

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector



I Made Aditya Mantara Putra^{1*}, Johannes Ibrahim Kosasih^{2*}, I Nyoman Sukandia³

^{1,2,3} Faculty of Law, Warmadewa University, Denpasar Bali

ABSTRACT: The process of globalization and the rapid development of the financial sector supported by advances in information technology have created a very complex financial system in the banking world. As technology develops, information technology-based banking services such as internet banking and other service supporting technology have become very important. Apart from having a positive impact, information and communication technology (ICT) in the banking sector also creates opportunities for crime to occur (*cyber crime*). The government has issued regulations to protect customers and banks from criminal acts in the banking sector related to electronic providers, namely in Law Number 1 of 2024 concerning Information and Electronic Transactions. However, the existence of the law in question does not provide legal certainty in the context of protecting customers and banks against technology-based crime modes. This writing examines the mode of information technology-based crime that occurs in the banking sector and the nature of protection for customers and banks in realizing justice. The research method used is a normative legal research type with a statutory approach, conceptual approach and philosophical approach. The findings in this paper are a protection model that includes the bank's responsibility to protect customer data, as well as the involvement of the government and related authorities to prevent and deal with cyber crime with the aim of maintaining public trust and ensuring fairness in banking services.

I. INTRODUCTION

Indonesia is a legal state based on the 1945 Constitution of the Republic of Indonesia and Pancasila as the state philosophy. In this case it can be said that every aspect of life between citizens of one country and other citizens is certainly regulated by law. This is because the law is always faced by humans both as individuals and as citizens.

Humans in their position have an equal place in the eyes of the law as formulated in the constitution, Article 27 paragraph (1) of the 1945 Constitution of the Republic of Indonesia clearly states that:¹

"All citizens have the same position under the law and government and are obliged to uphold the law and government without exception."

Every citizen wants to get justice in law, equality of position in law is a form of justice. The state's duty is to create laws that do not discriminate against its citizens.² In Article 28 D paragraph (1) of the 1945 Constitution of the Republic of Indonesia, it is stated that:

"Every person has the right to recognition, guarantee, protection, and legal certainty that is fair and equal treatment before the law"

From this explanation, in law enforcement it can be understood that all citizens must comply with all applicable regulations. In the context of law enforcement, it is defined as the application of law to a fact or event. Law enforcement can also be understood as something that enforces or maintains the law by a law enforcement agency if there has been a violation of the law which will or may be violated. This definition implies that there are several factors that must be enforced by law, namely there are regulatory elements that regulate something followed by law enforcement and legal facts or there will be violations, breaking the law or the possibility of new customers where law enforcement will occur.

Philosophical foundations regarding the economy can be seen from the objectives of the Indonesian state as stated in Article 33 paragraph (4) of the 1945 Constitution of the Republic of Indonesia which states that:

¹ Johannes Ibrahim Kosasih & Hassanain Haykal, 2021, *Notary Legal Cases in the Sector of Banking Credit*, Sinar Graphics, Jakarta, p. 1.

² *Ibid.*

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

"The national economy is organized based on economic democracy with the principles of togetherness, efficiency, justice, sustainability, environmental insight, independence, and by maintaining the balance of progress and unity of the national economy."

Judging from this, philosophically the value of justice must be realized in the principle of togetherness. In Pancasila, the fifth principle is, "*Social justice for all Indonesian people*" contains values which are the goal of life to live together. This justice also includes justice and prosperity which are the goals of the Indonesian State in fulfilling the essential demands for physical and spiritual life.³

In today's modern world, the role of banking in the economic progress of a country is very large. Almost all sectors related to various financial activities always require bank services. In simple terms, a bank is defined as a financial institution whose business activities are collecting funds from the community and channeling these funds back to the community as well as providing other banking services.⁴

Bank is a public trust institution that acts as a financial intermediary (*financial intermediary*) between parties who have funds (*surplus unit*) with parties that need funds (*united deficit*) and as an institution that functions to facilitate the flow of payment traffic.⁵ In *Black's Law Dictionary*, the word "bank" is defined as: "*A financial establishment for the deposit loan, exchange, or issue of money and for the transmission of fund; esp., a member of the federal reserve system*". As for the translation, a bank is defined as a financial institution for lending, deposits, exchanging or issuing money and for the transmission of funds, especially members of the federal reserve system.

