MASALAH-MASALAH HUKUM
Available online on https://ejournal.undip.ac.id/index.php/mmh/
Volume 54, Issue 2, July 2025

STRENGTHENING LEGAL PROTECTIONS AGAINST SOCIAL ENGINEERING IN DIGITAL BANKING: CHALLENGES, GAPS, AND RECOMMENDATIONS

Putu Devi Yustisia Utami*, Ni Putu Purwanti
Faculty of Law, Universitas Udayana, Denpasar, Indonesia
*deviyustisia@unud.ac.id

Abstract

Social engineering is a form of manipulation used by malicious actors in digital banking services, exploiting social interaction mechanisms that can lead to financial losses for customers. Under Article 55 of the Financial Services Authority Regulation on Consumer Protection, financial institutions are obligated to safeguard customer funds. However, these protections often fail during social engineering incidents. This study utilizes both normative and empirical legal research methods to analyze common social engineering schemes, such as the distribution of APK files containing malware, phishing, pretexting, baiting, and quid pro quo. Consumer protection in the banking sector is regulated by several legal instruments, including the Consumer Protection Act, Financial Sector Development and Strengthening Act, and Financial Services Authority Regulation on Consumer Protection. Although these frameworks include fundamental consumer protection principles, they are inadequate in addressing the specific needs of customers affected by social engineering. Legal remedies for affected customers include filing complaints with banks or the Financial Services Authority, and pursuing litigation following fraud reports to the police, as stated in Article 378 of the Indonesian Criminal Code. The study recommends that the government issue more detailed implementing regulations under the Financial Services Authority's Consumer Protection framework to provide effective legal remedies for victims. Additionally, banks should implement financial literacy programs, and customers should exercise caution to avoid disclosing sensitive information in digital banking services.

Keywords: Social Engineering; Digital Banking; Consumer Protection; Fraud Schemes; Financial Services.

A. Introduction

In the digitalization era, the use of electronic media and internet-based technologies has become an integral part of societal activities, including in the financial and banking sectors (Meyer et al., 2023; Natalis & Djohan, 2025; Xia et al., 2024). The provision of banking services has evolved beyond conventional, in-person transactions to include electronic and digital services. This transformation has significantly improved access to financial services, offering the public, particularly banking customers, greater efficiency and convenience in conducting transactions (Martinelli, 2021). According to the Financial Services Authority No. 21 of 2023 concerning Digital Services by Commercial Banks (hereinafter referred to as Financial Services Authority No. 21/2023), digital services are defined as banking products and services that utilize information technology and electronic media, enabling customers to independently access banking services. Various forms of digital banking services offered by banks include electronic banking, mobile banking, SMS banking, Quick Response Code Indonesian Standard (QRIS), and digital banks (Atmaja & Paulus, 2022). However, the convenience of digital banking services comes with

unavoidable risks. The use of internet-based systems in digital banking creates opportunities for malicious actors to exploit technology, the internet, and customers' personal data (Mishra et al., 2022; Rakocevic et al., 2025). Common forms of cybercrime in the banking sector include skimming, phishing, spoofing, hacking customers' email accounts, and breaches targeting official banking institution websites.

Currently, a prevalent modus operandi in banking services is Social Engineering, which results in financial losses for consumers (Yuspin et al., 2024). According to (Indrajit & Teknik, 2017), social engineering (commonly abbreviated as Soceng) is a technique used to steal or obtain critical data and information through social interaction by exploiting human factors. This means that confidential data or information is illicitly acquired by manipulating human vulnerabilities, such as inducing trust, fear, or a desire to help.

In relation to digital banking services, the government has issued Financial Services Authority Regulation No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector (hereinafter referred to as Financial Services Authority Regulation No. 22/2023). Article 55, paragraph (1) stipulates that financial service institutions are obligated to safeguard the security of consumers' funds and/or assets under their responsibility (*das sollen*). However, in practice, despite the existence of this legal regulation, customer deposits in banks are often not adequately protected as intended (*das sein*). One notable case involved a customer of a state-owned commercial bank, who experienced fund depletion in their account without conducting any purchase or transaction. A similar incident occurred with a customer of a regionally-owned commercial bank, who lost funds after clicking on a link from a fraudulent customer service source. This phenomenon highlights a gap between the existing regulations in Indonesia (*das sollen*) and the social realities experienced by the community (*das sein*). This issue demands serious attention from both banks and consumers, given the increasing sophistication of digital banking fraud schemes, which inevitably lead to financial losses for customers.

Previous research by Ratulangi (2021) titled "*Cyber Crime Offenses in Banking Activities*" examined various cybercrimes in the banking sector, with a primary focus on criminal law aspects. Subsequently, Siswanto & Lenita (2024) conducted a study entitled "*The Principle of Prudence of Banking Customers in Safeguarding Business Security against Social Engineering Fraud*," which emphasized the application of the prudence principle in anticipating social engineering fraud. Both studies primarily focused on criminal offenses in banking, whereas the present research concentrates on consumer protection within the financial services sector of banking. The author had previously published an article titled "*Digital-Based Financial Education and Literacy: Its Implementation in Preventing Social Engineering Schemes in the Digital Banking Sector,*" which focused on the factors contributing to social engineering and the implementation of financial education and literacy by banks and the Financial Services Authority as preventive measures against social engineering in the banking sector (Utami et al., 2025). The current study serves as a continuation of the author's prior research, further examining the regulatory framework for consumer protection in the banking sector and specifically exploring the legal remedies available to customers who suffer losses due to social engineering schemes.

