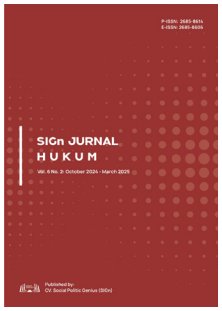

SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614
https://jurnal.penerbitsign.com/index.php/sjh/article/view/v7n1-8

Vol. 7 No. 1: April - September 2025 Published Online: April 26, 2025

Article Title

Phishing in the Banking Sector: Between Cybercrime and Consumer Protection

Author(s)

Dian Ekawati*
Universitas Pamulang, Indonesia || dosen02090@unpam.ac.id
**Corresponding Author*

Dadan Herdiana
Universitas Pamulang, Indonesia || dosen02088@unpam.ac.id

Amelia Haryanti
Universitas Pamulang, Indonesia || dosen00811@unpam.ac.id

How to cite:

Ekawati, D., Herdiana, D., & Haryanti, A. (2025). Phishing in the Banking Sector: Between Cybercrime and Consumer Protection. *SIGn Jurnal Hukum, 7*(1), 133-151. https://doi.org/10.37276/sjh.v7i1.422

ABSTRACT

The escalating utilization of electronic banking services corresponds with a heightened threat of cybercrime, particularly phishing, leading to significant financial losses for customers and eroding public trust in the digital banking system. This research aims to analyze the forms of legal protection available and the construction of banks' civil liability, as well as to identify the legal remedies accessible to customers victimized by phishing under Law Number 8 of 1999. Employing a normative legal research methodology integrating statute and conceptual approaches, the study analyzed relevant legislation and legal doctrines. Findings indicate that banks bear specific legal obligations mandated by Financial Services Authority Regulations, Law Number 27 of 2022, and Law Number 8 of 1999, about the assurance of system and data security. Consequently, banks' civil liability for phishing-induced losses can be established, primarily on the grounds of unlawful acts (tort), contingent upon proof of failure to discharge these specific duties involving fault or negligence. However, the practical determination of liability remains complex, invariably factoring in customer contributory negligence. Victims possess options including criminal reporting and general civil litigation, yet Law Number 8 of 1999 offers a more structured consumer dispute resolution pathway. This pathway encompasses mandatory internal complaints submitted to the bank, potentially followed by escalation to LAPS SJK as the principal forum for out-of-court settlement. The study concludes that while the legal framework establishes a basis for bank liability, the adequate protection of customers is heavily contingent upon evidentiary success in disputes and the optimized functioning of resolution mechanisms, particularly LAPS SJK.

Keywords: *Banking; Bank Liability; Consumer Protection; Cybercrime; Phishing.*

INTRODUCTION

Banking institutions play a vital role as fundamental pillars within a nation's economic architecture, serving as financial intermediaries, agents of trust, and agents of development (Manga & Dianti, 2023). Banks inherently contribute to monetary stability and the acceleration of national development by mobilizing public funds and channeling them back into the economy through credit or financing facilities, alongside providing various other financial services (Manangin, 2022). Sound and trustworthy banks constitute an essential prerequisite for the growth of economic activity and the enhancement of public welfare, thereby positioning this sector strategically, necessitating comprehensive legal regulation and oversight (Sinaga & Maulisa, 2022).

The exponential development of information technology has driven a fundamental transformation within the global banking industry, including in Indonesia, ushering in the era of digital banking (Paminto et al., 2024). Electronic banking (e-banking) services, such as Internet banking, mobile banking, and transactions via Automated Teller Machines (ATMs), have become an integral part of the modern financial services landscape, offering operational efficiencies for banks as well as ease, speed, and convenience of access for customers (Oktana et al., 2023). While yielding numerous benefits, this digitalization simultaneously introduces new and complex risks, particularly concerning the security of systems and customer data within the dynamic and often vulnerable cyber ecosystem (Sihombing et al., 2024).

With the widespread adoption of e-banking services, the threat of cybercrime targeting the banking sector and its clientele has emerged, with phishing being one of the most pervasive and detrimental forms (Ismail et al., 2022). Phishing constitutes a sophisticated form of cyber fraud wherein the perpetrator (phisher) employs social engineering techniques to deceive victims into divulging sensitive personal information, such as usernames, passwords, credit card numbers, or One-Time Passwords (OTPs) (Juniamalia & Fadlian, 2023). Phishers typically impersonate trusted entities or institutions, such as the bank itself, through fraudulent electronic communications like emails, Short Message Service (SMS) texts, instant messages (e.g., WhatsApp), or by creating spoofed websites (web forgery) meticulously designed to resemble legitimate ones, thereby ensnaring victims (Banjarnahor & Priyana, 2022).

Phishing schemes exploit psychological vulnerabilities and the limited technical understanding of certain users of digital banking services (Orji, 2019). Victims are often induced to click on malicious links or enter their credentials onto fraudulent web pages under various pretexts, including system updates, account verification, attractive prize offers, or even spurious security alerts ironically designed to steal the victim's security credentials (Damayanti & Priyono, 2022). The success of phishing hinges not only upon the technical sophistication of the phisher in mimicking legitimate entities but also significantly upon the victim's negligence or lack of due diligence in verifying the authenticity of the communications or links received, creating a significant security vulnerability beyond the direct control of the banking institution's security infrastructure.