The legal basis for banking activities is in principle regulated in Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking, hereinafter referred to as the Banking Law. Furthermore, banking activities are regulated in Law Number 4 of 2023 concerning Development and Strengthening of the Financial Sector (hereinafter referred to as the PPSK Law), the existence of this law has changed several provisions in the Banking Law. The PPSK Law was formed with the aim of encouraging the contribution of the financial sector to inclusive, sustainable and fair economic growth in order to improve people's living standards, reduce economic inequality and create a prosperous, advanced and dignified Indonesia.

The provisions regarding banking are regulated in CHAPTER IV which provides the definition of bank in Article 1 Paragraph (2) of the Jo PPSK Law. The Banking Law states that:

"Banks are business entities that collect funds from the public in the form of savings and distribute them to the public in the form of credit or financing and/or other forms in order to improve people's living standards"

Furthermore, a bank is a financial services institution, the legal basis for this financial services institution can be seen in the PPSK Law, in Article 1 paragraph (10) which states that:

"Financial Services Institutions, hereinafter abbreviated to LJK, are institutions that carry out activities in the banking, capital markets, insurance, pension funds, financing institutions and other financial services institutions based on the provisions of laws and regulations in the financial services sector"

Banking is the lifeblood of the economy in all countries, many wheels of the economy are driven primarily by banking, either directly or indirectly. Banking in Indonesia plays a very important role, especially as Indonesia is a country that is developing in all sectors. This is explained in Article 4 of the Banking Law, namely that Indonesian banking aims to support the implementation of national development in order to increase equality, economic growth and national stability towards improving the people at large. To maintain survival in a turbulent financial system, a bank must be able to compete with competing banks and *financial intermediary* other units that also provide financial services. A bank is said to be successful in winning business competitions if it is able to provide better bank financial services than its competitors, while at the same time being able to adapt to every change in the environment. With their managerial skills, bank officials' strategies can transform turbulent environmental threats into various profitable business opportunities.

Examining the role of banks which have the function of collecting funds from the community and channeling funds back to the community, in their role there is a relationship between banks and customers which is based on elements of trust and law. A bank can only carry out activities and develop its bank if the public believes in placing their money in the banking products available at that bank. Based on the trust of the community, banks can mobilize funds from the community to be placed in their banks and channel the money back to the community in the form of credit.⁶

³ Agus Santoso, 2014, *Law, Morals & Justice A Study of Legal Philosophy*, 2nd printing, PT. Fajar Interpratama Mandiri, Jakarta, p. 86.

⁴ Cashmere, 2002, *Banking Basics*, PT. Raja Grafindo Persada, Jakarta, p. 2-3

⁵ Adrian Sutedi, 2007, *Banking Law: An Overview of Merger Money Laundering, Liquidation and Bankruptcy*, Sinar Graphics, Jakarta, p. 1.

⁶ Rony Sautama Hotma Bako, 1995, *Bank and Customer Relationships regarding savings and deposit products*, PT citra Aditya Bakti, Bandung, p. 32.

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

The process of globalization and the rapid development of the financial sector supported by advances in information technology have created a financial system that is very complex, dynamic and interconnected between one financial sub-sector and another. Banks that do not integrate information technology in their products and services will increasingly be abandoned by customers. Therefore, every bank will try as much as possible to equip all their products and services with an information technology base. However, apart from having a positive impact, information and communication technology (ICT) in the banking sector also creates opportunities for new criminal acts to occur (*cyber crime*). Therefore, information technology can be considered a "double-edged sword" which, apart from making a positive contribution to banks in improving their performance, is also an effective means for the emergence of crimes and unlawful acts that are detrimental to customers and the bank itself.⁷

Realizing this, the Government has issued several legal provisions to protect customers (consumers) and banks, including Law Number 8 of 1999 concerning Consumer Protection and Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Information and Electronic Transactions. One of the considerations for the birth of this law is the government's need to support the development of Information Technology through legal and regulatory infrastructure that ensures the use of information technology is carried out safely, prevents misuse, and pays attention to the religious and socio-cultural values of the Indonesian people.⁸

Some examples of Information Technology-based banking products and services which are currently widely used by the public and are superior products for most banks include Mobile Banking, SMS-Banking, telephone banking, ATM, CDM, EDC, and internet banking. Internet banking, which is very popular with customers, is a bank service that allows customers to obtain information, communicate and carry out banking transactions via the internet network.

