Eduvest – Journal of Universal Studies
Volume 5 Number 8, August, 2025
p- ISSN 2775-3735- e-ISSN 2775-3727

Fraud Crime in Banking Using Social Engineering and Trickery Techniques

Prasta Rully Andika, Nuraliah Ali, Rizki Setyobowo Sangalang
Universitas Palangka Raya, Indonesia
Email: pangpetoy@gmail.com, nuraliahali@law.upr.ac.id, rizkisetyobowo@law.upr.ac.id

ABSTRACT

The rise of social engineering techniques in banking fraud poses significant threats to financial security and customer trust. This study examines the criminal liability for fraud committed against banking customers using social engineering and trickery methods, focusing on psychological manipulation and deception to obtain sensitive information. Employing a normative legal research approach, the study analyzes Indonesian criminal law, including Article 378 of the Criminal Code and the ITE Law, to assess regulatory frameworks and enforcement mechanisms. Findings reveal that social engineering fraud, such as phishing and identity spoofing, exploits human vulnerabilities, leading to substantial financial losses and reputational damage. The research highlights gaps in legal protections for victims and emphasizes the need for stricter regulations and enhanced public awareness to combat these crimes. Implications suggest that banks and policymakers must adopt proactive measures, including advanced cybersecurity protocols and customer education, to mitigate risks. Strengthening law enforcement and victim restitution mechanisms is also critical to deterring perpetrators and ensuring justice.

KEYWORDS *Customer, Fraud, Social Engineering*

INTRODUCTION

Today, the world has developed in such a way that it has caused many changes in the order ranging from the rapid development of technology and industry to social and cultural in society (Silva & et al., 2019). This also causes changes in patterns and techniques in committing crimes. As will then be discussed, Social Engineering is a threat that is often ignored but can be exploited at any time, to take advantage of weaknesses in a security network, namely humans or users of the system itself (Allen, 2011). Where in the past humans or users were considered the weakest part of a network's security, as there is an expression and a principle that reads that the strength of a chain depends on or lies on the weakest connection or in foreign languages is better known as the principle of the strength of a chain depends on the weakest link (Indrajit, 2013).

In the article submitted by Richardus Eko Indrajit, there is an explanation that the strength of a chain is based on the weakest link (Eisenstein et al., 2019; Andersen & McAteer, 2020). Furthermore, the weakest chain in a network system is called Human (Smith et al., 2018; He et al., 2021). Even if a system is protected with advanced hardware and software to ward off all kinds of attacks as is common in electronic systems such as Viruses, IDS/IPS, Hacking, and so on, the device will not be able to protect itself from human manipulation or negligence by the humans who operate it (Harrison et al., 2017; Xu & Lee, 2020; Yu et al., 2021).

Social engineering or in Indonesian known as Social Engineering can also be called human hacking, as the name implies, is a hacking technique that is carried out on human targets by manipulating their emotions, thoughts, and psychology so that they voluntarily leak important information. Social engineering is also a very serious threat even in the banking sphere because the impact will be very detrimental ranging from financial losses, destruction of reputations and laws for banks and their customers.

Social engineering is a term used for various crimes committed by utilizing interaction with humans. This technique uses psychological manipulation to trick victims into making security mistakes and providing sensitive information. Social engineering is also often used by hackers to get important information because they understand that humans or users are the weakest chain in the network security system. Even though the programmer has built a good security system*, if it is operated by incompetent users, the system can still be easily attacked by hackers (Safitri et al., 2020).

Social Engineering in another sense can also be interpreted as an effort to carry out social transformation either in a planned manner in an opportunity to realize a goal that is carried out. This term certainly has a broad and pragmatic meaning, but the object remains the same, namely society so that it then makes society a social order that will be engineered against it. Less and Presley, sociologists, define social engineering as an effort that contains elements of planning, which are implemented until they are actualized in real life (Rahmat, 1999).