The implications of phishing extend beyond the direct financial losses suffered by individual customers, although this aspect is significant in itself. Moreover, the prevalence of phishing incidents threatens to erode the foundation of public trust in the security and reliability of the digital banking system – a critical asset upon which the industry fundamentally relies (Putri & Sugiyono, 2024). An ineffective response to this threat can incur substantial social costs, disrupt intermediation and transmission functions within the payment system, and generate legal uncertainty that may impede the broader adoption of financial technology (Hasanudin & Babussalam, 2024). Consequently, comprehensively addressing phishing is a critical issue not only for customers and banking institutions but also for regulators and the stability of the national financial system.

This phishing phenomenon within the banking context inherently resides at the intersection of several complex branches of law: Banking Law, Cybercrime Law, and Consumer Protection Law (Ekawati, 2018). Law Number 7 of 1992[1] stipulates operational standards and prudential obligations for banking institutions, including

[1]Law Number 7 of 1992, as amended several times, lastly by Article 78 of Government Regulation in Lieu of Law Number 2 of 2022.

concerning the provision of information technology services, as regulated by the Financial Services Authority. Furthermore, Law Number 11 of 2008[2] provides the legal framework for addressing cyber criminal offenses, such as unauthorized access to electronic systems and fraud. Concurrently, Law Number 8 of 1999 establishes the foundation for protecting customer rights as consumers of financial services, encompassing the rights to safety, security, convenience, and accurate information.

A fundamental issue frequently arising in phishing cases is allocating legal liability, particularly civil liability, when customers sustain financial losses. It raises crucial questions concerning the extent of the bank's liability, as the provider of e-banking services, for customer losses precipitated by phishing attacks, particularly where contributory negligence exists on the part of the customer in safeguarding the confidentiality of their data. Ambiguity or divergent perspectives regarding the determination of liability, compounded by the complexities of evidentiary requirements in cyber-related disputes, necessitates thoroughly examining the concrete forms of legal protection available to customers and effective dispute resolution mechanisms under the prevailing statutory framework, primarily Law Number 8 of 1999.

Against this complex backdrop, this research primarily aims to analyze two crucial aspects in-depth. *Firstly*, the study seeks to analyze the forms of legal protection and the construct of banks' civil liability towards customers victimized by phishing in the context of utilizing e-banking services. *Secondly*, the research endeavors to identify and examine various legal remedies, both litigation and non-litigation, available to customers who have fallen victim to phishing for the resolution of their cases and the recovery of their losses, with a specific focus on the legal framework established by Law Number 8 of 1999. Through analyzing these aspects, this study is anticipated to contribute conceptually to advancing legal scholarship, provide guidance for legal and banking practitioners, and enhance broader public awareness and legal comprehension concerning rights and obligations when confronting the threat of phishing in the digital age.

METHOD

This study fundamentally constitutes normative legal research, doctrinal or library-based research (Qamar & Rezah, 2020). This methodology is selected based on the research focus, which is essentially aimed at examining and analyzing law as a system of positive norms (law as it is written in the books), encompassing legal principles, written legal norms stipulated in legislation, and relevant legal doctrines pertinent to the issue of phishing within the context of digital banking services. It particularly concerns aspects of legal protection for customers and the construction

[2]Law Number 11 of 2008, as amended several times, lastly by Law Number 1 of 2024.

of the civil liability of banking institutions. Two primary approaches are employed concurrently within the normative legal research framework to comprehensively dissect the formulated legal issues: the Statute Approach and the Conceptual Approach. The Statute Approach involves an in-depth examination of the hierarchy and substance of various legal norms enshrined in the relevant legislation. Concurrently, the Conceptual Approach is utilized to identify, comprehend, and analyze the meaning, scope, and logical interrelations among key legal concepts pertinent to the subject matter, such as consumer protection, civil liability, unlawful acts, electronic system security, cybercrime, and good faith within the bank-customer relationship.

This normative legal research exclusively utilizes secondary data sources, which are generally classified into primary and secondary legal materials (Sampara & Husen, 2016). Primary legal materials, representing sources of law with the highest authority and binding force, comprise a range of legislation that directly or indirectly govern or pertain to the investigated legal issues. Key among these are the Civil Code, particularly provisions concerning Obligations that regulate unlawful acts and principles of liability; Law Number 8 of 1999, serving as the foundation for the rights and obligations of consumers and financial services providers; Law Number 11 of 2008, governing the legal aspects of electronic transactions and cybercrime; Law Number 27 of 2022, pertinent to the obligations regarding customer data protection; as well as various relevant Financial Services Authority Regulations. In addition, the research draws upon secondary legal materials, which encompass resources offering explanations, interpretations, analyses, or critical reviews of primary legal materials. These include authoritative legal textbooks, articles published in reputable scholarly legal journals, findings from relevant prior research, legal dictionaries, and the doctrines or opinions of prominent legal scholars in civil law, banking law, information technology (cyber) law, and consumer protection law. All primary and secondary legal materials were meticulously identified, inventoried, and gathered systematically using library research and document analysis techniques from credible sources.

Subsequently, the gathered legal materials were analyzed qualitatively, employing a combination of analytical techniques conventional to normative legal research (Irwansyah, 2020). The legal interpretation was applied as the fundamental method to explore and ascertain the meaning embedded within written legal norms, utilizing grammatical (literal) interpretation, systematic interpretation (examining norms about other legal provisions), and teleological/sociological interpretation (discerning the purpose or social objectives of the norm). This process aimed to achieve a holistic understanding of the legislative intent and the context for applying these norms to the issue of phishing. Content analysis was also meticulously employed to dissect, classify, and synthesize the substantive ideas, concepts, principles, and pertinent legal arguments within primary and secondary legal materials. Drawing upon the outcomes

of the interpretation and content analysis, legal reasoning and argumentation were systematically constructed—logically, coherently, and systematically—to address each research question, particularly in formulating arguments concerning the forms of legal protection, the civil liability of banks, and the legal remedies available to customers victimized by phishing. Finally, the entire analysis was presented in a qualitative descriptive manner, specifically through a structured, systematic, and argumentative narrative, to furnish a profound and comprehensive understanding of the legal complexities surrounding the phenomenon of phishing in the Indonesian banking industry. The disciplined application of these methods aimed to ensure the validity and reliability of the analysis and conclusions drawn in this study.