Internet banking is an electronic banking product that makes it easier for customers to carry out non-cash transactions via computers and internet networks. Services provided through internet banking include services that are also available in conventional banking, such as opening savings accounts, transferring funds between accounts, and electronic bill payments which enable customers to receive and make payments. Internet banking really helps customers in connecting with banks, because with this service, banking access can be done via a personal computer. Internet banking provides many benefits for customers and banks, but behind the benefits, there are also potential negative impacts. One of the negative impacts of using internet banking is the possibility of crimes in the banking sector, such as theft of customer data and credit card numbers, which can then be misused by unauthorized parties.

In Law Number 1 of 2024 Jo. Law Number 11 of 2008 concerning Electronic Information and Transactions, Article 15 states that:

- “(1) Every Electronic System Operator must operate the Electronic System reliably and safely and be responsible for the proper operation of the Electronic System.
- (2) Electronic System Operators are responsible for the Operation of their Electronic Systems.
- (3) "The provisions as intended in paragraph (2) do not apply if it can be proven that force majeure, error and/or negligence on the part of the Electronic System user can be proven."

Furthermore, Article 21 paragraph (1) states that:

"The sender or recipient can carry out electronic transactions themselves, through parties authorized by them, or through electronic agents."

Furthermore, in Article 21 paragraph (2), it is stated that:

"The party responsible for all legal consequences in the implementation of Electronic Transactions as intended in paragraph (1) is regulated as follows:

- a. if done alone, all legal consequences in the implementation of Electronic Transactions are the responsibility of the parties to the transaction;
- b. if carried out by granting a power of attorney, all legal consequences in the implementation of Electronic Transactions are the responsibility of the person giving the power of attorney; or
- c. if carried out through an Electronic Agent, all legal consequences in the implementation of the Electronic Transaction are the responsibility of the Electronic Agent organizer.

From the description of the article above, it can be observed that if one day a customer as a consumer using banking services at any time receives a message from the bank, which in fact the message is a crime mode, and then the customer accidentally presses the link attached by someone who intends to commit a crime, then it is certain that customer data will be used intentionally and cause harm to the customer who owns the account. This phenomenon often occurs in practice, and customers are

⁷ Andi Hamzah, 1993, *Criminal Law Relating to Computers*, Sinar Graphics, Jakarta, p. 3.

⁸ Nani Widya Sari, 2018, *Cyber Crime in the Development of Computer-Based Information Technology*, *Surya Kencana Dua Journal: Dynamics of Legal and Justice Issues*, Vol. 5, No. 2, hal. 579

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

often in a weak position. Customers can only carry out a complaint process to the bank and wait for the results. In this context, a question arises regarding who provides protection and is responsible for the customer's losses. If you look at the provisions in the ITE Law, then the loss is a personal responsibility because you have been negligent, but on the one hand, the customer's actions were carried out unintentionally and he felt he really trusted the bank where he kept his funds. In this case, if the bank is responsible for the customer's losses, then the bank will suffer losses and affect the bank's own profits, because it bears losses that are not due to the bank's fault.

This certainly raises interpretations, because there are no regulations that regulate complete protection for customers when something happens due to a crime mode in the banking sector. Referring to the essence of Article 28 D paragraph (1) of the 1945 Constitution of the Republic of Indonesia, which in principle gives every person the right to protection in a fair manner, it can be said that this value will not be realized in the context of the problems outlined above. . Herein lies the urgency that deserves to be studied regarding the protection of customers and banks against information technology-based crime modes in the banking sector.

Crime *cyber* is a criminal act that is not limited to a certain area and does not require direct contact between the perpetrator and the victim. With these characteristics, all countries, including Indonesia, which are active in internet activities will feel the impact of the evolution of crime in cyberspace. Changes in the 21st century, known as the information age, have changed the approach to crime prevention and control from conventional methods to electronic methods. The availability of networks and personal computers makes every computer device a potential tool for criminals. The phenomenon of globalization in criminal activity allows criminals to cross electronic borders, presenting significant challenges for countries, legal systems and their citizens. This fact cannot be ignored because the internet has become an effective means for committing fraud in the banking sector without being constrained by geographic boundaries or certain regions.