This study focuses on addressing the following research problems: what are the common forms of social engineering schemes encountered by customers using digital banking services, how is consumer protection regulated for victims of social engineering schemes based on Indonesian law and regulations, and what legal remedies are available for customers who suffer losses as a form of legal protection against social engineering schemes. The objectives of this research are to identify the types of social engineering schemes encountered by customers of digital banking services, to analyze the regulatory framework for consumer protection concerning social engineering schemes under Indonesian legislation, and to understand the legal remedies available for customers who suffer losses as a form of legal protection against social engineering schemes.

B. Method

This study employs a mixed-methods approach, integrating both normative and empirical legal research methodologies to provide a comprehensive analysis of the issues at hand. The normative-empirical method combines doctrinal (library-based) research with field research, allowing for a balanced exploration of legal principles and practical realities. The doctrinal aspect focuses on a thorough examination of legal texts, such as statutes, regulations, and case law, to establish the theoretical framework for understanding consumer protection in the banking sector. On the other hand, the empirical component is designed to complement and validate the findings derived from normative analysis by incorporating real-world data obtained through fieldwork.

The empirical data collected during fieldwork serve to reinforce and contextualize the conclusions drawn from normative legal analysis, providing a deeper insight into the practical application of laws and regulations within the banking sector. This approach acknowledges the importance of both theoretical understanding and the lived experiences of those directly involved in the banking sector, offering a more nuanced perspective on consumer protection and the regulation of social engineering schemes in digital banking. By employing both statutory and factual approaches, the study aims to create a comprehensive picture that reflects not only the written laws but also the practical realities and challenges faced by banking institutions and their customers.

The research is guided by a descriptive-analytical orientation, which focuses on identifying and analyzing the various aspects of consumer protection in the banking sector. This approach allows for a detailed examination of the regulatory framework, legal remedies, and the role of banking institutions in safeguarding their customers from social engineering schemes. By describing the current state of legal protections and identifying gaps or challenges, the study seeks to contribute to the development of more effective consumer protection policies and practices within the banking sector.

Data collection for this study is carried out through two primary methods: a literature review and field interviews. The literature review involves a comprehensive analysis of academic articles, books, legal texts, and other relevant sources that provide a theoretical basis for understanding the regulatory environment in the banking sector. This review helps to establish a solid foundation for the normative analysis and allows the researcher to identify key issues and trends in the existing body of knowledge.

Field interviews, conducted at the Financial Services Authority Office in Bali Province and with representatives from various banking institutions, serve as the empirical component of the study. These interviews involve both state-owned and privately-owned commercial banks operating within the Province of Bali. Through these interviews, the researcher is able to gather firsthand insights from banking professionals, regulators, and other stakeholders involved in consumer protection and the prevention of social engineering schemes. The information gathered from these interviews helps to contextualize the legal findings and provides a more practical understanding of how regulations are implemented and enforced in the field.

C. Results and Discussion

1. Social Engineering in Digital Banking: Vulnerabilities, Methods, and Consumer Protection Challenges

The proliferation of financial products offered through digital banking services has enabled the public to conduct transactions more efficiently, eliminating the need for physical visits to the bank (Kaur et al., 2021; Tay et al., 2022). While this development represents a significant advancement in banking convenience, it also introduces substantial vulnerabilities. Digital banking platforms are increasingly susceptible to criminal exploitation, particularly in the form of sophisticated cyber-enabled fraud schemes targeting both customers and financial institutions

(Johannes Ibrahim et al., 2021) Various forms of criminal activity in the banking sector frequently target customers who utilize digital banking services. One notable type of banking-related crime is known as social engineering, a technique used to steal or obtain sensitive data and information by exploiting human psychology through interpersonal interaction. This method relies on manipulating individuals (rather than breaching technical system) by building trust or invoking emotional responses in order to gain unauthorized access to confidential information (Indrajit & Teknik, 2017). According to a report from economy.okezone.com as off 2023, the Financial Services Authority has received a total of 433 complaints related to external fraud, comprising scams, account breaches and social engineering schemes (Triamanda, 2022). This indicates that social engineering schemes occur frequently and inevitably result in losses for individuals who lack adequate understanding and have limited education regarding digital financial literacy.

Social engineering is a relatively new hacking technique that has gained significant traction due to its ability to exploit human vulnerabilities, making it easier for malicious actors to execute. Rather than targeting software weaknesses, social engineering focuses on manipulating individuals by triggering emotions like curiosity, trust, fear, or even the desire to help. These manipulations are carried out through electronic communications, often sent via smartphones, making it more accessible and harder to detect (Darmaningrat et al., 2022). The increasing dependence on digital platforms for everyday transactions and banking services makes individuals prime targets for social engineering schemes. Several common forms of these schemes have emerged, each relying on a unique method of deception to exploit users and gain access to their sensitive data.