RESULTS AND DISCUSSION

A. The Legal Framework for Banking Phishing: Banks' Essential Obligations and Customers' Fundamental Protections

The phishing phenomenon targeting banking customers in Indonesia must be construed not merely as a technological risk but as an act possessing a distinct legal qualification within the national legal framework, primarily as a form of cybercrime (Erdiyanto, 2023). The actions of phishers, frequently employing diverse fraudulent schemes such as fraudulent offers for priority customer status upgrades, misleading information concerning interbank transfer fees, fictitious credit card application solicitations, or instructions for card replacement via unofficial links, are essentially aimed at gaining unauthorized access or deceiving customers into surrendering confidential personal data and banking credentials (Yusuf et al., 2022). Such actions substantively fulfill the elements of criminal offenses (delicts), for instance, under Article 30 of Law Number 11 of 2008 concerning unauthorized access to electronic systems or under Article 28 section (1) of Law Number 1 of 2024 about the dissemination of false and misleading information that results in consumer detriment. Acknowledging phishing as an unlawful act within the cyber domain serves as a crucial starting point for mapping the legal landscape governing the relationship between banks, customers, and external threats in the evolving digital banking ecosystem.

Proceeding from the reality of the phishing threat, legal analysis invariably involves an examination of the position and obligations of banks as strictly regulated financial services institutions entrusted with public confidence. Law Number 7 of 1992 fundamentally establishes the prudential banking principle as the primary foundation for banking operations. This principle mandates that banks consistently conduct their operations diligently, professionally, and responsibly to safeguard the interests of depositing customers and maintain financial system stability. Within the context of services based on information technology, this

prudential principle logically translates into an inherent obligation for banks to ensure that the electronic systems they provide possess adequate levels of security and reliability and are managed through effective risk management frameworks designed to anticipate and mitigate diverse potential threats, including cyber fraud such as phishing. This general obligation forms the basis for formulating more specific standards and legal liabilities for banking institutions in the digital age.

The standards governing banks' obligations concerning providing information technology and risk management are further elaborated through a series of Financial Services Authority Regulations. For instance, Financial Services Authority Regulation Number 11/POJK.03/2022 explicitly mandates that banks implement good information technology governance, build reliable information technology infrastructure, and implement comprehensive information security systems. It encompasses implementing robust, multi-layered customer authentication mechanisms, such as using One-Time Passwords (OTP) sent via verified secure channels for high-risk transactions or activities, as an essential component of safeguarding customer account access. Correspondingly, Financial Services Authority Regulation Number 18/POJK.03/2016 also mandates banks to proactively identify, measure, monitor, and control operational risks, where risks related to information technology failure and external fraud are explicitly included. Compliance with the technical and procedural standards stipulated in these Financial Services Authority Regulations is no longer merely a matter of best practice but constitutes a binding legal obligation for every bank providing e-banking services.

Another critical dimension reinforcing banks' obligations is protecting customer personal data, now comprehensively regulated in Law Number 27 of 2022. As data controllers, banks bear full legal responsibility for ensuring that the entire processing lifecycle of customer personal data—encompassing acquisition, storage, utilization, and destruction—is conducted lawfully, fairly, transparently, and, crucially, securely. Law Number 27 of 2022 mandates that banks implement appropriate technical and organizational security measures commensurate with the level of risk involved to prevent unauthorized access, disclosure, or modification of personal data, including the banking credential data primarily targeted by phishing attacks. This obligation to protect the confidentiality and integrity of personal data is directly correlated with phishing prevention efforts since the success of phishing frequently hinges on the phisher's ability to acquire sensitive customer data that banks are obligated to protect.

Banks' obligations, however, are not confined solely to the technical aspects of system and data security; they extend to the duty to furnish customers with adequate information and education. Law Number 8 of 1999 and Financial

Services Authority Regulation Number 22 of 2023 expressly mandate financial services providers, including banks, to provide accurate, precise, truthful, and not misleading information regarding the products and services offered, encompassing their potential risks. Within the phishing context, this obligation encompasses the proactive dissemination of information concerning customers' legal rights as consumers and continuous education regarding cybersecurity risks, the latest phishing modus operandi, and safe online banking practices. Educational efforts through various official bank communication channels—such as issuing warnings never to share personal data (including PINs or OTPs) with anyone, even those purporting to represent the bank, and advising constant vigilance against suspicious links or attachments, urging transactions only through official platforms—constitute concrete implementations of the bank's duty to empower and protect customers through the dissemination of relevant and adequate information.

Conversely, on the other side of this legal spectrum, customers, as consumers of financial services, are endowed with fundamental rights guaranteed under Article 4 of Law Number 8 of 1999. The rights most pertinent to confronting the phishing threat include the right to comfort, security, and safety in consuming goods and/or services; the right to accurate, clear, and truthful information; and the right to have their opinions and complaints heard. The right to security and safety implicitly entails that customers are entitled to expect a reasonable level of protection afforded by the bank's systems against foreseeable threats (Ferdiansyah et al., 2024). Furthermore, the right to information underscores the customer's entitlement to adequate explanations regarding the secure operation of services and the potential attendant risks, forming the basis for banks to deliver effective education. Acknowledging these fundamental customer rights completes the depiction of the legal framework governing the bank-customer relationship within the digital services context.