Based on this background, researchers can formulate the problem as follows:

1. What are the modes of information technology-based crime that occur in the banking sector?
2. What is the essence of protecting customers and banks against information technology-based crime modes in the banking sector in an effort to realize the value of justice?

II. RESEARCH METHODS

In principle, legal research has a philosophical basis and is supported by certain methods, so that the research can produce something useful and can be completed as planned. Van Peursen translates the meaning of method literally, initially method was defined as a path that must be taken to become an investigation or research, proceeding according to a certain plan.⁹ Legal research is a process to find legal rules, legal principles, and legal doctrines, in order to answer the legal issues faced, so that legal research is done to produce new arguments, theories or concepts as a prescription in solving the problems faced.¹⁰

In this writing, the research method applied is Normative Legal Research, which involves analysis of primary legal materials, secondary legal materials and tertiary legal materials.¹¹ Normative legal research is a type of legal research that evaluates laws that have been written from various points of view, involving aspects such as theory, history, philosophy, structure and composition, scope and material, consistency, general explanation, each article, formality, and binding force. a law, as well as the use of legal language.¹² The approach applied in this research is to use 3 (three) methods, namely the statutory approach, the conceptual approach and the philosophical approach.

III. RESULTS AND DISCUSSION

3.1. Information Technology-Based Crime Modes That Occur in the Banking Sector

Technology has now become an important part of social life and is considered a primary necessity. One of its main functions is as a supporting facility that facilitates various human activities, especially transactions. With technology, transactions can be carried out more quickly and efficiently, thereby facilitating economic interactions and other activities in modern society. Technological progress also goes hand in hand with the development of the internet, which is the main driver for the birth of various innovations in various aspects of life, especially in the business sector. The term technology, which comes from the Greek, namely *technikos* (meaning art or skill) and *logos* (meaning science or main principle), implies that behind skills there is knowledge or basic principles that underlie them.¹³

⁹ Johnny Ibrahim, 2006, *Normative Legal Research Theory and Methodology*, Bayu Publishing, Malang, p. 26

¹⁰ Peter Mahmud Marzuki, 2009, *Legal Research*, Kencana, Jakarta, p.35.

¹¹ I Made Aditya Mantara Putra, 2020, Legal Responsibility of Banks towards Customers in the Event of Transaction Failure on the Mobile Banking System, *Kertha Wicaksana Journal*, Faculty of Law, Warmadewa University, Denpasar, p. 134.

¹² Abdulkadir Muhammad, 2004, *Law and Legal Research*, Publisher PT. Citra Aditya Bakti, Bandung, pp. 101-102.

¹³ Abdul Wahid and M. Labib, 2005, *Mayantara Crime (Cyber Crime)*, Refika Aditama, Bandung, p.15.

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

When we talk about information technology, we mean any type of technology that helps us manage data. Starting from collecting data, processing it, storing it, to disseminating it. The ultimate goal of all these processes is to produce quality information, namely information that is correct, relevant and timely. This information is what we then use to make decisions, whether for daily needs, business, or even government. Technology that supports this process includes computers, computer networks that connect various devices, and communication technology that allows us to share data globally.

In the current era of globalization, easy access to information and communication has changed many things, including the business world. Digital technology allows us to connect with people all over the world instantly. As a result, trade activities between countries are increasing, because companies can easily communicate and transact with their business partners in various parts of the world. As an understanding, the phenomenon of cyber crime in Indonesia has always been a topic that attracts public attention. Not only the general public, but also those who are directly related to cybercrime, such as law enforcement officers and academics, especially in the legal field. In the realm of legal academics, this discussion is becoming increasingly interesting in line with the government's efforts to formulate laws and regulations related to cyber crime.