According to historical reviews, the emergence of the term social engineering was when the new order regime was at the height of its tyranny around 1986. Social engineering is social planning that leads to social transformation, supported by the internalization of high humanization values. Often we interpret engineering as a negative effort, this is because we are trapped in a situation of power or the practical activities of engineering are carried out by political elites who have the goal of personal interests or certain groups.

However, Jalaludin Rahmat brings a new nuance about the meaning of the term towards positive changes (transformation) that ultimately overcome various social problems that arise. And there's one interesting thing that a change won't happen when we're still stuck in a misconception. This means that human resources are one of the core forces for change, because social change occurs naturally or it can be in an undesirable direction, Social transformation emphasizes more on changes towards a better quality of life or changes towards a just, democratic, and egalitarian society (Dhakiri, 2000).

It is adapted from Kaspersky.com that social engineering is a manipulation technique that takes advantage of human error to gain access to personal information or valuable data. In the world of cybercrime, this type of fraud can lure users to be suspicious even users can easily reveal data, spread malware infections and provide access to guarded systems (Kaspersky Officer, 2022).

Attacks like this can happen online *, in person, and through other interactions that are difficult to predict. Generally, social engineering has two specific goals, namely to sabotage and steal. Since this deception is based on psychological manipulation, the attack strategy will be built on the way the victim thinks and acts. Thus this psychological manipulation is very useful to trick and influence the behavior of the victim (Kaspersky Officer, 2022).

The development of telecommunications and informatics technology is triggered by fierce competition that always gives birth to various innovations and leaps in telematics technology. This of course greatly affects business patterns and strategies, including the banking industry. Diversity of services, convenience, speed and very cheap service prices are very common demands from customers.

Information is one of the valuable assets for an organization so a company will go to great lengths to protect the information they have using advanced security systems. In the banking sphere, the development of information technology has made banking businesses

expand their services into the digital realm that turns manual transactions into technology-based transactions. This is characterized by the procurement of e-banking, mobile banking, and internet banking services. With this digitalization, banking institutions are encouraged to prioritize trust, efficiency, and service quality factors to always reorganize their businesses by implementing high-level security systems such as updating computer systems, implementing strong encryption, and creating complex computer programs to ensure the security and smooth running of operational systems (Anindya, 2021).

To ensure the smooth and secure of the operational system, banking institutions implement a security system that is balanced with the sophistication of the technology applied. The way to prevent potential interference and attacks on the security of computer systems is to implement complex computer programs and systems that provide security guarantees. Computer system upgrades and high-level data encryption are common solutions to problems that may occur. Not only the potential risks related to technology but other risks have also been taken into account (Junaedi, 2017).

Risk in the context of banking is a potential event, both anticipated and unanticipated that has a negative impact on the Bank's income and capital. All forms of potential risks have been taken into account by banking institutions. In fact, Bank Indonesia as the central bank has regulated in SE BI No.13/23/DPNP dated October 25, 2013 has regulated Risk Management, namely the adequacy of procedures and methods used in identifying, measuring, monitoring, and controlling risks arising from bank business activities so that they can remain manageable at limits that are still acceptable (risk appetite banks) and profitable (Junaedi, 2017).

The high security wall in banking makes the vulnerability gap created too small for hackers to hack using hacking techniques in general, causing hackers to carry out direct attacks on human targets using social engineering methods. Social engineering is also a very serious threat to the banking sphere because the impact caused will be very detrimental, ranging from financial losses, reputational and legal destruction for banks and their customers (Anindya, 2021).

As has happened, it was quoted from idxchannel.com that there was a customer money of one of the state-owned banks in Pangkalan Bun, Central Kalimantan due to fraud using social engineering. This is because the customer provides personal and confidential banking data to other parties. The total loss of the victim, who is also a senior doctor in East Kotawaringin Regency, reached 274 million rupiah on June 6, 2022. The Bank also urges customers to be more careful not to provide confidential information on personal data and banking data to other people or parties on behalf of the Bank (Dzakwan, 2022).