In summation, examining the legal framework surrounding banking phishing in Indonesia reveals a reasonably comprehensive normative structure that establishes significant standards of obligation for banks while affording fundamental protections to customers (Sari & Sutabri, 2023). Banks, guided by the principle of prudence and specific mandates from Financial Services Authority Regulations and Law Number 27 of 2022, possess essential legal obligations to provide secure e-banking systems, manage information technology risks prudently, safeguard personal data, and furnish adequate information and education. Concurrently, customers, as consumers, are protected under Law Number 8 of 1999, which guarantees their fundamental rights to safety, security, information, and proper service. This understanding of the equilibrium between

bank obligations and customer rights constitutes the crucial normative foundation for the subsequent analysis concerning the civil liability of banks in the event of phishing incidents resulting in customer losses.

B. Analysis of Banks' Civil Liability in Phishing Incidents

When customers incur financial losses resulting from phishing attacks that exploit electronic banking services (Suhyana et al., 2021), the focus within civil law shifts towards the potential liability of the banking institution, notwithstanding that the principal criminal act is perpetrated by a third party (the phisher). Analyzing the civil liability of banks in these instances is inherently complex, as it entails an interplay among the actions of the phisher, the bank's internal security systems and procedures, and the conduct or negligence of the customer. Indonesia's civil law framework, particularly the Civil Code, provides the primary foundation for examining potential bank liability, principally through the doctrine of unlawful acts (*onrechtmatige daad*) as stipulated in Article 1365 of the Civil Code and the potential for breach of contract (default) arising from the contractual relationship established between the bank and the customer.

Establishing bank liability under Article 1365 of the Civil Code necessitates the cumulative proof of four essential elements: the existence of an unlawful act; fault attributable to the allegedly liable party (the bank); the incurrence of loss by another party (the customer); and a causal link (causality) between the fault and the loss. Within the context of banking phishing, the element of an unlawful act can be construed as the bank's failure to discharge the legal obligations previously identified. A bank's failure to implement adequate information technology security standards mandated by Financial Services Authority Regulations, negligence in protecting customer personal data as obligated by Law Number 27 of 2022, or inadequacy in providing information and education regarding phishing risks as mandated by Law Number 8 of 1999 and associated Financial Services Authority Regulations, can arguably be qualified as conduct contrary to the bank's legal duties, or, at minimum, contrary to the fundamental principles of propriety and prudence expected within the banking industry.

Subsequently, the element of fault (*schuld*) attributable to the bank must be established. In numerous phishing disputes, this often manifests as negligence (*culpa*), a concept whose relevance is also affirmed in Article 1366 of the Civil Code. Bank negligence can be evaluated based on various factors, such as deficiencies in the design or implementation of e-banking security systems failing to detect or prevent anomalous transactions; inadequate active monitoring of potential cyber threats; tardy responses to reported security incidents; or customer education methods proving ineffective in reaching or being comprehended by the majority of

users (Tompul, 2022). The assessment of such negligence objectively compares the bank's actions or omissions against the standard of conduct reasonably expected of a professional and prudent banking institution in managing operational and technological risks in the digital era. Establishing proven negligence on the part of the bank provides a strong foundation for asserting its liability.

Proving the element of loss (*schade*) in phishing cases is typically straightforward, generally manifesting as the depletion of funds from the customer's account. A more substantial evidentiary challenge frequently arises concerning the element of causality (*causaal verband*) between the bank's fault or negligence and the loss suffered by the customer. The bank might contend that the proximate cause of the loss lies solely with the phisher's fraudulent actions and/or the customer's susceptibility to deception. Nonetheless, from a legal standpoint, the argument for causality can be established by demonstrating that the bank's negligence—for example, in the form of a weak security system or minimal education—created conditions or vulnerabilities that significantly facilitated the success of the phishing attack or exacerbated the resultant losses. The basis for claiming damages finds explicit support in the provisions of Article 58 of Law Number 27 of 2022, which grants data subjects harmed by violations of personal data protection the right to seek compensation. This further underscores the civil consequences stemming from a bank's failure to protect customer data within the context of unlawful acts according to Article 1365 of the Civil Code.

Alternatively, bank liability can be constructed for breach of contract (default). The legal relationship between a bank and its customer is fundamentally contractual, encompassing both the account opening agreement and the terms and conditions governing the use of e-banking services. Within these agreements, the bank assumes contractual obligations, whether explicitly stated or implied by the nature of the service, to provide banking services securely and reliably. A bank's failure to deliver a level of system security congruent with industry standards, or that which customers can reasonably expect, thereby permitting account compromise via phishing, can logically be deemed a breach of these contractual duties (Irmawati et al., 2024). Under principles of contract law, the party in breach is obligated to compensate the aggrieved party for losses resulting from the default.

Nevertheless, any analysis of bank liability, whether grounded in tort (unlawful acts) or breach of contract, must invariably consider the factor of the customer's conduct. In numerous disputes, banks frequently advance the argument of contributory negligence (Tanudiharja et al., 2024), asserting that the customer substantially contributed to the loss through their actions, for instance, by disregarding security warnings issued by the bank, clicking on overtly suspicious phishing links, or consciously or inadvertently divulging credential information

or OTP codes to impersonating third parties. The argument concerning customer contributory negligence finds grounding in principles of civil law and constitutes a crucial factor for judges or arbitrators when determining the extent of the bank's liability. Should negligence be established on the part of both parties, principles of apportionment of liability or reduction of damages may be applied, commensurate with each party's degree of fault—an assessment heavily contingent upon the specific facts proven in each case.

