

Actualization Of Bank Principles Of Precaution In An Efforts To Protect Customers Against Social Engineering Banking Crime Modes

I Made Aditya Mantara Putra, Johannes Ibrahim Kosasih, I Nyoman Sukandia, AA Ngr Mayun Narindra

adityamantara@gmail.com

Faculty of Law, Warmadewa University, Indonesia

Article Info

Received: 2025-01-20

Revised: 2025-02-20

Accepted: 2025-05-29

Keywords:

*Bank; Customer;
Protection; Social
Engineering Crime*

Abstract

This study is based on the increasing cases of social engineering fraud in the banking sector that threaten customer security. The urgency of this study lies in the need to understand how the bank's precautionary principle can be actualized to protect customers from increasingly sophisticated crime modes. The purpose of this study is to analyze the application of the precautionary principle in customer protection efforts and to identify steps that can be taken by banks to reduce the risk of such crimes. The research method used is a normative method supported by empirical data. Empirical data were collected through in-depth interviews with bank management, namely at PT. Bank BRI Denpasar Renon Branch and PT. Bank BPD Bali Denpasar Branch. The results of the study indicate that although banks have implemented several precautionary principles, there are still gaps in their implementation that can be exploited by criminals. This study found that customer education and improving digital security systems are important steps that need to be taken to strengthen customer protection. The output of this study is expected to provide practical recommendations for banks in optimizing the application of the precautionary principle and increasing customer awareness of the potential risks of social engineering crimes. In addition, the results of this study can also be a reference for better banking policies in protecting customers in the digital era.____

I. Introduction

Globalization currently affects various aspects of human life, including in the fields of economics and technology. These developments encourage each individual to continue to adapt, innovate, and strive to meet needs and improve welfare. Rapid technological advances have also caused changes in people's lifestyles towards the millennial era. In this process, financial institutions play an important role in supporting the smooth running of economic activities. These financial institutions are divided into two types, namely those in the form of banks and those that are not banks. The interaction between the community and financial institutions is based on trust. This trust means that the community prefers one financial institution over another because of the belief that their funds can be withdrawn at any time when needed.¹

In the effort to develop the Indonesian economy as a developing country, the law plays a role in protecting, regulating, and planning economic life so that economic activities can run towards the progress and welfare of society. The law influences the economic sector by establishing rules that regulate various economic activities. In addition, the role of banking institutions is also emphasized as an important element in supporting the smooth running of economic life.²

The provisions regarding banking are regulated in Chapter IV which provides a definition of a bank in Article 1 paragraph (2) of Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (hereinafter referred to as the PPSK Law), which stipulates that:

"A bank is a business entity that collects funds from the public in the form of savings and distributes them to the public in the form of credit or financing and/or other forms in order to improve the people's standard of living."

Furthermore, a bank is a financial services institution, where 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 as LJK, are institutions that carry out activities in the banking, capital markets, insurance, pension fund, financing institutions and other financial services institutions sectors based on the provisions of laws and regulations in the financial services sector."

Reviewing the role of banks that function as collectors of funds from the community and redistribute them, there is a relationship between banks and customers that is based on trust and legal aspects. Banks can only operate and grow if the community has the trust to save their funds in various banking products offered. This trust allows banks to collect funds from the community, then redistribute them in the form of credit to support economic activities.³

In carrying out banking activities, basic principles are needed as a foundation. The principles underlying the contractual relationship between banks and customers include the principle of economic democracy, the principle of prudence, the principle of trust (fiduciary

¹ Anita Christiani, 2010 *Banking Law (Analysis of the Independence of Bank Indonesia, Supervisory Body, Islamic Banks and the Principle of Knowing Your Customer)*, Atma Jaya University, Yogyakarta, p. 1.

² I Made Aditya Mantara Putra, I Nyoman Putu Budiarta, Johannes Ibrahim Kosasih, 2024, *Customer Transactions of Cash Pick Up Service (Prudential Banking Principles)*, Scopindo Media Pustaka, Surabaya, p. 3.

³ Rony Sautama Hotma Bako, 1995, *Bank and Customer Relationships regarding Savings and Deposit Products*, PT Citra Aditya Bakti, Bandung, p. 32.

principle), the principle of confidentiality (confidential principle), and the principle of knowing your customer (know your customer principle).⁴The principles above are very important to be implemented by banks to provide a sense of comfort for customers when making transactions at the bank. In addition, these principles are also important because without the principles underlying the contractual relationship between the bank and the customer, it affects the level of customer trust who will save or borrow funds at the bank.