The term cyber crime may not be very familiar to the public, because its use is still relatively rare. Therefore, in order not to be left behind by other countries, people need to understand cyber crime. This aims to be able to anticipate the possibility of cyber crime and find appropriate solutions or legal assistance. Apart from that, this understanding is important so that we do not make mistakes that violate the law without realizing it. According to the British police, cyber crime includes all forms of use of computer networks for criminal purposes or high-tech crimes that take advantage of the convenience of digital technology. Furthermore, cyber crime is a crime committed by individuals or groups using computers and other telecommunications devices. People who have expertise in operating computers, such as operators, programmers, analysts, managers, or cashiers, also have the potential to commit this crime. Cyber crime can be carried out in various ways, such as destroying data, stealing data, or using it illegally. One of the main factors that drives the growth of cyber crime is the rapid development of current communication technology, such as telephones, cell phones and other telecommunications equipment related to the development of computer technology.¹⁴

In an era of rapidly developing technology, digitalization has become an important part in various sectors, including banking. Digital banking services, which utilize information technology to provide online services, are designed to facilitate various financial transactions, from fund transfers to investment management. However, behind this convenience, the threat of various modes of crime is increasing. In facing the threat of other modes of cybercrime, digital banks bear a great responsibility to maintain the security of their systems.

Based on Financial Services Authority Regulation (POJK) Number 11 of 2022 concerning the Implementation of Information Technology, digital banks are required to implement good information technology governance and ensure cyber resilience. Article 2 and Article 21 in the regulation emphasize that digital banks must provide safe, reliable and responsible services as a preventive measure against risks such as phishing and hacking. If this provision is violated, the bank may be subject to administrative sanctions, ranging from a written warning, freezing of some business activities, to a reduction in governance assessment which affects the bank's soundness level.

Apart from ensuring technical security, digital banks are also responsible for protecting consumers, in accordance with POJK concerning Consumer and Community Protection in the Financial Services Sector. Article 21 paragraph (1) POJK concerning the Implementation of Digital Banking Services requires banks to implement consumer protection principles, including providing 24-hour customer complaint and inquiry services. If a customer experiences a loss due to bank services, the bank's responsibility is not only limited to material aspects, but also includes financial education to the customer. Furthermore, in order to increase financial literacy, digital banks are also required to organize educational programs in accordance with POJK Number 3 of 2023 concerning Increasing Financial Literacy and Inclusion. Banks must integrate financial literacy programs into their annual plans to increase customer understanding of digital banking products and services. This educational program can be carried out through outreach which involves collaboration with government agencies, academics, non-government organizations, or other parties who have a similar vision. With these steps, digital banks not only strengthen their security systems, but also increase public awareness of the risks and protections in digital banking services.¹⁵

The modes of crime in the banking sector that use information technology can be described as follows:¹⁶

- a. *Carding*, is a crime committed by stealing someone else's credit card number, then using it for trading transactions on the internet, which causes financial losses for the credit card owner.

¹⁴ Sutarman, 2007, *Cyber Crime Modus Operandi and Management*, Laksbang Pressindo, Yogyakarta, p.4.

¹⁵ Chairunnisa, S., Murwadi, T., & Harrieti, N., 2024, Legal Protection for Customers for Phishing and Hacking Crimes on Digital Bank Services Reviewed Based on Indonesian Positive Law, *Journal of Law and Social Sciences*, 2(1), p. 2.

¹⁶ Blessed Renny See, 2022, Legal protection for customers and banks against information technology-based crimes (Cyber Crime), *Caraka Justitia Law Journal*, Vol. 2, No. 1, hal. 60.

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

- b. *Unauthorized Access to Computer and Service*, is a crime committed by entering/infiltrating a computer network system illegally, without permission or without the knowledge of the owner of the computer network system he is entering. Usually criminals will cause a service to malfunction. The attackers deliberately make a service malfunction, which causes financial loss.
- c. *Card Scimming*, namely this crime mode involves breaking into ATM customer accounts by installing skimmers and surveillance cameras in the ATM room. The skimmer functions to steal important data stored on the victim's ATM card, while the surveillance camera is used to record the customer's PIN number. Cases of ATM hacking using skimmers have occurred in many countries. Many countries consider perpetrators of this crime to be public enemies because they can threaten economic stability, especially confidence in the banking business.
- d. *Phishing*, is an act of online fraud that aims to steal internet users' personal information, such as usernames, passwords and credit card details. Actors are very adept at exploiting current issues such as natural disasters, competitions or the world cup. This technique is used to trick victims into providing personal data, such as User ID, PIN, bank account number and credit card number. After obtaining this information, the phisher will use it to access the victim's account, commit credit card fraud, or direct the victim to transfer money to a specific account with the promise of a reward.