In conclusion, the civil liability of a bank following a phishing incident is not automatic. However, a strong legal basis exists for establishing such liability, primarily through the mechanisms of tort (unlawful acts) or breach of contract. The determination of bank liability hinges upon proving the bank's failure to fulfill its legal obligations related to system security, data protection, and customer education (as regulated in Financial Services Authority Regulations, Law Number 27 of 2022, and Law Number 8 of 1999)—a failure which may constitute an unlawful act or breach of contract involving fault or negligence—and demonstrating a causal link to the customer's losses. Nevertheless, the element of customer contributory negligence remains a critical factor, invariably considered during dispute resolution, rendering the ultimate determination of bank liability highly contingent upon a meticulous analysis of the facts and the equitable application of legal principles in each case.

C. Dispute Resolution Mechanisms and Legal Remedies for Phishing Victims

Banking customers who sustain financial losses due to phishing, where indications suggest potential bank liability as previously analyzed, are entitled to pursue various legal remedies. Legal remedies, broadly defined, constitute the procedural avenues the legal system provides for seeking justice, safeguarding rights, or resolving disputes (Gadjong, 2023). In the specific context of losses arising from banking phishing, customers are presented with several alternative legal avenues, including the realm of criminal law, primarily focused on the phisher; the domain of civil law pursued through litigation in the general courts; and specialized consumer dispute resolution mechanisms stipulated under Law Number 8 of 1999 and its implementing regulations within the financial services sector. Selecting the appropriate legal path necessitates thoroughly understanding each option's characteristics, objectives, procedures, and potential outcomes.

An initial course of action available is to report the phishing incident as a potential criminal offense to law enforcement officials, namely the Indonesian National Police. The legal grounds for such reporting may derive from the criminal provisions within Law Number 11 of 2008 concerning offenses such as unauthorized access to electronic systems, manipulation of electronic information, or electronic

fraud resulting in losses; Article 378 of the Penal Code regarding Fraud; and potentially even Law Number 8 of 2010 (concerning money laundering) if the proceeds of the crime have been laundered or concealed. The primary objective of the criminal justice process in this regard is to identify, apprehend, and prosecute the phisher according to applicable laws. Although crucial for law enforcement and deterrence, it must be noted that the principal focus of the criminal route lies in holding the phisher accountable and does not inherently guarantee the customer's recovery of financial losses from the bank, save potentially through restitution mechanisms, the application of which might be limited.

Separately or concurrently with the criminal process against the phisher, customers may pursue civil remedies to seek compensation for incurred losses, particularly if grounds exist to assert liability against the bank. Customers have the right to initiate a civil lawsuit against the bank in the competent District Court, grounding their claim on allegations of unlawful acts (tort) or breach of contract, consistent with the prior analysis. This avenue of litigation represents a formal dispute resolution mechanism yielding legally binding judgments (Situmeang, 2021). However, litigation within the general court system frequently entails protracted timelines and substantial costs and imposes a considerable burden of proof upon the customer to persuade the court regarding the bank's fault or negligence and its causal connection to the losses stemming from the phishing incident.

Recognizing the limitations of conventional litigation, the Indonesian consumer protection legal framework furnishes alternative dispute resolution (ADR) mechanisms designed to be more accessible and efficient for consumers, including bank customers. The foundational first step within this framework involves utilizing the mandatory internal complaint handling mechanism (Internal Dispute Resolution - IDR), which every bank must provide, as mandated by Law Number 8 of 1999 and affirmed in Financial Services Authority Regulation Number 22 of 2023. Aggrieved customers are entitled, and indeed encouraged, to initially submit their complaints, either in writing or orally, to the bank's designated complaint handling unit. This internal mechanism mandates that the bank receive, record, and review the complaint, conduct internal verification or investigation as necessary, and furnish an explanation and/or a settlement response to the customer within the timeframe stipulated by Financial Services Authority regulations. This stage aims to foster dialogue and facilitate direct, amicable settlement attempts between the customer and the bank.

Should the customer's complaint fail to elicit a response or a satisfactory resolution from the bank within the prescribed timeframe, or if mutual agreement proves unattainable, the avenue for out-of-court dispute settlement (External

Dispute Resolution - EDR) via specialized institutions becomes available (Sirait et al., 2025). The primary authorized body for disputes within the financial services sector is the Alternative Dispute Resolution Agencies in Financial Services Sector (LAPS SJK). LAPS SJK, whose operations are regulated in Financial Services Authority Regulation Number 61/POJK.07/2020 based on the principles of Law Number 8 of 1999, offers dispute resolution services employing mediation (facilitating a mutually agreed settlement with the assistance of a mediator), adjudication (rendering a decision by an adjudicator based on submitted documents), or arbitration (issuing an award by an arbitrator following an examination of the parties, which is final and binding). Customers may submit an application to LAPS SJK after the unsuccessful conclusion of the internal complaint process with the bank. It presents an alternative resolution pathway generally characterized by greater speed, lower costs, and simpler procedures than court litigation.