One prevalent method is the distribution of APK files containing malware. In this form of social engineering, malicious software is hidden within applications or files that users are prompted to download. Once installed, the malware operates without the user's knowledge, often targeting mobile banking apps or other financial applications. The primary goal is to steal personal and financial data, such as login credentials and banking details, which can then be used for fraudulent purposes. This form of attack is particularly effective because it leverages the user's trust in seemingly harmless applications, allowing the malware to go undetected (Adenansi & Novarina, 2017; He et al., 2015; Jakobsson & Ramzan, 2008; Javadpour et al., 2024).

Phishing is another widely used social engineering technique. This method involves sending fraudulent messages, typically via email or social media applications, disguised as communications from trusted institutions, such as banks or online services. The messages often contain links to fake websites that mimic legitimate ones, prompting the recipient to click on them. Once the victim visits the site, they are tricked into disclosing sensitive information such as passwords, bank account numbers, and personal identification details. Phishing attacks can be highly convincing, especially when they use familiar branding and language, making it difficult for users to distinguish between legitimate and fraudulent communications (Butarbutar, 2023; Gallo et al., 2024; Hewage et al., 2021). As digital communication becomes more ingrained in everyday life, phishing attacks continue to evolve, becoming more sophisticated and harder to detect.

Pretexting is another form of social engineering that involves fabricating a false narrative to obtain targeted information. In this scenario, an attacker may impersonate a trusted figure, such as a bank representative, government official, or service provider, and convince the victim to share confidential information. For instance, an attacker could pose as a package delivery person and ask the victim to provide sensitive details under the pretense of confirming delivery information. By creating a fabricated story that appears legitimate, the attacker lowers the victim's guard, making it easier to extract valuable personal and financial data. This method relies on the attacker's ability to craft a believable and convincing narrative that prompts the victim to act without questioning the situation

Baiting is another manipulative tactic used in social engineering. This method involves enticing potential victims with promises of rewards, such as free gifts, access to exclusive content,

or monetary benefits. These offers are designed to capture the victim's attention and lead them to unknowingly disclose their personal information. In the context of banking, baiting often involves offering fake promotions, such as winning a large sum of money, in exchange for providing login credentials or other sensitive financial details. The promise of an attractive reward clouds the victim's judgment, leading them to fall into the trap set by the attacker. As with other social engineering techniques, baiting relies on exploiting the victim's emotions and desires to manipulate their actions (Silalahi et al., 2022).

Lastly, quid pro quo is a form of social engineering in which the attacker offers assistance or services to the victim, often by impersonating an authority figure, such as a bank customer service representative. In this scenario, the attacker might promise to resolve an issue, such as canceling a fee or refunding a transaction, in exchange for the victim's personal information. For example, an attacker might call a victim and claim to be from the bank, offering to help reverse an ATM transaction fee increase. However, in return, the attacker may ask for sensitive information, such as account numbers, passwords, or one-time passwords (OTPs). This technique takes advantage of the victim's lack of awareness about the risks of sharing such information and often results in significant financial losses when the attacker uses the stolen data for fraudulent transactions.

These various forms of social engineering are designed to exploit human weaknesses, often with devastating consequences. As digital banking becomes more prevalent, individuals must remain vigilant and aware of the risks posed by these manipulative tactics. Protecting personal and financial information requires not only technological safeguards but also an understanding of the psychological strategies used by attackers to gain unauthorized access to sensitive data.

2. Legal Protection Gaps for Banking Consumers in Social Engineering Schemes

In the context of legal protection for banking customers who fall victim to social engineering schemes, several statutory regulations may be deemed relevant (Airehrour et al., 2018; Purkait, 2012). Law No. 8 of 1999 concerning Consumer Protection, known as the Consumer Protection Law, provides general legal protection for consumers by regulating both consumer rights and the obligations of business actors. According to Article 4, consumers are entitled to comfort, security, and safety when consuming goods or services, as well as the right to express their opinions and complaints regarding the products or services used. In relation to the legal protection of banking customers, these provisions imply that customers are entitled to safety and comfort when utilizing banking products. The law guarantees consumer protection by affirming the right of consumers to voice opinions and complaints when they encounter issues or suffer losses in connection with banking services. However, while the Consumer Protection Law serves as the primary legislation governing consumer protection in Indonesia, it remains conventional and lacks adaptability to the digital developments in the banking sector. The law primarily addresses the relationship between business actors and consumers without adequately addressing the role of third parties that may infiltrate or compromise the products and services offered by these business actors. This includes third-party intrusions into digital banking services, such as those involved in social engineering schemes. Additionally, the Consumer Protection Law does not explicitly require business actors to implement personal data protection measures for consumers, nor does it establish responsive dispute resolution mechanisms specifically tailored to digital transactions, such as those that are increasingly common in digital banking services.