The crime modes that utilize information technology above are only a small part of the many banking crimes that occur through information technology, whether committed by third parties or by third parties who collaborate with people within the bank. This cybercrime mode clearly has the potential to cause financial harm to customers. Therefore, the law through its various instruments must be able to provide protection for customers who are victims of the crime mode in question. In this case, bank customers have the status of consumers of banking institutions who are protected by law. Based on Law Number 8 of 1999 concerning Consumer Protection (UUPK), Article 1 number 1 states that "Consumer protection is all efforts to ensure legal certainty to provide protection to consumers." The state, through its implementing systems and instruments, provides legal guarantees and certainty by protecting consumers in Indonesian jurisdiction through steps aimed at preventing threats from irresponsible business actors. This guarantee provides a sense of security not only for consumers, but also for business actors, so that a healthy business climate can be created, facilitate the use of information technology in the banking sector, and eliminate worries about a lack of good faith from business actors in fulfilling their obligations to consumers.

3.2. The Essence of Customer and Bank Protection Against Information Technology-Based Crime Modes in the Banking Sector in Efforts to Realize the Value of Justice

The presence of law in society includes integrating and coordinating interests that may conflict with each other. In this regard, the law must be able to integrate it so that conflicts of interest can be reduced to a minimum. Organizing these interests is carried out by limiting and protecting these interests. In general, in a traffic of interests, protection of certain interests can only be done by limiting the interests of other parties.¹⁷

According to Satjipto Rahardjo in the book *Chatamarrasjid*, the law protects a person's interests by allocating a power to him to act in the context of his interests.¹⁸ This allocation of power is carried out in a measurable manner, in the sense of determining its breadth and depth. Such power is called a right. Thus, not every power in society can be called a right, but only certain satisfactions, namely those given by law to someone.

Banking institutions are institutions that are very dependent on public trust. Therefore, without trust from the public, of course a bank will not be able to carry out its business activities well. So it is not an exaggeration that in the banking world we must maintain public trust in such a way as to provide the best service and primarily provide legal protection for the interests of the public, especially customers of the bank concerned. From this description it can be understood that in order to avoid the possibility of distrust from the public towards the banking world, a form of legal protection is needed for customers, especially depositors, against the possibility of risk of loss.

Legal protection is a protection given to legal subjects in the form of legal instruments, both preventive and repressive, both written and unwritten or in other words legal protection is an illustration of the function of law, namely the concept of legal ethics can provide justice, order, certainty, benefit and peace. The rule of law basically aims to provide legal protection for the people against government actions based on two principles of the rule of law. The legal protection can be explained as follows:

- a. Preventive legal protection, namely legal protection for people who are given the opportunity to submit objections (*participation*) or his opinion before a government decision becomes definitive.
- b. Repressive legal protection, namely legal protection that aims to resolve a dispute.

¹⁷ Chatamarrasjid, 2005, *Indonesian National Banking Law*, 4th printing, Kencana, Jakarta, p. 131.

¹⁸ *Ibid.*

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

Both forms of legal protection are based and sourced from the recognition and protection of human rights, and are based on the principles of the rule of law.¹⁹

The legal relationship between deposit customers and banks is generally based on an agreement. For this reason, it is normal for customers' interests to receive legal protection in line with the protection provided by law to banks. It cannot be denied that it has existed *political will* from the government to protect the interests of bank customers, especially deposit customers. This is proven by the issuance of Law Number 8 of 1999 concerning Consumer Protection, apart from those regulated in Law Number 7 of 1992 jo. Law Number 10 of 1998 concerning Banking.