Furthermore, the Consumer Dispute Resolution Agency, whose operations are regulated in Ministerial Regulation Number 72 of 2020, generally possesses similar authority to resolve consumer disputes across various sectors, although LAPS SJK is currently the primary forum for the financial services sector. It is crucial to emphasize that all these avenues—whether civil litigation or consumer protection mechanisms—are fundamentally aimed at realizing the consumer's fundamental right to compensation, damages, and/or restitution, as guaranteed under Article 4 point (h) of Law Number 8 of 1999, should losses be proven to have arisen from the fault or negligence of the business actor (in this context, the bank, if its liability is established). These consumer dispute resolution mechanisms are designed to offer customers a more effective pathway to assert their right to loss recovery.

Therefore, customers victimized by banking phishing possess several legal options that can be pursued simultaneously or sequentially. Reporting the incident as a criminal offense primarily targets the prosecution and punishment of the phisher, whereas initiating a civil lawsuit in the district court provides a formal litigation mechanism for seeking damages from the bank. The consumer protection legal framework, however, presents a more structured and potentially more efficient dispute resolution pathway, starting from the bank's mandatory internal complaint mechanism, which may proceed to alternative forums such as LAPS SJK. A comprehensive understanding of each avenue's characteristics, procedures, advantages, and disadvantages is crucial, enabling customers to select and utilize the most suitable legal remedies to safeguard their rights and pursue optimal recovery for their losses when confronting the detrimental consequences of phishing.

CONCLUSIONS AND SUGGESTIONS

Based on the preceding analysis and discussion, it is concluded that the Indonesian legal framework furnishes a relatively comprehensive normative foundation for protecting bank customers against phishing and determining bank liability. Legal protection for customers emanates not only from the fundamental rights guaranteed under Law Number 8 of 1999, such as the rights to security and information, but is also buttressed by specific obligations imposed upon banks as providers of electronic systems and controllers of personal data. These duties encompass the implementation of prudent information technology security standards as mandated by Financial Services Authority Regulations, along with the duty to safeguard customer personal data under Law Number 27 of 2022. A logical corollary of this normative architecture is that the civil liability of banks for customer losses arising from phishing can be established, principally on the grounds of unlawful acts (tort), provided it is proven that the bank failed to discharge these legal duties, thereby demonstrating fault or negligence. Nonetheless, enforcing such liability within individual disputes presents complexities, particularly concerning the proof of causality and assessing customer contributory negligence—factors that frequently become pivotal in case settlements.

It is further concluded that customers victimized by phishing have access to a range of dispute resolution mechanisms and legal remedies for loss recovery, wherein the consumer protection legal framework provides a more structured pathway and oriented towards consumer empowerment. Alongside reporting the phisher's criminal actions to law enforcement and pursuing general civil litigation against the bank in district courts, the legal system offers a more accessible consumer dispute resolution process. This process commences with the mandatory internal complaint-handling mechanism within the bank, as regulated in Financial Services Authority Regulation Number 22 of 2023. Should resolution prove elusive at this internal stage, customers can escalate their case to LAPS SJK, an independent institution providing mediation, adjudication, or arbitration services, which is anticipated to offer greater efficiency and effectiveness for resolving disputes within the financial services sector. LAPS SJK, functioning under the auspices of Law Number 8 of 1999, serves as a central instrument enabling customers to realize their right to compensation or damages for losses incurred from phishing incidents, particularly if the bank's liability can be established.

Following these conclusions, several suggestions are proposed to strengthen customer protection and enhance legal certainty in managing banking phishing incidents. *Firstly*, banking institutions are advised to focus on complying with the minimum security standards mandated by regulators and proactively and continuously invest in state-of-the-art cybersecurity technologies and more advanced

fraud detection systems. Furthermore, digital literacy and educational programs for customers should be designed with greater innovation, sustainability, and measurable effectiveness in heightening vigilance against perpetually evolving phishing tactics. It serves as a crucial component of mitigating both inherent risks and potential counterclaims of contributory negligence. Reinforcing internal complaint-handling mechanisms characterized by transparency and a solution-oriented approach is vital for rebuilding customer confidence.

Secondly, it is recommended that the Financial Services Authority, in its regulatory capacity, continue to intensify its oversight of banks' compliance with the implementation of pertinent Financial Services Authority Regulations concerning information technology security, risk management, personal data protection, and consumer protection. Acknowledging the complexities inherent in determining liability in phishing cases, Financial Services Authority could consider issuing more detailed guidelines clarifying the principles or factors governing the allocation of liability for losses between banks and customers, particularly when the issue of contributory negligence emerges. It would foster greater consistency in dispute-resolution practices. Furthermore, the promotion, capacity building, and service outreach of LAPS SJK as a credible consumer dispute resolution forum require ongoing enhancement.

Thirdly, it is imperative for banking customers to continuously enhance awareness regarding phishing risks and exercise maximum caution when conducting online transactions and safeguarding personal data. Furthermore, customers should be empowered with knowledge concerning their legal rights as consumers and possess the understanding and confidence to utilize internal bank complaint procedures and external dispute resolution mechanisms via LAPS SJK should they incur losses due to phishing. Finally, for the academic community and future researchers, ample scope exists for further research into the empirical effectiveness of LAPS SJK in resolving phishing-related disputes, a deeper analysis of court jurisprudence concerning the apportionment of liability in cases involving contributory negligence, and an examination of the impact of emerging technologies (such as Artificial Intelligence - AI) on phishing methodologies and their attendant legal implications.