Law No. 4 of 2023 concerning the Development and Strengthening of the Financial Sector (Law No. 4/2023) regulates various aspects of the financial sector, including the banking industry. Chapter XVIII, Article 235, outlines the rights of consumers in the financial sector, which include the right to security when using financial products, the right to have their opinions and complaints regarding the products they use heard, the right to receive advocacy, protection, and access to consumer dispute resolution mechanisms, and the right to financial education. In the context of digital banking services, Law No. 4/2023 recognizes the consumer's right to security when using

banking products and guarantees the right to financial education to help consumers make informed and responsible use of banking services. However, this law does not yet provide adequate regulatory provisions to protect customers who suffer losses arising from the use of digital banking services, particularly in cases involving social engineering schemes. While Article 239 addresses consumer data protection, its scope remains insufficient, especially in cases involving the misuse of data by third parties. Moreover, the law does not clearly establish the liability of financial service institutions in cases where inadequate banking security systems allow perpetrators to carry out social engineering schemes. This legal gap weakens the position of consumers when seeking accountability and redress after suffering losses from such incidents.

Financial Services Authority Regulation (POJK) No. 22 of 2023 concerning Consumer and Public Protection in the Financial Services Sector also offers important protections for banking consumers (Wiedyasari & Yuspin, 2024). Article 24(1) mandates that financial service providers ensure system security and cyber information resilience to protect consumers. This regulation aims to protect banking consumers by requiring financial institutions to use reliable technology that is not easily compromised by unauthorized parties, including those using social engineering schemes. However, despite these provisions, social engineering remains a significant threat and continues to cause financial losses for victims. Regarding liability, Article 10(1) and (2) of the Financial Services Authority Regulation No. 22/2023 state that if losses are caused by negligence, errors, or unlawful acts committed by the bank or its representatives, the financial service institution is responsible for the consumer's losses. However, if it can be proven that the losses were caused by the consumer's own involvement, fault, negligence, or unlawful acts, the financial service institution is not liable for the damages. This provision highlights a limitation in the regulation, as it holds the consumer accountable for their involvement in the loss, even though social engineering schemes often exploit the weaknesses and negligence of banking customers, who may unknowingly disclose personal information that is later misused. On the other hand, the sophistication and vulnerabilities of digital banking security systems also play a critical role in determining the success or failure of these schemes. The adequacy of the technological safeguards implemented by the bank is thus an essential factor in assessing the bank's liability in these cases.

Considering the three legal frameworks mentioned, it can be concluded that, normatively, these regulations incorporate the fundamental principles of consumer protection applicable to the banking sector. However, the current legal provisions fail to provide concrete and effective protection for customers who suffer losses due to social engineering schemes. The Consumer Protection Law does not specifically address consumer protection in the context of digital business actors. Furthermore, both Law No. 4/2023 and Financial Services Authority Regulation No. 22/2023 tend to place the burden of proof primarily on the customer's negligence, despite the fact that the security of digital banking systems is also a crucial factor (Hakim & Putra, 2025; Usanti & Setiawati, 2024). Existing regulations often stipulate that banks, as financial service institutions, are not liable in these cases. Moreover, neither Law No. 4/2023 nor the Financial Services Authority Regulation No. 22/2023 provides clear legal remedies or avenues through which victims of social engineering can seek redress or legal protection. In many instances, customers who suffer financial losses do not receive compensation, as their action of disclosing confidential data is deemed consumer negligence, whether intentional or unintentional (Indrawati, 2025).

This situation reveals a legal imbalance, where the burden of proof and responsibility for securing digital banking systems is disproportionately shifted onto the consumer. In cases involving social engineering schemes, customers often find themselves held accountable for losses, even though the vulnerabilities in digital banking systems and the methods used by malicious actors play a significant role in these incidents. While the current legal framework provides some level of consumer protection, it fails to address the complexities and risks associated with digital banking, particularly in the context of social engineering. This gap

highlights the need for more specific regulations that directly address consumer protection in the digital banking sector (Oyewole et al., 2024; Turillazzi et al., 2023).

To address this imbalance, there is an urgent need for the implementation of regulations under the existing Financial Services Authority Regulation No. 22/2023. Such regulations should establish clear and enforceable minimum security standards for digital banking products. These standards would ensure that banks are required to implement reliable security measures capable of protecting customer funds from third-party breaches, including those arising from social engineering schemes. Digital banking services must be fortified with robust defenses against cyberattacks, ensuring that customers' personal and financial information remains safe.

In addition to security standards, regulations should also focus on the proportional allocation of liability between customers and banks. In cases where losses arise due to both consumer negligence or error and weaknesses in digital banking IT systems, a fair distribution of responsibility is necessary. While consumers should be aware of the importance of safeguarding their personal information, financial institutions are ultimately responsible for maintaining the security and integrity of their systems. A well-defined framework for determining liability would ensure that consumers are not unfairly burdened with the full extent of losses, especially when banks are also at fault for inadequate security measures.

Furthermore, regulatory reform should include the provision of clear and accessible legal remedies for customers who fall victim to social engineering schemes. This includes establishing technical guidelines that outline the steps consumers can take to recover losses and seek redress when deceived by fraudulent tactics. A straightforward process for filing complaints, seeking compensation, and holding financial institutions accountable would strengthen consumer confidence in digital banking. This would also create an environment where customers are more likely to trust their banking institutions, knowing that they have legal avenues to pursue when they face financial harm due to social engineering.

