejahatan Siber Dalam Bidang Perbankan," *Cyber Secur. dan Forensik Digit.*, vol. 1, no. 2, pp. 57–61, 2018.
- [11] D. M. Putra, "Perlindungan Hukum Terhadap Nasabah Pada Perbankan Digital," *J. Ekon. Bisnis, Manaj. dan Akunt.*, vol. 1, no. 1, pp. 69–84, 2022.
- [12] H. A. A. B. Tarigan and D. H. Paulus, "Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital," *J. Pembang. Huk. Indones.*, vol. 1, no. 3, pp. 294–307, 2019.
- [13] I. Rifa'i et al., *Metodologi Penelitian Hukum*. 2023.
- [14] G. R. A. Putra, "Manusia sebagai subyek hukum," *ADALAH*, vol. 6, no. 1, pp. 27–34, 2022.
- [15] Undang-Undang Republik Indonesia, "Undang-Undang No. 10 Tahun 1998 tentang Perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan," 1998.
- [16] N. N. Muryatini, "Perlindungan Hukum Bagi Nasabah Pengguna Anjungan Tunai Mandiri (ATM) dalam Sistem Perbankan di Indonesia," *J. Magister Huk. Udayana (Udayana Master Law Journal)*, *Univ. Udayana*, vol. 5, no. 1, pp. 119–130, 2016.
- [17] F. Fitriah, "BENTUK DAN TANGGUNGJAWAB PIHAK BANK TERHADAP DANA SIMPANAN PARA NASABAH," *Solusi*, vol. 16, pp. 301–320, Sep. 2018, doi: 10.36546/solusi.v16i3.139.
- [18] C. Fatimah, "Hubungan Hukum Antara Bank dan Nasabah Penyimpan Dana Menurut Undang-Undang Perbankan," *Lex Soc.*, vol. 5, no. 9, 2017.
- [19] Sekretariat Negara, "Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019 Tentang Penyelenggaraan Sistem Dan Transaksi Elektronik," *Media Huk.*, vol. 7, no. 2, p. 70, 2012.
- [20] L. C. Andira and I. Hariyani, "Keabsahan Kontrak Elektronik Dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi," *J. Ilmu Kenotariatan*, vol. 1, no. 2, pp. 34–54, 2020.
- [21] N. Falahiyati, "Tinjauan Hukum Kontrak Elektronik Dalam Pinjam Meminjam Uang Berbasis Teknologi Informasi (Transaksi Peer To Peer Lending)," *J. Justitia*, vol. 2, no. 1, pp. 1–11, 2020.
- [22] M. J. Kusuma and M. H. SH, *Hukum perlindungan nasabah bank: Upaya hukum melindungi nasabah bank terhadap tindak kejahatan ITE di bidang perbankan*. Nusamedia, 2019.
- [23] M. D. Ghifari, "Perlindungan Hukum Terhadap Nasabah Yang Mengalami Kerugian Akibat Kesalahan Sistem Bank Dalam Layanan Mobile Banking," *J. Kertha Semaya*, vol. 12, no. 4, pp. 719–728, 2023.
- [24] F. Nur, "Penegakan Hukum terhadap Kejahatan Digital Perbankan," *Innov. J. Soc. Sci. Res.*, vol. 3, no. 6, pp. 3234–3249, 2023.
- [25] JDIH BPK, "Peraturan OJK No.16 Tahun 2022," no. 19, 2022.
- [26] R. Rosita, "Alternatif Dalam Penyelesaian Sengketa (Litigasi dan Non Litigasi)," *Al-Bayyinah*, vol. 1, no. 2, pp. 99–113, 2017.
- [27] A. Q. Aini and E. F. Khoiroh, "Perlindungan Hukum Nasabah dalam Kasus Pembobolan Rekening Bank di Indonesia," *J. Multidisiplin Ilmu Akad.*, vol. 1, no. 6, pp. 165–172, 2024.
- [28] Mahkamah Agung Republik Indonesia, "Putusan Perkara Nomor 155/Pdt.G/2022/PN Ptk.," 2023. <https://putusan3.mahkamahagung.go.id/direktori/putusan/zaeedd214b3ddd3285a7313435353536.html>,

BIOGRAPHIES OF AUTHORS

	<p>Agita Justisia Br. Tarigan Bachelor of Law at Udayana University. Studied Bachelor for 4 years by taking a concentration in Business Law. Then continued her Master's Studies at Udayana University. Email: agitajt@gmail.com</p>
---	--

**I Gusti Agung Mas Rwa Jayantiari**

Bachelor of Law at Udayana University, then continued her Master's Studies at Brawijaya University. After completing her master's education, she continued her Doctoral Education in Law at Udayana University.

Email: mas_jayantiari@unud.ac.id