Banking crime modes are now developing by stealing customer data for financial gain, along with the rapid digitalization of banking. Advanced technology is used by banks to improve efficiency and services, such as e-banking, which facilitates real-time transactions without time and place restrictions. However, this progress also increases the risk of crimes such as social engineering fraud. Therefore, banks and customers must always be careful and vigilant in making transactions. Social engineering fraud is an online crime that aims to steal or damage personal information from targets. Perpetrators, such as hackers, use various methods, including social media features. In addition to utilizing social media features, hackers also carry out social engineering through fake emails, WhatsApp messages, or phone calls to build trust from targets. This crime certainly has a serious impact on business, slowing economic growth, and reducing customer trust in online transactions. In this case, if customers switch to manual transactions to avoid fraud, economic activity will slow down, which ultimately has an impact on overall economic growth. From this description, the following problems can be formulated:

1. How is the implementation of the banking prudential principle as a form of customer protection against banking social engineering crime modes?
2. What is the impact of the social engineering fraud crime mode in the banking world in Indonesia?

2. Research Method

In this study, data were collected using normative legal research methods or referred to as literature studies which are also supported by empirical data. Normative legal research is research with an approach that is often used in the development of legal science, especially in the field known as Legal Dogmatics (Rechtsdogmatiek). Legal scholars such as Mochtar Kusumaatmadja and Koesnoe term it as positive legal science, while Philipus M. Hadjon calls it Dogmatic Legal Science. H. Ph. Visser't Hooft uses the term practical legal science. The way a science works, including the methods used, is very dependent on the purpose or what the science wants to express.⁵The literature study process also includes searching, collecting, and reading various sources of information, such as books, websites, journals, theses, laws, and other relevant materials, which are also supported by data from interviews. During this process, data sources and legal materials are identified, categorized, and inventoried to support research analysis and discussion.⁶This study applies a descriptive-qualitative method in data processing and analysis. This approach aims to detail the information

⁴Hermansyah, 2006, *National Banking Law in Indonesia*, PT. Kencana, Jakarta, p. 19.

⁵Sulistiyowati Irianto and Shidarta, 2011, *Legal Research Methods: Constellation and Reflection*, 2nd ed., Indonesian Obor Library Foundation, Jakarta, p. 142.

⁶1986, *Introduction to Legal Research*, University of Indonesia, Jakarta, p. 51.

obtained from literature studies and interviews, describe the data in depth, and test the level of truth and validity of information relevant to the research context.⁷By using this method, researchers can provide a comprehensive picture of the research object. Qualitative analysis allows researchers to explore data in depth, resulting in a more complete and accurate understanding of the legal issues being studied.

3. Results and Discussion

Implementation of Banking Prudential Principles as a Form of Customer Protection Against Banking Social Engineering Crime Modes

The principle of prudence in banking is a basis that confirms that banks are required to apply the principle of prudence in carrying out their functions and business activities in order to maintain trust and funds collected from the public. In the context of Islamic banking in Indonesia, the implementation of operational activities must be guided by the principle of economic democracy and apply the principle of prudence in accordance with the provisions of Article 2 of Law Number 21 of 2008 concerning Islamic Banking.⁸Furthermore, this precautionary principle emphasizes the bank's vigilance to always maintain aspects of banking, including those related to bank health, management capability, liquidity, profitability, capital, asset quality, etc. So the implementation of *prudential banking principle* This is related to all aspects of banking with the aim of protecting public funds, creating a healthy, liquid and solvent banking situation, so that the level of public trust remains high to deposit their funds in the bank.

The legal basis for the principle of bank prudence here is stated in Article 2 and Article 20A Paragraph (1) and (2) of the UUPPSK in conjunction with the Banking Law.⁹Article 2 of the Banking Law states that:

"Indonesian banking in conducting its business is based on economic democracy using the principle of prudence"

From the provisions of the article, what is meant by "economic democracy" based on the explanation of Article 2 of the Banking Law is economic democracy based on Pancasila and the 1945 Constitution. Furthermore, Article 20A Paragraphs (1) and (2) states that:

- (1) "Banks are required to apply the principle of prudence including risk management in carrying out business activities;
- (2) Banks are required to prepare internal procedures regarding the implementation of the precautionary principles as referred to in paragraph (1)"

Judging from the description of this article, the principle of prudence in banking requires banks to always be careful in carrying out their business activities, in the sense that they must always be consistent in implementing laws and regulations in the banking sector based on professionalism and good faith.