In this case, of course, it can be suspected of committing a Criminal Act in the form of Fraud which in its own rules has been regulated in Article 378 of the Criminal Code with the following rules:

> *"Whoever, with the intention to unlawfully benefit himself or others, by using a false name or false dignity, by deception, or a series of lies, induces another person to hand over something to him, or to give a debt or to write off the receivables is threatened with fraud with imprisonment for a maximum of four years".*

In banking itself, *social engineering* is often used to take personal information data to steal money in accounts, take over accounts, or misuse customers' personal data. Departing from these problems, this study will identify *social engineering* acts that are often carried out in the banking sphere by analyzing and studying problems that have occurred as well as finding out the extent to which criminal regulation in Indonesia regulates this *social engineering.* Because in its scope it is still not possible to find criminal responsibility from the perpetrator and a vacuum in norms has been found regarding the criminal act committed by the perpetrator.

In this study, it will explain the regulation of criminal liability in the criminal act of fraud of banking customers using Social Engineering techniques as well as the criminal law regulations in Indonesia.

RESEARCH METHOD

This legal writing research uses a normative type of legal research, which is a research approach that is carried out based on the main legal materials by examining theories, concepts, legal principles and laws and regulations related to this research. This legal research method examines normative law that focuses on regulations regarding Fraud Crimes using *Social Engineering* methods in Indonesia and the motives of the treatment of fraud committed by fraudsters, especially banking customers.

The approach methods used in this study are the *Conceptual Approach* and also the *Statute Approach*, which are then analyzed by *the Desriptive Analysis* method with the aim of producing a new prescriptive that can be applied in law enforcement.

RESULT AND DISCUSSION

Definition of language and terms *Social Engineering and Trickery*

In its sense, the term social comes from the English word "social" meaning "society", while in the term social it is (HarperCollins, 1991):

> *"1. of certain species of insect and animal species, including humankind. Living together in organized colonies or group. 2. Pertaining. 3. concerned with responsibility for the mutual relation and welfare of individuals. For example, social worker."*

Human beings as social beings are often faced with the problems mentioned above, especially discussing the concept of human beings living together and organized as a species and group that needs each other and is responsible for mutually beneficial relationships as an example of work.. According to Philip Kotler, social problems are certain conditions in the social order that are considered not in accordance with norms and disturb members of society, both individuals and groups, and can be reduced or eliminated through joint (collective) efforts.

However, humans are often considered the weakest component in a computer network system. Even if a system is protected with advanced hardware and software to ward off attacks such as firewalls, anti-viruses, IDS/IPS, and so on, if the humans who operate it are careless, then the whole equipment becomes meaningless. Cybercriminals are so aware of this that they use *social engineering* to obtain important information that is kept secret by humans for specific purposes.

Social engineering is a technique of stealing or taking important/crucial/confidential data or information from a person by using a humane approach through social interaction mechanisms. Or in other words, Social engineering is a technique of obtaining confidential data/information by exploiting human weaknesses (Indrajit, 2022). According to Jalaluddin Rakhmat, social engineering is the theft or taking of important/crucial/confidential information from a person by using a humane approach through social interaction mechanisms. Or in other words, social engineering is a technique of obtaining confidential data/information by exploiting human weaknesses (Rakhmat, 1999).

In *social engineering*, the perpetrator takes advantage of the natural nature of humans. This means that how human nature can be known and learned is also used for certain purposes. There are many methods used by criminals in launching their businesses in order to get what they want. It is usually done by taking advantage of the psychological side such as praising, being friendly, doing something excessive to get closer to the target such as giving something that can make the victim feel happy and happy, or by persuading.

There are many ways that perpetrators can play on the target's emotions so that they will unknowingly provide confidential information. In *social engineering,* there are several common patterns that hackers commonly do, including:

1. Collecting information, Information can be in the form of organizational structure and a list of names in it, birthday dates, and so on to develop relationships with the target.
2. Develop relationships/relationships, After getting enough information, the next step is to try to approach one of the employees who has been targeted. The information that has been obtained is used to gain trust from the target.
3. Exploiting, After gaining the trust of the targeted person, the next step is to exploit the information that has been obtained to enter the company's system.
4. Execution, After successfully entering the system, the hacker can easily steal, alter, and even damage the system and data without being hindered by the security system.