In connection with legal protection for customers, Marulak Pardede stated that in the Indonesian banking system, regarding protection for customers who save funds, it can be done in 2 (two) ways, namely:²⁰

- a. Implicit protection (*implicit deposit protection*), namely protection resulting from effective bank supervision and guidance, which can prevent bank bankruptcy. This protection is obtained through:
 - Legislation in the banking sector;
 - The protection produced by effective supervision and construction carried out by Bank Indonesia;
 - Efforts to maintain the continuity of the bank's business as an institution in particular and protection of the banking system in general;
 - Maintaining the bank's health level;
 - Carrying out business in accordance with the precautionary principle;
 - Methods of providing credit that do not harm the bank and the interests of customers; And
 - Providing risk information to customers.
- b. Explicit protection (*explicit deposit protection*), namely protection through the establishment of an institution that guarantees public savings, so that if a bank fails, this institution will replace public funds deposited with the failed bank. This protection is obtained through the establishment of an institution that guarantees public savings, as regulated in Presidential Decree Number 26 of 1998 concerning Guarantees for Commercial Bank Liabilities.

In this regard, legal protection for customers and banks in the face of information technology-based crimes in the banking sector is very important, considering the large potential losses that can be caused both to customers and the banking institutions themselves. The increasingly widespread cybercrime, such as hacking, online fraud and digital identity theft, affects the level of public trust in the banking sector. Therefore, it is important for law to exist as an instrument that can integrate and coordinate various interests that may conflict with each other, so as to create fair and appropriate protection for customers and banks.

Furthermore, protection for customers related to technology-based crime modes can be divided into two main forms of legal protection, namely preventive and repressive, with the following description:

- a. Preventive Legal Protection: Protection provided preventively aims to avoid losses or violations that could befall customers. This form of protection can take the form of strict monitoring policies on bank information technology systems, implementing high security standards in digital transactions, as well as educating customers about potential risks and how to avoid them. For example, banks can conduct regular audits of their IT systems and provide security training to customers.
- b. Repressive Legal Protection: Repressive protection focuses on efforts to resolve disputes or losses that have occurred due to cybercrime. This can be done by giving customers the right to file a claim or lawsuit against the bank or other party responsible for the losses experienced. The state also has a role in ensuring that there is a legal system that can provide compensation or sanctions to the party responsible, whether it is a bank that is negligent in safeguarding customer data or a third party who commits a crime.

From the description above, realizing the value of justice in protecting customers and banks means ensuring that both parties receive balanced rights and obligations. Customers have the right to protection from losses caused by information technology-based crimes, while banks have an obligation to maintain security systems and provide clear information regarding existing risks. In this context, the law plays a role in regulating this relationship fairly, so that both parties can experience appropriate benefits and protection.

Justice does not only refer to providing compensation or sanctions for injured parties, but also includes preventive efforts that involve the active role of all parties in maintaining the integrity of the banking system and reducing the potential risk of information technology-based crime. Thus, protecting customers and banks from information technology-based crimes is an

¹⁹ Zahirin Harahap, 2001, *State Administrative Court Procedure Law*, Raja Grafindo Persada, Jakarta, p. 2.

²⁰ Chatamarrasjid, *Op.Cit*, matter. 133.

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

integral part of efforts to create a banking system that is safe, transparent and fair, and can maintain public trust in the banking sector.

IV. CONCLUSIONS AND SUGGESTIONS

4.1. The knot

1. Information technology-based crime modes that occur in the banking sector have developed along with rapid digitalization and ease of access to information. These crimes include various types, such as carding, unauthorized access, card skimming, and phishing, which often target bank customers and threaten the stability of the banking system. Criminals exploit weaknesses in digital security systems to steal personal data or access customer accounts, causing significant financial losses. Therefore, legal protection for customers is very important to prevent and deal with this crime, as regulated in various regulations such as the Consumer Protection Law and Financial Services Authority Regulations. Banking institutions, especially digital banks, must implement a strict security system and educate customers to increase awareness of potential cyber crimes and ensure that there is a guarantee of protection that can provide a sense of security and legal certainty for consumers.
2. The essence of protecting customers and banks against information technology-based crime modes in the banking sector is related to efforts to realize the value of justice through regulating balanced rights and obligations between both parties. Legal protection for customers can be carried out through preventive measures, such as strict supervision of information technology systems and risk education to customers, as well as repressive measures in the form of resolving disputes or losses due to cyber crime. In this context, the law plays a role in integrating the interests of customers and banks fairly, ensuring that customers are protected from losses due to cybercrime, while banks are responsible for maintaining security systems and informing customers of risks. With appropriate legal protection, both preventive and repressive, a banking system that is safe, transparent, fair and can maintain public trust in the banking world is created.