According to P. Sugarda, the principle of prudence in banking is closely related to the risks and policies taken by banks in managing finances. If someone is trusted to manage funds, then it must be done responsibly and with great care, so that it reflects the implementation of

⁷ Abdulkadir Muhammad, 2004, *Law and Legal Research*, PT. Citra Aditya Bakti, Bandung, p. 34.

⁸2001, *Legal Aspects of Banking in Indonesia*, Gramedia Pustaka Utama, Jakarta, p. 18.

⁹Indonesian Bankers Association, 2014, *Understanding Banking Operations 2*, Gramedia Pustaka Utama, Jakarta, p. 224.

the right and not careless mandate.¹⁰Sutan Remy Sjahdeini stated that the principle of prudence in banking needs to be applied by banks, not only to protect customers from losses, but also because banks have an important position in the national financial system which concerns the interests of the wider community.¹¹Meanwhile, according to Asikin, the principle of caution or *prudential banking principle* which is applied in banking generally to support economic activities and is able to create economic stability but specifically as a form of protection for people who save their funds in banks. In the banking sector, the application of the principle of prudence is part of the monetary system that covers the interests of society in general and is the obligation of the bank to ensure that people who entrust their funds to the bank are not harmed.

Social engineering crime is a manipulation method that can threaten data security. The perpetrators of this social engineering can infiltrate viruses, hack systems, or carry out various illegal cybercrimes. This type of fraud is often difficult to detect so that the victim's data can be stolen without their knowledge. Social engineering fraud takes advantage of user errors in acting or making decisions to gain access to important information. The perpetrators often use subtle tricks so that the victim is not suspicious, so that data can be obtained more easily.¹²Social engineering crimes can be divided into several types, namely:

- a. Scareware, which is an attempt to scare the victim. This technique is usually done by displaying fake notifications or warnings on the victim's device. The scareware perpetrator will imitate the appearance, features, or original system of the device to make it look convincing, so that the victim believes that their device has been infected with a virus or malware. As a result, the victim is influenced to click certain buttons or follow the instructions given by the scareware notification. After the victim follows these steps, the perpetrator can exploit the gaps created to obtain the victim's personal data.
- b. Baiting, which is a crime committed by first giving bait to the victim. One form of baiting that often occurs is when a website asks for permission to access your device. If you give that permission, the perpetrator will have the opportunity to steal personal data stored on your device.
- c. Pretexting, a crime committed by a method where the perpetrator pretends to be a close person or coworker of the victim. For example, the perpetrator may send an email informing the victim that they have won a prize. However, before the prize can be received, the victim is asked to reply to the message or follow certain instructions made convincingly by the perpetrator.
- d. Phishing, which is an attack by sending official messages or emails to victims while pretending to be an authorized party. Thus, the victim becomes trusting and willing to follow instructions or visit websites directed by the perpetrator. The main purpose of this phishing is to obtain personal information, financial data, or accounting data of the victim.

¹⁰2019, *Banking Law: Analysis of Principles, Products, Risks and Management in Banking*, Scopindo, Surabaya, p. 34.

¹¹ *Ibid.*

¹²Siswanto, 2024, *Principles of Banking Customer Prudence in Maintaining Business Security from Social Engineering Fraud*, *Justiciable Journal*, University of Bojonegoro, Vol. 7 No. 1, p. 9.