REFERENCES

Banjarnahor, A. C., & Priyana, P. (2022). Analisis Yuridis Cybercrime terhadap Penanganan Kasus Phising Kredivo. *Hermeneutika: Jurnal Ilmu Hukum, 6*(1), 32-36. https://doi.org/10.33603/hermeneutika.v6i1.6754

Colonial Regulations, *Staatsblad* Number 23 of 1847 on the *Burgerlijk Wetboek voor Indonesie*/the Civil Code. https://jdih.mahkamahagung.go.id/legal-product/kitab-undang-undang-hukum-perdata/detail

Damayanti, M., & Priyono, E. A. (2022). Legal Consequences for LDMO Disclosing Personal Data of Transacting Parties: A Study of Legal Protection. *SIGn Jurnal Hukum, 4*(2), 221-232. https://doi.org/10.37276/sjh.v4i2.217

Ekawati, D. (2018). Perlindungan Hukum terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan. *Unes Law Review, 1*(2), 157-171. https://doi.org/10.31933/law.v1i2.24

Erdiyanto, R. P. (2023). Penipuan Mengatasnamakan Bank Berbentuk Phising. *Jurnal Inovasi Global, 1*(2), 71-79. https://doi.org/10.58344/jig.v1i2.11

Ferdiansyah, D. S., Ameeralia, N. V., Putri, A. A. K., & Fikrie, S. N. (2024). Peran OJK dalam Perlindungan Konsumen terhadap Kebocoran Data pada Konsumen Jasa Keuangan Indonesia. *Media Hukum Indonesia, 2*(3), 301-305. Retrieved from https://ojs.daarulhuda.or.id/index.php/MHI/article/view/482

Gadjong, A. A. (2023). The Agreement of Personal Shopping Service through E-Commerce Platforms: A Case Study of Consumer Protection. *SIGn Jurnal Hukum, 4*(2), 388-401. https://doi.org/10.37276/sjh.v4i2.230

Government Regulation in Lieu of Law of the Republic of Indonesia Number 2 of 2022 on Job Creation (State Gazette of the Republic of Indonesia of 2022 Number 238, Supplement to the State Gazette of the Republic of Indonesia Number 6841). https://peraturan.go.id/id/perppu-no-2-tahun-2022

Hasanudin, A. F., & Babussalam, A. B. (2024). Perlindungan Hukum bagi Korban Kejahatan Phising yang Menguras Saldo M-Banking. *Jurnal Gagasan Hukum, 6*(1), 16-29. https://doi.org/10.31849/jgh.v6i01.18827

Irmawati, E., Pieries, J., & Widiarty, W. S. (2024). Perlindungan Hukum atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif UU No 27 Tahun 2022 tentang Kebocoran Data. *Jurnal Syntax Admiration, 5*(1), 12-27. https://doi.org/10.46799/jsa.v5i1.964

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Ismail, N., Ramlee, Z., & Abas, A. (2022). The Legal Proof of Macau Scam in Malaysia. *Malaysian Journal of Syariah and Law, 10*(1), 23-33. https://doi.org/10.33102/mjsl.vol10no1.307

Juniamalia, A., & Fadlian, A. (2023). Perspektif Undang-Undang Tentang Informasi dan Transaksi Elektronik terhadap Cyber Crime dalam Bentuk Phising. *De Juncto Delicti: Journal of Law, 3*(1), 30-46. https://doi.org/10.35706/djd.v3i1.7985

Law of the Republic of Indonesia Number 1 of 1946 on the Penal Code Regulations. https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/814

Law of the Republic of Indonesia Number 1 of 1960 on Amendment of the Penal Code (State Gazette of the Republic of Indonesia of 1960 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 1921). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1357

Law of the Republic of Indonesia Number 7 of 1992 on Banking (State Gazette of the Republic of Indonesia of 1992 Number 31, Supplement to the State Gazette of the Republic of Indonesia Number 3472). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/622

Law of the Republic of Indonesia Number 10 of 1998 on Amendment to Law Number 7 of 1992 on Banking (State Gazette of the Republic of Indonesia of 1998 Number 182, Supplement to the State Gazette of the Republic of Indonesia Number 3790). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/468

Law of the Republic of Indonesia Number 8 of 1999 on Consumer Protection (State Gazette of the Republic of Indonesia of 1999 Number 22, Supplement to the State Gazette of the Republic of Indonesia Number 3821). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/409

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/138

Law of the Republic of Indonesia Number 8 of 2010 on Prevention and Eradication of the Crime of Money Laundering (State Gazette of the Republic of Indonesia of 2010 Number 122, Supplement to the State Gazette of the Republic of Indonesia Number 5164). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/232

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1683

Law of the Republic of Indonesia Number 27 of 2022 on Personal Data Protection (State Gazette of the Republic of Indonesia of 2022 Number 196, Supplement to the State Gazette of the Republic of Indonesia Number 6820). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1814

Law of the Republic of Indonesia Number 6 of 2023 on Enactment of Government Regulation in Lieu of Law Number 2 of 2022 on Job Creation Into Law (State Gazette of the Republic of Indonesia of 2023 Number 41, Supplement to the State Gazette of the Republic of Indonesia Number 6856). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1825

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1842

Manangin, S. A. (2022). The Clause of the Murabahah Financing Agreement in Sharia Banking. *SIGn Jurnal Hukum, 3*(2), 135-150. https://doi.org/10.37276/sjh.v3i2.160

Manga, A. F. C., & Dianti, F. (2023). Legal Consequences of Unlawful Acts against Banks in Letter of Credit Transactions. *SIGn Jurnal Hukum, 5*(2), 292-311. https://doi.org/10.37276/sjh.v5i2.292