Most social *engineering attacks* will rely on actual communication between the attacker and the victim. Attackers will typically motivate victims to compromise, rather than using sophisticated methods and equipment to breach their *cybersecurity*. The way the attack works is also very structured and not messy. According to *CSO Online*, the way *Social engineering* works is as follows (Fruhlinger, 2022):

a. The attacker plans the strategy by gathering information about the victim's background and workplace;
b. Infiltrating by establishing a relationship or initiating an interaction, starts with building the victim's trust;
c. Exploit the victim once trust is formed and their weaknesses are visible; and
d. Disconnect after the kobran performs the desired action.

This process can take place in a single email interaction or for months in a series of chats on social media. However, in the end, the attack will end after the victim performs the actions that the attacker expects. It's like sharing personal information or exposing *malware* to their *device*'s system . Social *engineering* attacks also come in many forms, and can be carried out anywhere where human interaction is involved.

Fraud Crimes against Banking Customers using *Social Engineering and Trickery techniques*.

Criminal acts are acts that do or do not do something that is declared by laws and regulations as prohibited and threatened with criminal penalties (Arif, 2008). Criminal acts are a basic definition in criminal law (*normative juridical).* A crime or evil act can be interpreted juridically or criminalologically. Crime or evil act in the normative juridical sense is an act of

deed as manifested in criminal regulations. Meanwhile, crime in a criminological sense is a human act that violates the norms that live in society concretely.

Regarding the definition of criminal acts (*strafbaar feit*), one of the scholars expressed his opinion, namely Pompe gave the definition of criminal acts into 2 (two) definitions, namely:

a) The definition according to theory is a violation of norms, committed because of the fault of the violator and threatened with criminal penalties to maintain the rule of law and save the public welfare (Andrisman, 2011).
b) The definition according to positive law is an event/*fact* that is formulated by the laws and regulations as an act that can be punished:

Simons defines a criminal act as an act (handeling) that is threatened with criminal punishment by the law, contrary to the law (*onrechtmatig*) committed by mistake (*schuld*) by someone who is able to be responsible. The formulation of the definition of a criminal act by simons is seen as a complete formulation because it will include (Wiyanto, 2012):

a) Criminally threatened by the law;
b) Against the law;
c) Committed by someone with guilt (*schuld*);

Andi Hamzah gave an explanation of criminal acts as follows, Criminal acts are human behaviors formulated in laws against the law, which should be punished and committed with mistakes. The person who commits a criminal act will be held criminally accountable if the perpetrator has a mistake, a person has a mistake if at the time of committing the act seen from the perspective of society shows a normative view of the offense committed (Hamzah, 2001).

According to Moeljatno, criminal acts are acts that are prohibited by a law, which prohibition along with threats (sanctions) in the form of certain penalties, for anyone who violates these rules (Rosidah, 2011).

The crime of fraud or "*fraud*" contained in Articles 378-395 of the Criminal Code Chapter XXV is fraud in a broad sense, while Article 378 of the Criminal Code mentions the term *"oplichting"* which has the meaning of fraud in a narrow sense. From an Indonesian point of view, the word fraud is an adjective of the root word deception, which gets a prefix and a suffix so that it becomes a fraud, which means a person who commits an act of fraud or the subject of the perpetrator (Ananda, 2009).

In general form, fraud is contained in Article 378 of the Criminal Code, which is as follows:

> *"Whoever with the intention of benefiting himself or others by going against his rights, either by using a false name or a false state, either by reason and deceit, or by fabricating false words, persuading people to give away goods, making debts or writing off debts, shall be punished for fraud."*

Then it is also explained that in the case of fraud law is known as *zwenelarij* or *swindling* by giving the following meaning (Puspa, n.d.):

> "*The act of persuading to give an item, canceling debts, writing off receivables unlawfully using a false name, the purpose of benefiting oneself is a criminal act or crime for which the perpetrator can be prosecuted or prosecuted*".