- e. Telecom Fraud, a crime committed by impersonating a close relative, co-worker, or someone the target can trust. This type of telecom fraud is usually done by telephone, for example when there is a case of fraud via a call asking the target to transfer money at the nearest ATM.
- f. Spear Phishing, which is a crime that is also phishing, but more structured. The target of spear phishing is also more specific than regular phishing. Spear phishing that has a target requires the perpetrator to know at least the basic information of the victim. The spear phishing perpetrator then disguises himself, by adjusting the message based on the victim's contacts or characteristics. The goal is that the spear phishing attack is not conspicuous or the victim will not be easily aware.¹³

From the various types of social engineering, it can also be seen how it works, namely by working with the fraudster first designing a strategy by collecting various information about the potential victim. After that, the fraudster enters the victim's daily life and begins to build a relationship with the main goal of gaining trust. When the victim truly trusts and shows weakness, the fraudster will take advantage of this condition to exploit the victim. Once the goal is achieved, the fraudster will end the relationship with the victim. This process can occur in just one interaction, for example via email, but can also last for months through various media such as chat on social media platforms. The success of social engineering occurs when the victim shares important or personal information with the fraudster. Regarding social engineering in banking, banks as institutions that are highly trusted by the public should help minimize or mitigate the risks that occur in the future for customers. This can be realized by implementing the principle of bank prudence in carrying out its business activities.

Talking about legal protection, it will not be separated from talking about the rights of each individual. Dworkin stated that rights are what must be upheld by anyone. As Dworkin's opinion in Lawrence Friedman:

"Rights are best understood as trumps over some background justification for political decisions that the state has at goal for the community as whole."¹⁴(rights are best understood as the highest values of background justification for political decisions that express a goal for society as a whole)."

Dworkin acknowledges that intervention in individual life to eliminate rights is justified, if a specific basis can be found. Furthermore, according to Dworkin, as quoted by Peter Mahmud Marzuki, rights are not what is formulated but the values underlying the formulation. Facts are so valuable that they give rise to the theory of interests and the theory of will, as described by Jeremy Bentham and Rudolf Von Jhering, who view rights as interests that are protected by law.¹⁵

Furthermore, Philipus M. Hadjon is of the opinion that: "The principle of legal protection for the people against government actions is based on and originates from the concept of recognition and protection of human rights. Because according to history in the west, the birth of concepts on the recognition and protection of human rights is directed at restrictions and

¹³Ibid., hal. 10.

¹⁴ Lawrence Friedman, 1987, *The Legal System: A Social Science Perspective*, Russell Sage Foundation, p. 164.

¹⁵ Peter Mahmud Marzuki, 2006, *Introduction to Legal Science*, Kencana Prenada Media Group, Jakarta, p. 176.

the placement of obligations on society and government". In this case, Philipus M. Hadjon also stated that "legal protection for the people is divided into 2 types, namely preventive legal protection and repressive legal protection. Preventive legal protection aims to prevent disputes from occurring, while conversely repressive legal protection aims to resolve disputes".¹⁶

Based on the theory of legal protection in question, if it is associated with the application of the principle of bank prudence, it can be said as an effort to prevent the occurrence of social engineering crimes in banking. In implementing the principle of banking prudence to protect customers from social engineering fraud as an effort to form preventive legal protection, banks need to take several strategic steps. First, banks need to organize socialization regarding the potential risks of this crime so that customers have an adequate understanding of the types of fraud that often occur in the banking sector, including social engineering fraud. Second, banks are required to provide a complaint or confirmation channel that can be accessed by customers 24 hours a day, considering that this crime generally occurs via the internet using social media and other digital methods. Thus, customers can immediately report if they find suspicious activity in the name of the bank. Finally, banks must be proactive in reminding customers about the potential dangers of this crime, so that customers are always alert and careful in every banking transaction. These steps are expected to create a sense of security and increase customer trust in bank services.

Furthermore, referring to the provisions in Bank Indonesia Regulation Number 3 of 2023 concerning Bank Indonesia Consumer Protection, Article 1 number 3 states that:

"Bank Indonesia Consumer Protection, hereinafter referred to as Consumer Protection, is all efforts that guarantee legal certainty to provide protection to consumers."

Furthermore, Article 7 paragraph (2) describes the principles of consumer protection, which include:

- a. "equality and fair treatment;
- b. openness and transparency;
- c. education and literacy;
- d. responsible business behavior;
- e. protection of consumer assets against misuse;
- f. protection of consumer data and/or information;
- g. effective handling and resolution of complaints; and
- h. compliance enforcement".