Regulatory reform is crucial for achieving a more balanced and fair approach to consumer protection in the digital banking sector. Such reforms must not only emphasize the responsibility of consumers to remain vigilant and protect their personal data but also ensure that financial institutions are held accountable for securing their products and services. This includes obligating banks to invest in stronger security measures and providing compensation to consumers under certain conditions. By sharing the responsibility for digital security, both banks and consumers can be held accountable in a manner that promotes fairness. This regulatory overhaul would foster greater legal certainty and fairness, ultimately ensuring that digital banking is safer for consumers and that they are better protected against evolving cyber threats, including social engineering schemes.

3. Legal Protections and Dispute Resolution in Social Engineering Cases in Banking

Social engineering attacks targeting banking customers often result in financial losses, particularly when customers unknowingly become victims by clicking malicious links or installing harmful applications (Al Qwaid, 2025; Aslan et al., 2023). Currently, there are no specific regulations that explicitly govern the resolution mechanisms for incidents involving social engineering. However, in cases of customer losses, the Financial Services Authority Regulation No. 22/2023 stipulates that customers have the right to file complaints and seek dispute resolution. The provision of such dispute resolution procedures represents a form of reactive legal protection for banking customers who have incurred losses. Generally, the dispute resolution process available to customers begins with filing a complaint. Banks are required to provide legal certainty to protect consumers by establishing written policies and procedures on consumer protection, as mandated by Article 6 of the Financial Services Authority Regulation No. 22/2023, which states that "written policies and procedures on consumer protection must also include the handling of

complaints and dispute resolution related to product and/or service." When customers experience losses related to depleted funds in their accounts, the initial step they can take is to file a complaint.

According to Article 1, point 6 of Financial Services Authority Regulation No. 18/POJK.07/2018 concerning Consumer Complaint Service in the Financial Services Sector, complaints may be submitted either verbally or in writing. If the complaint is made verbally, the financial service institution is obligated to verify the complaint. Conversely, if the complaint is submitted in writing, the institution must verify the completeness of the documents provided by the consumer. Pursuant to Article 14 of Financial Services Authority Regulation No. 18/POJK.07/2018, upon receiving a complaint, the financial service institution is required to conduct an internal review of the complaint in a competent, accurate, and objective manner, including an analysis to verify the validity of the consumer's claim. For complaints submitted verbally, the financial institution must follow up within five business days from the date the complaint is received, while written complaints must be followed up and resolved within 20 business days from the date the institution receives all supporting documents in full.

Field research conducted at several sample banks in Bali Province revealed that, similar to procedures applicable to other loss cases resulting from the use of banking services, victims of social engineering are advised to promptly report the incident to the bank. The report must be accompanied by the necessary supporting documents to request a temporary blocking of funds in the relevant account or transaction channel to prevent further financial loss. Complaints may be submitted orally, such as through the bank's call center services, or in writing, such as via the bank's official email address. Customers may also file complaints in person by visiting the nearest branch or sub-branch office. In addition to filing a complaint with the bank, customers may submit a report directly to the Financial Services Authority (OJK). Written complaints can be submitted via email, WhatsApp, or through the Consumer Protection Portal Application. Oral complaints can be submitted by telephone, or consumers may visit the OJK office in person. Reports may also be submitted to the Illegal Financial Activity Eradication Task Force (SATGAS PASTI).

In terms of consumer dispute resolution, Article 1, point (4) of Financial Services Authority Regulation No. 22/2023 defines consumer protection as efforts to provide knowledge and understanding regarding financial products and services, as well as ensuring legal certainty in protecting consumers' rights within the financial services sector. Furthermore, Article 55, paragraph (1) of Financial Services Authority Regulation No. 22/2023 mandates that financial institutions safeguard the security of consumer funds and assets under their responsibility. This implies that banks, as financial services institutions, have a duty to maintain the security of customer funds deposited within the bank and provide legal protection to customers by safeguarding their deposited funds and offering secure, resilient banking products, particularly in the face of social engineering schemes.

The dispute resolution process for losses arising from social engineering schemes aims to ensure accountability for the damages incurred by banking customers. Pursuant to Article 14, paragraph (1) of Financial Services Authority Regulation No. 18/POJK.07/2018, financial institutions are required to promptly follow up on consumer complaints with a thorough internal investigation. When handling social engineering cases, banks are tasked with investigating the circumstances surrounding the incident to determine whether the loss resulted from banking system errors or other factors. Article 10, paragraphs (1) and (2) of Financial Services Authority Regulation No. 22/2023 provide further guidance, stating that in cases where losses are caused by negligence, errors, or unlawful acts committed by the bank or its representatives, the financial institution is responsible for the consumer's losses. However, if the losses are caused by the consumer's involvement, fault, negligence, or unlawful acts, the financial institution is not liable for the damages.