Fraud itself basically always begins with persuasive acts by using false words so that they can easily gain the trust of the person they are persuaded by. Fraud comes from the word

deception which means dishonest or lying deeds or words, false and so on with the intention of misleading, outsmarting or seeking profit. An act of fraud is an act that harms others so that it is included in the action that can be subject to criminal penalties.

In the Criminal Code, precisely in Article 378 of the Criminal Code, the crime of fraud (*oplichthing*) is stipulated in general form, while those listed in Chapter XXV of Book II of the Criminal Code, contain various forms of fraud against property formulated in several articles, each of which has special names (fraud in a special form). The entire article in Chapter XXV is known as bedrog or fraudulent acts.

The definition of fraud according to the opinion mentioned above clearly appears that what is meant by fraud is a trick or a series of lying words so that a person feels deceived because of what seems to be true. Usually a person who commits fraud, is to explain something that seems to be true or happens, but in fact his words are not in accordance with reality, because the purpose is only to convince the person who is being targeted to follow his wishes, while using a false name so that the identity of the person concerned is not known, as well as using a false position so that people are sure of his words.

Fraud itself among the public is a very reprehensible act but rarely from the perpetrators of these crimes is not reported to the police. A small fraud where the victim does not report it makes the fraudster continue to develop his actions which in the end the fraud perpetrator becomes a large-scale fraudster.

Because it uses electronic media, it should also be noted that there are times when the use of Law Number 11 of 2008 concerning Electronic Transaction Information (hereinafter abbreviated as the ITE Law) which regulates in article 28 paragraph (1) as follows:

(1) Everyone deliberately and without rights spreads false and misleading news that results in consumer losses in Electronic Transactions.

And in the Criminal provisions of the ITE Law which is regulated in article 45 paragraph (2) regulates criminal sanctions in article 28 paragraph (1), which are as follows:

(2) Every person who meets the elements as referred to in Article 28 paragraph (1) or paragraph (2) shall be sentenced to a maximum of 6 (six) years in prison and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah).

Next is an explanation of the Customer, the Customer is a customer (*customer*), namely an individual or company that gets benefits or products and services from a banking company, including purchasing, leasing and service activities (Nasution & Sutisna, 2015). According to Article 1 paragraph (17) of Law No. 10 of 1998, the customer is "Parties who use bank services." Customers have an important role in the banking industry, where the funds that customers save in banks are the most important funds in the bank's operations to run their business. The definition of customer, according to experts, is as conveyed by the following experts, according to Kasmir, "Customers are consumers who buy or use products sold or offered by banks" (Koeswara, 2013).

According to Saladin, customers are "Consumers as providers of funds" (Jupitri & Sari, 2012), while according to Tjiptono the definition of customer is "Everyone who buys and uses the company's products or services". And according to Komaruddin, a customer is "A person or a company that has a bank statement, deposit or other similar savings account" (Wiryaningtyas, 2016). From this understanding, it can be concluded that a customer is a person

or a corporate business entity that has a deposit and loan account and conducts these deposit and loan transactions with a bank.

In the law's own view, a criminal or perpetrator of a crime is someone who is considered to have violated the rules of the law and needs to be sentenced. However, it is also necessary to know about the measures that determine whether a person can be treated as a criminal or not. Criminality comes from the word "*crimen*" which means crime (Hiariej, 2016). The definition of criminality according to language is the same as crime, namely a crime that can be punished according to the law, while the definition of criminality according to the term is interpreted as a crime that is classified as a violation of positive law (the law that applies in a country).

Modus operandi includes various things, such as the strategies used in planning crimes, the tools or methods chosen to carry out criminal acts, and tactics used to avoid detection or arrest by the authorities. Each criminal may have a unique modus operandi , which they design based on their experience, knowledge, and skills (Dirjosisworo, 2016).