From the description of the principle, it provides an understanding that banks as service providers, especially in storing public funds, must provide preventive and repressive efforts against the existence of social engineering crime modes. Therefore, in supporting the preventive legal protection so that it can be optimal, banking customers must also have a principle of caution, both to protect themselves and their businesses by always being vigilant in sharing personal data; being careful in using social media and being aware of files downloaded from the internet. The reason is, there are a number of sites that can ask for permission to access personal devices; be careful before clicking on links that are often used by criminals. Currently, there are often unknown links sent via websites, emails, or social media from unknown sources; you should not immediately trust people you have just met,

¹⁶ *Ibid*, p. 38.

especially if you only know them from online media. For that, so that someone can confirm their identity first or immediately activate the spam feature in your email to avoid social engineering modes.

Regarding repressive legal protection (resolution efforts) in the event of social engineering crimes in the banking world and causing losses to customers, this can be realized through various mechanisms, namely:

1. Criminals can be prosecuted through criminal provisions in the Criminal Code or special regulations such as the Electronic Information and Transactions Law (UU ITE) to ensure strict law enforcement.
2. The police and prosecutors have the authority to investigate and prosecute the perpetrators involved, with the aim of collecting evidence and bringing the case to court.
3. Perpetrators who are proven guilty can be subject to criminal sanctions, either in the form of imprisonment or a fine, as an effort to provide a deterrent effect and prevent similar crimes from recurring.
4. Customers who are victims can file a civil lawsuit to claim compensation for the losses they have suffered.
5. The role of supervisory institutions such as Bank Indonesia (BI) and the Financial Services Authority (OJK) is also very important in supervising and imposing administrative sanctions on banks if they are proven to be negligent in protecting their customers' data.

From the explanation above, the application of the precautionary principle by banks is a very important form of legal protection for customers in facing the risk of social engineering crimes in the banking sector. This precautionary principle includes the bank's vigilance towards various aspects that support banking health, including risk management, liquidity, and asset quality, so that public funds can be maximally protected. The implementation of this precautionary principle is also an instrument of preventive legal protection, which is implemented through strategic steps such as socialization to customers about the potential for social engineering crimes, the provision of a 24-hour complaint channel, and proactive reminders from the bank so that customers are more aware of various fraud modes. In addition, customers also need to increase their precautionary principles independently to avoid social engineering-based fraud. If the crime has occurred and caused losses to customers, repressive legal protection is also available through criminal, civil, and supervision by banking authorities such as the OJK or Bank Indonesia. All forms of legal protection are expected to be able to increase public trust in the banking world and reduce the risk of losses caused by social engineering crimes.

The Impact of Social Engineering Fraud Crime Mode in the Banking World in Indonesia

Various crimes in financial institutions, especially banking, often occur because banks are often targets or means for perpetrators of crimes. Crimes in the banking sector itself are difficult for law enforcement to reach, because there are no regulations that regulate them

comprehensively in the PPSK Law or the Banking Law. Law enforcers must seek a legal basis from various existing laws, such as the Criminal Code or other regulations. Thus, law enforcement officers need to find a legal basis so that perpetrators of crimes can be subject to sanctions for violations or cases that occur in the banking sector. Regarding crimes in the banking sector, this crime is basically a form of crime that has developed over time. There are three important elements that make an action categorized as a crime. First, the action is prohibited by law, namely positive law. Second, the crime is processed through state mechanisms, not by individuals personally. This means that reports, investigations, inquiries, detentions, prosecutions, case examinations, and criminalization must be carried out by the government through official institutions within the framework of the criminal justice system. Third, perpetrators of crimes are subject to criminal sanctions, not just compensation to victims. These criminal sanctions can be in the form of the death penalty, imprisonment, detention, or fines.¹⁷

The crime that is said to be organized crime has developed in such a way and become a challenge for law enforcement, especially in Indonesia. This is because many criminals have changed the way they commit crimes with various modes so as to deceive and make it difficult for law enforcement to overcome them. This is also an impact of globalization and technological advances that continue to revolutionize the forms of crime that occur in banking. The organized crime referred to here is the mode of social engineering crime. In the rapidly developing digital era, the banking world in Indonesia is facing various new challenges, one of which is the rise of social engineering-based fraudulent crime modes. This crime not only threatens the security of customer data, but can also have a broad impact on the stability of the banking sector as a whole. Social engineering fraud exploits human psychological weaknesses to gain illegal access to important information, which is then used to harm the victim. The impact of this crime is not only financial, but can also erode public trust in banking institutions. Therefore, understanding the impact of this social engineering crime is very important to identify potential losses and formulate strategic steps to protect customers and maintain the integrity of the banking sector in Indonesia.