This provision implies that when the loss of a customer's funds is caused by a failure in the banking system or by the negligence of the bank itself, Article 10, paragraph (1) of Financial

Services Authority Regulation No. 22/2023 applies. This article obliges financial service institutions to take full responsibility for losses incurred by consumers. Such legal responsibility is further reinforced by Article 1365 of the Indonesian Civil Code, which states that "any unlawful act that causes harm to another person obliges the person who, due to their fault, caused the harm to compensate for the damage." However, if the loss is not the result of a failure within the bank's internal system, human error by bank employees, or internal fraud, but is instead caused solely by the customer's negligence, such as falling victim to a social engineering scheme, then Article 10, paragraph (2) of Financial Services Authority Regulation No. 22/2023 applies, and in this case, the bank is not held liable for the customer's loss.

Field research conducted at several banking institutions, along with findings from the Financial Services Authority, reveals that social engineering cases are often caused by consumers' failure to protect their personal data. This includes actions such as clicking on malicious links, disclosing confidential PINs or OTP codes, or installing unauthorized applications. When the consumer's negligence is evident, the bank is legally exempt from liability for the resulting financial loss.

In the absence of liability on the part of the bank, as stipulated in Article 10, paragraph (2) of Financial Services Authority Regulation No. 22/2023, customers may pursue repressive legal measures to seek legal protection. This is in accordance with Article 25, paragraph (1) of Financial Services Authority Regulation No. 18/POJK.07/2018, which allows consumers to seek legal resolution through litigation. In such cases, customers can initiate legal proceedings by first filing a criminal complaint with the police, particularly when the incident involves fraud, as seen in social engineering schemes. The actions committed by perpetrators in these schemes can be categorized as criminal fraud under Article 378 of the Indonesian Criminal Code, which states: "Anyone who, with the intent to unlawfully benefit themselves or another person, by using a false name or false status, deceit, or a series of lies, causes another person to hand over property, give a loan, or cancel a debt, shall be deemed to have committed fraud and may be sentenced to a maximum of four years imprisonment."

The essential elements of the criminal act of fraud, as stipulated in Article 378 of the Indonesian Criminal Code, include deceit or trickery, false statements or lies within a series of deceptive actions, the use of false names or false identities, and a series of fraudulent circumstances designed to unlawfully obtain personal gain or benefit without legal entitlement. These elements directly apply to social engineering schemes, where the loss of customer funds is, in essence, the result of the customer's own negligence, especially when they unknowingly disclose personal information, passwords, or OTP links to perpetrators. This vulnerability arises from the nature of social engineering, which exploits human behavior, social interaction, and momentary lapses in vigilance.

Social engineering schemes are designed to manipulate individuals by exploiting psychological tendencies such as trust, urgency, fear, and obedience to authority (Longtchi et al., 2024; Workman, 2008). To reduce the number of victims, one of the most effective measures is to strengthen preventive efforts through continuous and targeted customer education. Financial institutions must raise awareness about the importance of protecting personal banking data and remaining vigilant against emerging forms of banking-related fraud. By educating customers on how to identify and avoid potential threats, financial institutions can help mitigate the impact of social engineering schemes and empower consumers to protect themselves.

D. Conclusion

Common forms of social engineering schemes in the banking sector include the distribution of APK files containing malware, phishing, pretexting, baiting, and quid pro quo. These schemes are designed to manipulate bank customers into unintentionally disclosing sensitive personal and banking information, often leading to substantial financial losses. Current consumer protection in

the banking sector is regulated under several legal instruments, including Law No. 8 of 1999, Law No. 4 of 2023, and Financial Services Authority Regulation No. 22 of 2023. While these frameworks incorporate fundamental principles of consumer protection, they are not yet sufficient to provide specific and effective legal remedies for banking customers who fall victim to social engineering schemes. There is a clear need for more detailed regulation in the form of a derivative regulation under the POJK on Consumer Protection. Such regulation should include the regulation of minimum security standards for digital banking products that are reliable and capable of safeguarding customers' funds from third-party breaches or cyberattacks. Additionally, provisions should address the proportional allocation of liability between customers and banks in cases where customer losses arise due to both consumer negligence or error and weaknesses in the digital banking service's information technology (IT) systems. Furthermore, technical guidelines should be established to provide clear and accessible legal steps for customers who fall victim to social engineering schemes.

In general, customers who suffer losses may file complaints with either the bank or the Financial Services Authority. If the loss is proven to be caused by negligence, error, or unlawful conduct on the part of the bank, the bank, as a financial service institution, is legally obligated to compensate the customer. However, if the loss is found to result solely from the customer's own involvement, carelessness, or failure to protect personal data, the bank is not held liable under the POJK Consumer Protection. In such circumstances, the customer still retains the right to pursue litigation, beginning with the filing of a criminal complaint for fraud with the police, as stipulated in Article 378 of the Indonesian Criminal Code.

This study recommends that the government, through the Financial Services Authority, issue a more detailed implementing regulation under the existing Financial Services Authority Regulations on Consumer Protection to provide concrete legal protection for customers affected by social engineering schemes. Strengthening consumer protection regulations within the financial services sector, as outlined above, is essential to improving the legal safeguards available to customers. It is also recommended that banks actively implement ongoing education and financial literacy programs for digital banking users to raise awareness about the latest fraud schemes and emphasize the importance of safeguarding personal banking data. Finally, banking customers are urged to exercise greater caution when using digital banking services. They should be more vigilant and avoid disclosing sensitive information such as PINs or passwords, especially in response to unsolicited requests from unknown individuals or suspicious sources.