The perpetrators of fraud crimes with social engineering techniques use various modus operandi to steal sensitive information and manipulate victims. Some of the modus operandi that are generally used, according to Dhull & Hooda, *Social engineering* techniques are divided into two types as follows (Dhull & Hooda, 2016):

1. Based on social interaction, it means that the perpetrator is in direct contact with his target through social interaction where the perpetrator has direct social interaction with his target to steal information or manipulate the target. Techniques that fall into this type include:
   a. *Shoulder surfing*
      Shoulder surfing, is done by standing next to the target to steal personal data. For example, stalking the target ATM PIN. The *shoulder surfing* technique is done by standing next to the target to steal personal information. An example is stealing an ATM PIN from a target.
   b. *Hoaxing*
      Providing false information by convincing the target so that the target believes and enters the crime trap. Hoaxing techniques are carried out by providing false information and convincing the target to take certain actions so that the target is caught in a crime.
   c. *Tailgating*
      Tailgating, perpetrators gain access by stalking individuals who have legal access.
      The tailgating technique is carried out by stalking individuals who have legal access to gain access to a place or system.
   d. *Creating Confusion*
      The perpetrator creates confusing things and takes advantage of the situation.
      The technique of creating confusion is carried out by creating confusing situations and using them to commit crimes.
   e. *Dumpster Diving*
      This technique is carried out by searching for information on discarded document waste.

The dumpster diving technique is carried out by looking for important information in the garbage or documents that have been discarded.

f. *Impersonation*
   This technique is done by impersonating identities/disguising themselves to gain legal access to computer systems or networks.
   The impersonation technique is done by impersonating or impersonating someone else to gain legal access to a system or network.

g. *Reverse Social Engineering*
   Manipulate goals by offering help that benefits the goal.
   The reverse *social engineering* technique is carried out by manipulating the target by offering help that actually provides benefits to the perpetrator.

2. Computer interaction-based, meaning that the perpetrator uses a computer to gather the necessary information. The second type of *social engineering* technique, where the perpetrator uses a computer to collect information from his target.
   a. *Pop-up windows*
      This technique is done by appearing a small pop-up window on the target computer screen that contains fake messages or attractive offers that trick users into clicking on a link or filling in the personal information requested.
   b. *E-mail attachment*
      The perpetrator sends an email containing attachments that may contain malware to spy on the target computer. When the user clicks on the attachment, malware will be installed and take over the user's computer system.
   c. *Phishing*
      It is done by deceiving users into revealing their personal information. It is usually done by sending an email on behalf of a trusted company or institution that asks users to fill out the requested personal data form. The perpetrators will then use the information obtained for their own interests, such as taking over accounts or conducting financial transactions without the user's permission.
   d. *Fire Spoofing*
      The perpetrators create fake websites that mimic the look and name of well-known brands to trick users. These fake websites are then disseminated randomly in the hope of getting interested and unsuspecting targets. When users visit such fake websites, they will be asked to disclose personal information that can be leveraged by the perpetrators.
   e. *Baiting*
      The perpetrator provides a bait or trick that attracts the user's attention, such as free devices or other offers. When users take such feeds, they can fall victim to eavesdropping or hacking of confidential data by the perpetrators.

Regulation of Fraud Crimes with *Social Engineering and Trickery* Techniques against Banking Customers in Criminal Law in Indonesia

In Article 1 number 8 of Law of the Republic of Indonesia Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning Victim Witness Protection, it

is explained that "protection" refers to all efforts made to fulfill the rights and provide assistance to witnesses and/or victims in order to provide a sense of security, and must be carried out by the Witness and Victim Protection Institute (LPSK) or other institutions in accordance with the provisions of this Law.