Currently, social engineering is one of the important issues that has received serious attention in the field of cybersecurity. Social engineering itself is a method of psychological manipulation used by irresponsible parties to deceive individuals, with the aim of obtaining confidential information or provoking actions that can cause data leaks. In Indonesia, there have been a number of cases of large data leaks due to this method.¹⁸ The threat of social engineering is now growing in Indonesia, having a significant impact on various sectors. Some examples that reflect this impact are the data leak at Tokopedia in 2020, which involved around 91 million users, although the exact cause has not been confirmed, social engineering attacks such as phishing are suspected to be one of the triggers. In 2023, the police reported a significant increase in online fraud cases that utilize social engineering, especially through fake prize draw modes on social media. This mode ensnares victims to submit personal information or transfer money with the lure of prizes. Banks in Indonesia have also been targeted by social engineering attacks, such as vishing (phishing via telephone) and smishing

¹⁷Johannes Ibrahim Kosasih & Hassanain Haykal, 2021, *Notary Legal Cases in the Field of Banking Credit*, Sinar Grafika, East Jakarta, p. 308.

¹⁸Yogi Kristiyanto, et al., 2024, *Impact of Social Engineering Attacks Case Study of Data Breach in Indonesia*, Proceedings of Managerial and Entrepreneurship VIII, IPWIJA University, p. 10.

(phishing via SMS). Fraudsters often pretend to be bank officers to obtain sensitive data such as credit card numbers and PINs.

Furthermore, banking operational activities here must be able to balance between the responsibilities that must be fulfilled (principles of banking obligations) and bank governance (principles of banking management), while still adhering to the principles of banking ethics. In implementing the principles of banking obligations, the most important thing is to grow public trust that is increasingly high in banks. The higher the level of trust, the more it will indirectly have a positive impact on macroeconomic conditions. Banking obligations put forward by Rimsky K. Judisseno, include:¹⁹

- a. General obligations, which include providing good service, a sense of security, and equal treatment (*equal treatment*) to customers such as savers, borrowers and other users of banking services;
- b. Special obligations, which include obligations to the government, employees, and owners. The government usually asks banks to participate in the success of development and maintain monetary stability in order to improve the standard of living of the people in order to achieve a just and prosperous society. In addition to fulfilling its obligations to the government, banks must also pay attention to the interests of their owners, namely better profit sharing. Better profits will encourage owners or shareholders to continue to invest their capital in banking institutions. Finally, the obligation of banks to their employees is that banks can guarantee continuity of work and a better career future.

From the description above, it can be understood that the banking sector has an obligation to maintain public trust, which must be supported by good management. Good bank management needs to pay attention to the principles of bank health. The main objective of implementing the principle of prudence is so that the bank is always in a healthy, liquid, solvable, and profitable condition. By implementing this principle of prudence, it is hoped that the level of public trust in banks will remain high, so that they do not hesitate to save in the bank. Therefore, the general explanation in the Banking Law emphasizes the importance of this principle of prudence, as well as the need to improve the provisions related to bank business activities, especially in terms of channeling funds. For this reason, several banking regulations have established guidelines in the application of the principle of prudence that must be adhered to by every bank.

CNN Indonesia reported that every month around 2,000 private bank customers in Indonesia experience cybercrime through social engineering methods. These crimes most often target bank customers, digital wallet users, and e-commerce and social media consumers.²⁰ Social engineering is common in Indonesian society and still claims many victims due to the low level of public awareness and knowledge about information security. Amirudin, Head of Anthropology Study Program at the Faculty of Cultural Sciences, Diponegoro University, also revealed that there are still differences in understanding between individuals about which data is considered private and which is considered open, thus creating ambiguity about the boundaries of personal data. This ambiguity is also a factor

¹⁹ Trisadini, 2002, *Monetary and Banking System in Indonesia*, Gramedia Pustaka Utama, Jakarta, p. 104.