Oktana, R., Akub, S., & Maskun, M. (2023). Social Media in the Process of Evidence of Electronic Information and Transaction Crimes. *SIGn Jurnal Hukum, 4*(2), 320-331. https://doi.org/10.37276/sjh.v4i2.252

Orji, U. J. (2019). Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria. *Tilburg Law Review, 24*(1), 105-124. https://doi.org/10.5334/tilr.137

Paminto, S. R., Amalia, M., Mulyana, A., & Auliya, A. H. (2024). Peran Hukum dalam Melindungi Korban Penipuan Media Sosial Perspektif Sosiologi. *Journal Customary Law, 2*(1), 1-18. https://doi.org/10.47134/jcl.v2i1.3335

Putri, R. A. T., & Sugiyono, H. (2024). Tanggung Jawab Bank terhadap Tindakan Phising dalam Sistem Penggunaan E-Banking (Studi: Kasus Phising pada PT. Bank Rakyat Indonesia (Persero) Tbk). *Jurnal Interpretasi Hukum, 5*(1), 682-690. https://doi.org/10.22225/juinhum.5.1.8318.682-690

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn).

Regulation of Minister of Trade of the Republic of Indonesia Number 72 of 2020 on the Consumer Dispute Resolution Agency (Bulletin Gazette of the Republic of Indonesia of 2020 Number 1039). https://peraturan.go.id/id/permendag-no-72-tahun-2020

Regulation of the Financial Services Authority of the Republic of Indonesia Number 18/POJK.03/2016 on the Implementation of Risk Management for Commercial Banks (State Gazette of the Republic of Indonesia of 2016 Number 53, Supplement to the State Gazette of the Republic of Indonesia Number 5861). https://peraturan.go.id/id/peraturan-ojk-no-18-pojk-03-2016-tahun-2016

Regulation of the Financial Services Authority of the Republic of Indonesia Number 61/POJK.07/2020 on Alternative Dispute Resolution Agencies in Financial Services Sector (State Gazette of the Republic of Indonesia of 2020 Number 290, Supplement to the State Gazette of the Republic of Indonesia Number 6599). https://peraturan.go.id/id/peraturan-ojk-no-61-pojk-07-2020-tahun-2020

Regulation of the Financial Services Authority of the Republic of Indonesia Number 11/POJK.03/2022 on the Implementation of Information Technology by Commercial Banks (State Gazette of the Republic of Indonesia of 2022 Number 5/OJK, Supplement to the State Gazette of the Republic of Indonesia Number 5/OJK). https://peraturan.go.id/id/peraturan-ojk-no-11-pojk-03-2022-tahun-2022

Regulation of the Financial Services Authority of the Republic of Indonesia Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector (State Gazette of the Republic of Indonesia of 2023 Number 40/OJK, Supplement to the State Gazette of the Republic of Indonesia Number 62/OJK). https://peraturan.go.id/id/peraturan-ojk-no-22-tahun-2023

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Sari, P., & Sutabri, T. (2023). Analisis Kejahatan Online Phising pada Institusi Pemerintah/Pendidik Sehari-Hari. *Jurnal Digital Teknologi Informasi, 6*(1), 29-34. https://doi.org/10.32502/digital.v6i1.5620

Sihombing, R. P., Kusno, K., & Siregar, A. A. (2024). Investigative Effectiveness in the Digital Era: A Case Study of Technological Innovation at the Rokan Hilir Police Resort. *SIGn Jurnal Hukum, 6*(2), 52-67. https://doi.org/10.37276/sjh.v6i2.368

Sinaga, E. P., & Maulisa, N. (2022). The Rights of Creditors of Guarantee Holders in a Limited Liability Company Declared Bankrupt. *SIGn Jurnal Hukum, 4*(1), 72-86. https://doi.org/10.37276/sjh.v4i1.171

Sirait, R. U., Sudirman, L., & Disemadi, H. S. (2025). Legal Protection for Banking Institutions in Small and Medium Enterprise Credit Agreements. *SIGn Jurnal Hukum, 6*(2), 468-481. https://doi.org/10.37276/sjh.v6i2.408

Situmeang, S. M. T. (2021). Penyalahgunaan Data Pribadi sebagai Bentuk Kejahatan Sempurna dalam Perspektif Hukum Siber. *Sasi, 27*(1), 38-52. https://doi.org/10.47268/sasi.v27i1.394

Suhyana, F. A., Suseno, S., & Ramli, T. S. (2021). Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain. *SIGn Jurnal Hukum, 2*(2), 138-156. https://doi.org/10.37276/sjh.v2i2.92

Tanudiharja, G. F., Handayani, T., & Yuanitasari, D. (2024). Pertanggungjawaban Hukum Bank atas Kelalaian Melaksanakan Identifikasi dan Verifikasi dalam Penyelenggaraan Layanan Perbankan Digital. *Media Hukum Indonesia, 2*(4), 34-46. Retrieved from https://ojs.daarulhuda.or.id/index.php/MHI/article/view/792

Tompul, V. B. R. (2022). Data Nasabah Dibocorkan oleh Oknum Pegawai Bank. *Binamulia Hukum, 11*(2), 171-176. https://doi.org/10.37893/jbh.v11i2.300

Yusuf, D. M. M., Yola, V., Maiharani, D., & Dwi, E. (2022). Analisis terhadap Modus-Modus dalam Hukum Cyber Crime. *Jurnal Hukum, Politik dan Ilmu Sosial, 1*(2), 64-70. https://doi.org/10.55606/jhpis.v1i2.725