Article 1 Number 8 of Law of the Republic of Indonesia Number 31 of 2014 concerning Amendments to Law Number 13 of 2006 concerning the Protection of Witnesses and Victims, explains that "protection" includes various actions that aim to fulfill rights and provide assistance to witnesses and/or victims, in order to provide a sense of security. The Witness and Victim Protection Agency (LPSK) or other institutions in accordance with the provisions of this Law are responsible for carrying out such protection measures. This Article also states that witnesses and/or victims have the right to receive assistance and protection.

In the regulation of the Indonesian Criminal Law in Article 378 of the Criminal Code (KUHP) regulates legal protection for Bank customers who are victims of data theft. The article states that a person who, with the intention of unlawfully benefiting himself or others, commits fraud by using a false name or false dignity, by deception, or a series of lies, which induces another person to hand over goods or to give a debt or to write off receivables, may be punished with imprisonment for four years.

In addition, there are also regulations regarding *Social Engineering* in Law No. 11 of 2008 concerning Information and Electronic Transactions which in the regulation in Article 30 reads as follows:

(3) Each Person knowingly and without rights or unlawfully accesses the Computer and/or Electronic System of another Person in any way.
(4) Any Person knowingly and without rights or unlawfully accesses the Computer and/or Electronic System in any way for the purpose of obtaining Electronic Information and/or Electronic Documents.
(5) Any Person knowingly and without rights or unlawfully accesses the Computer and/or Electronic System in any way by breaching, breaking through, exceeding, or breaking into the security system.

Then it is also explained in Article 36 of the same Law that Every Person deliberately and without rights or against the law commits an act as referred to in Articles 27 to 34 that results in losses to Others. So it is clear that *social engineering* acts are criminal offenses that can be included after fraud or theft.

The case of theft of bank customer data using *the social engineering* mode shows that customers who are victims of these crimes are entitled to legal protection and assistance as victims of criminal acts. The majority of victims of banking crimes are those who are directly involved in various banking activities (Sholehuddin, 1997).

Article 1 number 9 and number 10 of the Law explain the form of protection that can be given. Article 1 number 9 explains that compensation is compensation provided by the state if the perpetrator is unable to provide full compensation to the victim or his family. Meanwhile, Article 1 number 10 explains that restitution is compensation given to the victim or his family by the perpetrator or a third party.

In the context of the case of data theft of Bank customers, whether it is using *the Social engineering* method, based on the explanation of the Article, customers who are victims of data

theft and suffer losses to their balances are entitled to legal protection in the form of compensation or restitution from the bank other than the perpetrator who is charged with fraud.

The development of technology has brought rapid changes in our lives. These advancements have affected various aspects of life, including business. In business, technology allows access to information remotely and allows transactions to be conducted online without the need for face-to-face. However, behind the benefits, the development of information technology also brings a new problem, namely the emergence of sophisticated crimes known as *cybercrime* or *cybercrime*. These crimes occur through the use of computer and telecommunications technologies, and allow perpetrators to carry out criminal activities anonymously and across national borders (Suhariyanto, 2012).

In an increasingly digitally connected society, cybercrime is a serious threat. These crimes include different types of activities such as online fraud, identity theft, cyberattacks, and the spread of illegal content. In a world that is increasingly dependent on information technology, protection against *cybercrime* is becoming increasingly important.

In response to these challenges, governments, law enforcement agencies, and the private sector have been working together to develop strategies and measures to address cybercrime. This includes increasing public understanding and awareness of *cybercrime threats*, improving the security of technology systems and infrastructure, and implementing strict and effective laws to deal with cybercriminals.

In the face of cybercrime, it is also important for individuals to take proper preventive measures. This includes using strong passwords, avoiding clicking on links or downloading suspicious files, installing up-to-date security software, and being cautious about sharing personal information online.

Overall, the development of information technology brings great benefits to our lives, but it also presents new challenges in the form of cybercrime. With cooperation between governments, law enforcement agencies, the private sector, and individuals, we can work together to prevent and address these cybercrimes , as well as maintain the security and integrity of our digital world. Fraud with *social engineering* mode is a challenge in tackling crime in the digital era.