²⁰ CNN Indonesia, "Per Month, 2 Thousand Bank Customers Become Victims of Cybercrime," <https://www.cnnindonesia.com/teknologi/20220826193538-185-839667/per-bulan-2-ribunasabah-bank-jadi-korban-kejahatan-siber>.

in the success of social engineering attacks, because people with limited understanding of personal data security tend to overshare on social media, even voluntarily providing personal information to parties whose identities are unclear.²¹ From the explanation above, it can be said that social engineering-based cybercrime in Indonesia is rampant and causes many victims every month, especially among bank customers, digital wallet users, and e-commerce and social media users. This is exacerbated by the low public awareness of personal data security and the ambiguity about which data is classified as private or open. This condition is exploited by criminals to commit fraud, often by exploiting the habits of people who like to share information excessively on social media.

The impact of the social engineering fraud crime mode in the banking world in Indonesia can be described as follows:

1. Financial Loss For Customers

Customers who become victims of social engineering experience direct financial losses, for example through OTP fraud, phishing, smishing, or vishing. The perpetrators often claim to be official parties (banks, police, government employees) to gain access to the victim's account. According to the Financial Services Authority (OJK, 2021), customer losses due to digital crimes including social engineering in Indonesia continue to increase every year.²²

2. Declining Confidence in Banking

Social engineering crimes have an impact on decreasing public trust in the banking system. This has the potential to cause customers to hesitate to use digital banking services or even save money in the bank. Trust is the main foundation in the relationship between customers and banks, so if this trust is disturbed, it will affect the stability of the financial system.²³

3. Reputational Risk to Banks

Banks can suffer reputational losses even though legally banks are often not fully responsible for customer negligence. However, in practice, the public still demands that banks be responsible for transaction security. According to the book *Principles of Banking Law* Cranston's work, a bank's reputation is one of its most important intangible assets and loss of reputation can have long-term impacts on a bank's performance.²⁴

4. Operational Expenses and Security Investments

Banks must allocate more funds to improve system security and educate customers, including installing fraud detection systems and employee training. This is a significant additional burden for the banking industry.²⁵

5. Systemic Impact on Economic Stability

If social engineering fraud cases occur massively, it will cause instability in the financial sector. This can trigger a large-scale withdrawals, which could ultimately impact the

²¹Tabina Dea Anindya, 2023, Social Engineering Dangers Education Using Quizizz Learning Media to Increase Banking Customer Information Security Awareness, *Scientific Journal of Technology and Computers*, Vol. 4, No. 3, Udayana University,

²²Financial Services Authority (OJK). (2021). *OJK Annual Report 2021*. Jakarta: OJK.

²³ Mishra, S., et al. (2019). "Trust in Digital Banking: A Literature Review and Future Research Agenda." *International Journal of Bank Marketing*, 37(6), 1585–1612.

²⁴ Cranston, R., Avgouleas, E., & Van Santen, K. (2018). *Principles of Banking Law*. Oxford University Press.

²⁵ Lieutenant, C. (2018). *Social Engineering: The Science of Human Hacking*. Wiley.

stability of bank liquidity and the health of the national economy.²⁶

Judging from the description above, the mode of social engineering fraud has become one of the main challenges in the banking sector in Indonesia. This crime is increasingly rampant due to the development of digital technology, low public awareness of personal data security, and ambiguity in understanding personal data versus open data. This crime has a significant impact on customers, ranging from direct financial losses to reduced trust in banking. In addition, banks face serious reputational risks and must bear additional operational burdens to improve security and education for customers. If allowed to spread, social engineering can cause systemic financial sector instability that has an impact on the national economy. Therefore, prevention efforts, education, and the application of the principle of prudence are urgent matters to maintain integrity and trust in the banking industry in Indonesia.

4. Conclusion

The conclusions of this study are as follows:

- a. The implementation of the principle of bank prudence is very important in protecting customers from social engineering crimes that target personal data through psychological manipulation. This principle includes risk management, bank health, and protection of public funds as a preventive measure, including education, complaint channels, and reminders for customers. If a crime occurs, repressive legal protection can be taken through criminal enforcement, civil lawsuits, and supervision by authorities such as the OJK and BI. Collaboration between bank prudence and customer vigilance is expected to maintain public trust and reduce the risk of losses due to social engineering.
- b. The social engineering fraud crime mode is a serious challenge for the banking world in Indonesia, especially because of its significant impact on customers and the banking industry as a whole. This crime causes direct financial losses, decreased customer trust, reputational risks for banks, and additional operational burdens. If not handled properly, this crime has the potential to threaten the stability of the financial sector systemically. Therefore, preventive efforts through education, strengthening regulations, and implementing the principle of banking prudence are very important to protect customers and maintain public trust in the banking industry in Indonesia.