4.2. Suggestion

1. Banking institutions, especially banks that carry out activities digitally, need to improve their security systems by using the latest technology that can identify and prevent potential cybercrime, such as the use of stronger data encryption and more sophisticated intrusion detection systems. It is also important to carry out more intensive education programs for customers regarding ways to protect personal information and identify potential threats such as phishing or card skimming.
2. The government and the Financial Services Authority (OJK) must continue to strengthen regulation and supervision of banking institutions to ensure that they comply with strict security standards, as well as ensure that there are strict sanctions for banks that fail to maintain the security of their systems. Apart from that, it is also important to increase people's digital literacy so that they are more aware and alert to the risks of cybercrime, so they can protect themselves from potential financial losses.

REFERENCES

- 1) Abdul Wahid and M. Labib, 2005, *Mayantara Crime (Cyber Crime)*, Refika Aditama, Bandung
- 2) Abdulkadir Muhammad, 2004, *Law and Legal Research*, Publisher PT. Citra Aditya Bakti, Bandung
- 3) Adrian Sutedi, 2007, *Banking Law: An Overview of Money Laundering Mergers, Liquidations and Bankruptcy*, Sinar Graphics, Jakarta
- 4) Agus Santoso, 2014, *Law, Morals & Justice A Study of Legal Philosophy*, 2nd Printing, PT. Fajar Interpratama Mandiri, Jakarta
- 5) Andi Hamzah, 1993, *Criminal Law Relating to Computers*, Sinar Graphics, Jakarta
- 6) Benedictus Renny See, 2022, *Legal Protection for Customers and Banks Against Information Technology-Based Crime (Cyber Crime)*, *Caraka Justitia Law Journal*, Vol. 2, no. 1
- 7) Chairunnisa, S., Murwadi, T., & Harrieti, N., 2024, *Legal Protection for Customers for Phishing and Hacking Crimes on Digital Bank Services Reviewed Based on Indonesian Positive Law*, *Journal of Legal and Social Sciences*, 2(1)
- 8) Chatamarrasjid, 2005, *Indonesian National Banking Law*, 4th Printing, Kencana, Jakarta
- 9) I Made Aditya Mantara Putra, 2020, *Legal Responsibility of Banks towards Customers in the Event of Transaction Failure on the Mobile Banking System*, *Kertha Wicaksana Journal*, Faculty of Law, Warmadewa University, Denpasar
- 10) Johannes Ibrahim Kosasih & Hassanain Haykal, 2021, *Notary Legal Cases in the Banking Credit Sector*, Sinar Graphics, Jakarta
- 11) Johnny Ibrahim, 2006, *Theory and Methodology of Normative Legal Research*, Bayu Publishing, Malang
- 12) Kasmir, 2002, *Basics of Banking*, PT. Raja Grafindo Persada, Jakarta

The Nature of Customer and Bank Protection against Information Technology Based Crime Modes in the Banking Sector

- 13) Nani Widya Sari, 2018, Cyber Crime in the Development of Computer-Based Information Technology, Surya Kencana Dua Journal: Dynamics of Legal and Justice Issues, Vol. 5, no. 2
- 14) Peter Mahmud Marzuki, 2009, Legal Research, Kencana, Jakarta
- 15) Rony Sautama Hotma Bako, 1995, Bank and Customer Relationships on Savings and Deposit Products, PT Citra Aditya Bakti, Bandung
- 16) Sutarman, 2007, Cyber Crime Modus Operandi and Handling, Laksbang Pressindo, Yogyakarta
- 17) Zahirin Harahap, 2001, State Administrative Court Procedure Law, Raja Grafindo Persada, Jakarta

LEGISLATION

- 1) The 1945 Constitution of the Republic of Indonesia
- 2) Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking.
- 3) Law Number 4 of 2023 concerning Development and Strengthening of the Financial Sector
- 4) Bali Province Regional Regulation Number 3 of 2017 concerning Village Credit Institutions



There is an Open Access article, distributed under the term of the Creative Commons Attribution – Non Commercial 4.0 International (CC BY-NC 4.0) (<https://creativecommons.org/licenses/by-nc/4.0/>), which permits remixing, adapting and building upon the work for non-commercial use, provided the original work is properly cited.