CONCLUSION

The mode of *social engineering and trickery* fraud against banking customers in Indonesia is increasingly complex. The modes vary from daily needs to earning deep profits. One common technique is phishing, where perpetrators create fake websites or send fake messages that resemble banks to steal sensitive information. The perpetrator can also request confidential information via phone or text message by claiming to be a bank or financial institution. They also use identity spoofing or social fraud to trick victims and gain access to accounts or personal information.

In criminal law in Indonesia, the crime of fraud with *social engineering* techniques against banking customers can be charged with Article 378 of the Criminal Code which regulates fraud. Fraudsters can be subject to criminal sanctions in the form of prison sentences and fines. In addition, banks can also take civil legal action against fraudsters to claim compensation for losses suffered by customers.

REFERENCES

Allen, M. (2011). Social engineering: A means to violate a computer system. SANS. http://www.sans.org/reading_room/whitepapers/engineering/

Ananda. (2009). Kamus besar Indonesian. Kartika.

Andersen, C., & McAteer, C. (2020). Understanding the human factor in cybersecurity: From awareness to behavior. Journal of Cybersecurity, 9(1), 1–10. https://doi.org/10.1093/cybsec/tyz029

Andrisman, T. (2011). Principles and basics of general rules of Indonesian criminal law. University of Lampung.

Anindya, T. D. (2021). Identification and prevention of social engineering crimes in the banking scope.

Arif, B. N. (2008). Bunga potpourri criminal law policy development of the drafting of the new criminal code concept. Kencana Prenada Media Group.

Dhakiri, M. H. (2000). Paulo Freire, Islam and liberation. Djambatan.

Dhull, R., & Hooda, S. S. (2016). Contrast study of social engineering techniques. IOSR Journal of Computer Engineering, 18(4), 66–68.

Dirjosisworo. (2016). Scope of criminology.

Dzakwan, S. (2022, August 13). Customer money in Pangkalan Bun raib soceng victim, here's the chronology. IDX Channel. https://www.idxchannel.com/banking/uang-nasabah-di-pangkalan-bun-raib-korban-soceng-ini-kronologi

Eisenstein, D., Sun, J., & Bell, S. (2019). The human element: Why cybersecurity strategies must address human vulnerabilities. Computers & Security, 87, 50–67. https://doi.org/10.1016/j.cose.2019.04.004

Fruhlinger, J. (2022). Social engineering: Definition, examples, and techniques. CSO Online. https://www.csoonline.com/article/3648654/social-engineering-definition-examples-and-techniques.html

Hamzah, A. (2001). Bunga potpourri of criminal law and criminal proceedings. Ghalia Indonesia.

Harrison, J., Stone, R., & Williams, L. (2017). Human error in cybersecurity: The role of organizational culture. Journal of Information Security, 8(4), 239–251. https://doi.org/10.1016/j.jisec.2017.08.002

He, Z., Wang, L., & Zhou, T. (2021). Addressing human factors in cybersecurity: A survey of user behavior and risk perception. Future Generation Computer Systems, 114, 229–241. https://doi.org/10.1016/j.future.2020.08.019

Silva, C., & et al. (2019). Application of machine learning techniques for predicting pipeline failures in the oil and gas industry. *Reliability Engineering \& System Safety*, *188*, 277–289.

Smith, J. R., Johnson, S. D., & Peters, L. (2018). The weakest link: Human vulnerabilities in the cybersecurity chain. International Journal of Information Management, 43, 17–28. https://doi.org/10.1016/j.ijinfomgt.2018.05.009

Xu, W., & Lee, Y. (2020). Human negligence in cybersecurity: Risks and countermeasures. Journal of Cybersecurity and Privacy, 1(2), 56–72. https://doi.org/10.3934/jcp.2020.2.56

Yu, K., Chen, L., & Liu, T. (2021). Human factors in cybersecurity: A framework for mitigating risks through user education. Computers & Security, 100, 102089. https://doi.org/10.1016/j.cose.2020.102089