References

- Abdulkadir Muhammad, 2004, *Law and Legal Research*, PT. Citra Aditya Bakti, Bandung
- 2019, *Banking Law: Analysis of Principles, Products, Risks and Management in Banking*, Scopindo, Surabaya
- Anita Christiani, 2010 *Banking Law (Analysis of the Independence of Bank Indonesia, Supervisory Body, Islamic Banks and the Principle of Knowing Your Customer)*, Atma Jaya University, Yogyakarta
- CNN Indonesia, "Per Month, 2 Thousand Bank Customers Become Victims of Cybercrime," <https://www.cnnindonesia.com/teknologi/20220826193538-185-839667/per-bulan-2-Cybercrime>,

²⁶ Nystrom, M. (2020). "Combating Social Engineering in Financial Services." *Journal of Financial Crime*, 27(2), 499–511.

[ribunasabah-bank-jadi-korban-kejahatan-siber.](#)

- Cranston, R., Avgouleas, E., & Van Santen, K., 2018, *Principles of Banking Law*. Oxford University Press.
- Lieutenant, C., 2018, *Social Engineering: The Science of Human Hacking*. Wiley.
- Hermansyah, 2006, *National Banking Law in Indonesia*, PT. Kencana, Jakarta
- I Made Aditya Mantara Putra, I Nyoman Putu Budiarta, Johannes Ibrahim Kosasih, 2024, *Customer Transactions of Cash Pick Up Service (Prudential Banking Principles)*, Scopindo Media Pustaka, Surabaya
- Indonesian Bankers Association, 2014, *Understanding Banking Operations 2*, Gramedia Main Library, Jakarta
- Johannes Ibrahim Kosasih & Hassanain Haykal, 2021, *Notary Legal Cases in the Field of Banking Credit*, Sinar Grafika, East Jakarta
- Lawrence Friedman, 1987, *The Legal System: A Social Science Perspective*, Russell Sage Foundation
- Mishra, S., et al., 2019, "Trust in Digital Banking: A Literature Review and Future Research Agenda." *International Journal of Bank Marketing*, 37(6)
- Nystrom, M., 2020, "Combating Social Engineering in Financial Services." *Journal of Financial Crime*, 27(2)
- Financial Services Authority (OJK), 2021, *OJK Annual Report 2021*, OJK, Jakarta
- Peter Mahmud Marzuki, 2006, *Introduction to Legal Science*, Kencana Prenada Media Group, Jakarta, p.
- 2001, *Legal Aspects of Banking in Indonesia*, Gramedia Main Library, Jakarta
- Rony Sautama Hotma Bako, 1995, *Bank and Customer Relationships regarding Savings and Deposit Products*, PT. Citra Aditya Bakti, Bandung
- Siswanto, 2024, Principles of Banking Customer Prudence in Maintaining Business Security from Social Engineering Fraud, *Justiciable Journal*, University of Bojonegoro, Vol. 7 No. 1
- 1986, *Introduction to Legal Research*, University of Indonesia, Jakarta
- Sulistiyowati Irianto and Shidarta, 2011, *Legal Research Methods: Constellation and Reflection*, 2nd printing, Indonesian Obor Library Foundation, Jakarta
- Tabina Dea Anindya, 2023, Social Engineering Dangers Education Using Quizizz Learning Media to Increase Banking Customer Information Security Awareness, *Scientific Journal of Technology and Computers*, Vol. 4, No. 3, Udayana University,
- Trisadini, 2002, *Monetary and Banking System in Indonesia*, Gramedia Main Library, Jakarta
- Yogi Kristiyanto, et al., 2024, Impact of Social Engineering Attacks Case Study of Data Breach in Indonesia, Proceedings of Managerial and Entrepreneurship VIII, IPWIJA University
- The 1945 Constitution of the Republic of Indonesia
- Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking
- Law Number 21 of 2008 concerning Islamic Banking
- Law Number 1 of 2023 concerning the Criminal Code
- Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector
- Bank Indonesia Regulation Number 3 of 2023 concerning Bank Indonesia Consumer Protection