REFERENCES

Adenansi, R., & Novarina, L. A. (2017). Malware Dynamic. *JOEICT (Journal of Education and Information Communication Technology)*, *1*(1), 37–43. https://doi.org/10.29100/.v1i1.91

Airehrour, D., Vasudevan Nair, N., & Madanian, S. (2018). Social Engineering Attacks and Countermeasures in the New Zealand Banking System: Advancing a User-Reflective Mitigation Model. *Information*, *9*(5), 110. https://doi.org/10.3390/info9050110

Al Qwaid, M. (2025). Cybersecurity Threats: Ransomware, Phishing, and Social Engineering. In *Complexities and Challenges for Securing Digital Assets and Infrastructure* (pp. 399–434). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-1370-2.ch018

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), 1333. https://doi.org/10.3390/electronics12061333

Atmaja, Y. S., & Paulus, D. H. (2022). Partisipasi Bank Indonesia Dalam Pengaturan Digitalisasi Sistem Pembayaran Indonesia. *Masalah-Masalah Hukum*, *51*(3), 271–286. https://doi.org/10.14710/mmh.51.3.2022.271-286

Butarbutar, R. (2023). Kejahatan Siber Terhadap Individu: Jenis, Analisis, Dan Perkembangannya. *Technology and Economics Law Journal*, *2*(2), 297–316. https://doi.org/10.21143/TELJ.vol2.no2.1043

Darmaningrat, E. W. T., Ali, A. H. N., Herdiyanti, A., Pribadi, A., Subriadi, S., Muqtadiroh, F. A., Astuti, H. M., & Susanto, T. D. (2022). Sosialisasi Bahaya dan Upaya Pencegahan Social Engineering untuk Meningkatkan Kesadaran Masyarakat tentang Keamanan Informasi. *SEWAGATI, Jurnal Pengabdian Kepada Masyarakat - LPPM ITS*, *6*(2), 160–169. https://doi.org/10.12962/j26139960.v6i2.92

Gallo, L., Gentile, D., Ruggiero, S., Botta, A., & Ventre, G. (2024). The Human Factor in Phishing: Collecting and Analyzing User Behavior When Reading Emails. *Computers & Security*, *139*, 103671. https://doi.org/10.1016/j.cose.2023.103671

Hakim, M. R., & Putra, M. R. S. (2025). Analysis of Digital Bank Customer Protection Against Loss of Funds in Accounts Reviewed According to Indonesian Positive Law. *Jurnal Usm Law Review*, *8*(2), 813–824. https://doi.org/10.26623/julr.v8i2.12073

He, D., Chan, S., & Guizani, M. (2015). Mobile Application Security: Malware Threats and Defenses. *IEEE Wireless Communications*, *22*(1), 138–144. https://doi.org/10.1109/MWC.2015.7054729

Hewage, C., Nawaf, L., Khan, I., & Alkhalil, Z. (2021). Phishing Attacks: A Recent Comprehensive Study and a New Anatomy. *Frontiers in Computer Science*, *3*(6), 563060. https://doi.org/10.3389/fcomp.2021.563060

Ibrahim, J., & Sirait, Y. H. (2021). *Kejahatan Transfer Dana: Evolusi Dan Modus Kejahatan Melalui Sarana Lembaga Keuangan Bank*. Sinar Grafika (Bumi Aksara).

Indrajit, R. E., & Teknik, S. B. (2017). Social Engineering. *SERI*, *999*, 6.

Indrawati, Y. (2025). Independence of Bank Indonesia Post Law No. 4 of 2023 on Development and Strengthening of the Financial Sector. *Journal of Central Banking Law and Institutions*, *4*(2), 203–226. https://doi.org/10.21098/jcli.v4i2.280

Jakobsson, M., & Ramzan, Z. (2008). *Crimeware: Understanding New Attacks and Defenses*. Addison-Wesley Professional.

Javadpour, A., Ja'fari, F., Taleb, T., Shojafar, M., & Benzaïd, C. (2024). A Comprehensive Survey on Cyber Deception Techniques to Improve Honeypot Performance. *Computers & Security*, *140*, 103792. https://doi.org/10.1016/j.cose.2024.103792

Kaur, S. J., Ali, L., Hassan, M. K., & Al-Emran, M. (2021). Adoption of Digital Banking Channels in an Emerging Economy: Exploring the Role of in-Branch Efforts. *Journal of Financial Services Marketing*, *26*(2), 107–121. https://doi.org/10.1057/s41264-020-00082-w

Longtchi, T. T., Rodriguez, R. M., Al-Shawaf, L., Atyabi, A., & Xu, S. (2024). Internet-Based Social Engineering Psychology, Attacks, and Defenses: A Survey. *Proceedings of the IEEE*, *112*(3), 210–246. https://doi.org/10.1109/JPROC.2024.3379855

Martinelli, I. (2021). Menilik Financial Technology (Fintech) dalam Bidang Perbankan yang dapat Merugikan Konsumen. *Jurnal SOMASI (Sosial Humaniora Komunikasi)*, *2*(1), 32–43. https://doi.org/10.53695/js.v2i1.353

Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R.-J. '"Bryan."' (2023). International Business in the Digital Age: Global Strategies in a World of National Institutions. *Journal of International Business Studies*, *54*(4), 577–598. https://doi.org/10.1057/s41267-023-00618-x

Mishra, A., Alzoubi, Y. I., Anwar, M. J., & Gill, A. Q. (2022). Attributes Impacting Cybersecurity Policy Development: An Evidence from Seven Nations. *Computers & Security*, *120*, 102820. https://doi.org/10.1016/j.cose.2022.102820

Natalis, A., & Djohan, N. H. (2025). Cybersex Trafficking: Legal Challenges and Protection for Women and Children in Indonesia. *International Cybersecurity Law Review*, *6*(3), 421–456. https://doi.org/10.1365/s43439-025-00149-1

Oyewole, A. T., Oguejiofor, B. B., Eneh, N. E., Akpuokwe, C. U., & Bakare, S. S. (2024). Data Privacy Laws and Their Impact on Financial Technology Companies: A Review. *Computer Science & IT Research Journal*, *5*(3), 628–650. https://doi.org/10.51594/csitrj.v5i3.911

Purkait, S. (2012). Phishing Counter Measures and Their Effectiveness – Literature Review. *Information Management & Computer Security*, *20*(5), 382–420. https://doi.org/10.1108/09685221211286548

Rakocevic, S. B., Rakic, N., & Rakocevic, R. (2025). An Interplay Between Digital Banking Services, Perceived Risks, Customers' Expectations, and Customers' Satisfaction. *Risks*, *13*(3), 39. https://doi.org/10.3390/risks13030039

Ratulangi, C. H. (2021). Tindak Pidana Cyber Crime Dalam Kegiatan Perbankan. *Lex Privatum*, *9*(5), 179-187. https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/33510

Silalahi, P. R., Daulay, A. S., Siregar, T. S., & Ridwan, A. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Profit: Jurnal Manajemen, Bisnis Dan Akuntansi*, *1*(4), 224–235. https://doi.org/10.58192/profit.v1i4.481

Siswanto, & Lenita, M. D. (2024). Prinsip Kehati-Hatian Nasabah Perbankan Dalam Menjaga Keamanan Bisnis Dari Social Engineering Fraud. *JUSTITIABLE - Jurnal Hukum*, *7*(1), 82–100. https://doi.org/10.56071/justitiable.v7i1.855

Tay, L.-Y., Tai, H.-T., & Tan, G.-S. (2022). Digital Financial Inclusion: A Gateway to Sustainable Development. *Heliyon*, *8*(6), e09766. https://doi.org/10.1016/j.heliyon.2022.e09766

Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The Digital Services Act: An Analysis of Its Ethical, Legal, and Social Implications. *Law, Innovation and Technology*, *15*(1), 83–106. https://doi.org/10.1080/17579961.2023.2184136

Triamanda, V. (2022). *Kejahatan Soceng Semakin Marak, Ratusan Nasabah Lapor ke OJK*. https://economy.okezone.com/read/2022/06/22/320/2616233/kejahatan-soceng-semakin-marak-ratusan-nasabah-lapor-ke-ojk

Usanti, T., & Setiawati, A. (2024). Customer Protection of Digital Services by Commercial Banks Concerning Consumer and Community Protection in the Financial Services Sector. *The International Journal of Politics and Sociology Research (IJOPSOR)*, *11*(4), 493–499. https://doi.org/10.35335/ijopsor.v11i4.223

Utami, P. D. Y., Purwanti, N. P., Yudaasmini, N. W. J., Manek, A. U., & Tantra, K. S. P. (2025). Edukasi Dan Literasi Keuangan Berbasis Digital: Penerapannya Dalam Mencegah Modus Social Engineering Pada Sektor Perbankan Digital. *Kertha Semaya : Journal Ilmu Hukum*, *13*(4), 625–638. https://doi.org/10.24843/KS.2025.v13.i04.p12

Wiedyasari, A. B., & Yuspin, W. (2024). Protection of Customer Personal Data of Bank Syariah Indonesia Reviewed From POJK Number 6/POJK.07/2022. *Unram Law Review (ULREV)*, *8*(1), 1–17. https://doi.org/10.29303/ulrev.v8i1.331

Workman, M. (2008). Wisecrackers: A Theory-Grounded Investigation of Phishing and Pretext Social Engineering Threats to Information Security. *Journal of the American Society for Information Science and Technology*, *59*(4), 662–674. https://doi.org/10.1002/asi.20779

Xia, L., Baghaie, S., & Mohammad Sajadi, S. (2024). The Digital Economy: Challenges and Opportunities in the New Era of Technology and Electronic Communications. *Ain Shams Engineering Journal*, *15*(2), 102411. https://doi.org/10.1016/j.asej.2023.102411

Yuspin, W., Putri, A. O., Fauzie, A., & Pitaksantayothin, J. (2024). Digital Banking Security: Internet Phishing Attacks, Analysis and Prevention of Fraudulent Activities. *International Journal of Safety and Security Engineering (IJSSE)*, *14*(6), 1699–1706. https://doi.org/10.18280/ijsse.140605