JOURNAL of MUJADDID NUSANTARA
ISSN: 3047-8030 (E)

Received: 28-05-2026 | Accepted: 25-06-2026 | Published: 29-06-2026

Customer Financial Protection and Bank Accountability in Cyber Banking Fraud

Nur Fitri Hariani[1]*, Amirullah[2], Billy Martasandy[3], Fauzan Muttaqien[4], Nuraini Muhammad Daud[5]

[1,2] STAI YAPIS Takalar, Indonesia

[3] Universitas Paramadina, Indonesia

[4] Institut Teknologi dan Bisnis Widya Gama Lumajang, Indonesia

[5] MIN 34 Aceh Utara, Indonesia

Email: nurfitriharianihasan@gmail.com[1]*, amirullahamir908@gmail.com[2], billyymartasandy@gmail.com[3], fauzanmuttaqien99@gmail.com[4], nuraddaudy@gmail.com[5]

ABSTRACT

This study examines the legal protection of customers who suffer financial losses from cyber banking fraud within the Indonesian digital banking system and reconstructs the model of bank liability in response to emerging cybersecurity risks. The novelty of this research lies in the development of an integrated liability reconstruction model that combines proportional liability, enhanced cybersecurity obligations, and mandatory customer compensation mechanisms as a unified framework for customer financial protection. Employing normative legal research with statutory, conceptual, and comparative approaches, the study analyzes banking regulations, consumer protection laws, electronic transaction regulations, and relevant legal doctrines concerning financial accountability in cyberspace. The findings demonstrate that the current regulatory framework remains fragmented and reactive, creating legal uncertainty regarding the allocation of liability between banks and customers in cyber fraud cases. Existing practices frequently place a disproportionate burden on customers by invoking negligence defenses, despite banks exercising substantial control over digital security infrastructures and transaction systems. To address this gap, the study proposes a reconstructed liability model that allocates responsibility according to the degree of control over cyber risks, imposes a heightened duty of cybersecurity compliance on banks, and establishes a customer-centered compensation scheme for unauthorized digital transactions. This model contributes to the advancement of banking law by providing a more balanced framework of accountability and financial protection. Practically, it offers regulatory guidance for policymakers, strengthens institutional responsibility for banks, and supports consumer protection agencies in developing more effective mechanisms for resolving cyber banking fraud disputes.

Keywords: Bank Accountability, Cyber Banking Fraud, Customer Financial Protection, Digital Banking.

INTRODUCTION

Although previous studies have provided valuable insights into customer protection within digital banking environments, important gaps remain in the existing scholarship. Agusthin et al. (2024) examined legal protection against phishing crimes in Indonesian digital banking services and emphasized the need to strengthen consumer protection mechanisms in cyberspace. Similarly, Chairunnisa et al. (2024) analyzed legal protection for victims of phishing and hacking under Indonesian positive law and found that existing legal frameworks face substantial limitations in responding to evolving cybercrime methods. Az-Zahra and Labib (2025) further highlighted the weak legal certainty experienced by victims of cyber banking fraud due to the absence of comprehensive regulations governing institutional accountability in unauthorized digital transactions. Likewise, Dluha and Ariska (2021) focused on legal protection for internet banking users based on consumer protection law and concluded that existing mechanisms remain largely reactive rather than preventive. From a different perspective, Akinbowale et al. (2024) emphasized the importance of integrating fraud investigation and mitigation strategies to strengthen institutional resilience against cyber threats.

Despite these contributions, previous studies primarily concentrate on customer protection, cybercrime prevention, and dispute resolution mechanisms, while providing limited analysis of how legal responsibility should be allocated between customers and banks when cyber banking fraud occurs. Existing scholarship generally treats banks as service providers subject to consumer protection obligations but does not critically examine banks as institutions possessing substantial control over digital infrastructures, cybersecurity systems, authentication mechanisms, and transaction monitoring processes. Consequently, the normative basis for determining the scope and extent of bank accountability in unauthorized digital transactions remains insufficiently developed.

Furthermore, the existing literature has not adequately integrated banking law, consumer protection law, and cyber law into a unified framework capable of addressing the complex legal relationships arising from cyber banking fraud. Most studies adopt a descriptive approach to legal protection and cybersecurity governance without proposing a comprehensive reconstruction of institutional accountability. As a result, significant legal uncertainty persists regarding whether financial losses caused by cyber fraud should be borne by customers, banks, or both parties according to their respective levels of control over cyber risks.

The jurisdictional focus of this study is Indonesia, where the rapid growth of digital banking services has generated new legal challenges concerning customer financial protection and institutional accountability. Although Indonesia has enacted various regulations concerning banking activities, electronic transactions, and consumer protection, these regulatory instruments remain fragmented and do not provide a clear framework for allocating liability in cyber banking fraud cases. This regulatory condition creates uncertainty in the resolution of unauthorized digital transaction disputes and may weaken public trust in digital banking services.

The novelty of this study lies in its reconstruction of bank accountability within cyber banking fraud cases through an integrated legal framework that combines customer financial protection, cybersecurity governance, and institutional responsibility. Unlike previous studies that mainly discuss customer rights or fraud prevention measures, this research specifically develops a normative accountability model based on proportional liability principles, enhanced cybersecurity obligations, and customer-centered financial protection. The proposed framework positions banks not merely as passive intermediaries but as institutions with strategic control over digital security systems and risk-management mechanisms. Therefore, the study argues that the allocation of legal responsibility should reflect the degree of institutional control over cyber risks rather than relying solely on customer negligence as the basis for determining liability.

This theoretical approach contributes to the development of banking and economic law by introducing a risk-based accountability paradigm that responds to the realities of digital financial transactions. It also complements previous findings concerning the need for stronger consumer protection and cybersecurity governance in digital banking systems (Islam et al., 2020; Buchi et al., 2019). Accordingly, this study aims to analyze the weaknesses of existing legal protection mechanisms for victims of cyber banking fraud in Indonesia and to formulate a more responsive model of bank accountability capable of strengthening legal certainty, customer financial protection, and public trust in the digital banking sector.

RESEARCH METHODS

This study employed a qualitative legal research method with an interdisciplinary approach to examine customer financial protection and bank accountability in cyber banking fraud cases within digital banking systems. Qualitative research was selected because the study emphasizes an in-depth understanding of legal norms, regulatory frameworks, and institutional responsibilities related to cyber-based financial crimes. According to Kaelan

(2010), qualitative interdisciplinary research is intended to analyze complex social and legal phenomena comprehensively by integrating various scientific perspectives relevant to the object of study. In this context, the research combines approaches from economic law, banking law, consumer protection law, and cyber law to construct a comprehensive analysis regarding legal protection for customers who suffer financial losses due to digital banking fraud.

This research applied a normative juridical approach supported by conceptual and statutory approaches. The statutory approach was used to analyze regulations governing digital banking transactions, consumer financial protection, electronic transactions, and bank liability in cyber fraud cases. Meanwhile, the conceptual approach was employed to examine legal doctrines and theoretical concepts concerning institutional accountability, customer protection, cybersecurity governance, and digital financial justice. Through these approaches, the study aimed to identify weaknesses within existing legal frameworks and formulate a more responsive model of bank accountability in the digital banking era.

The sources of data in this research consisted primarily of secondary legal materials, including laws and regulations, academic journals, legal doctrines, books, research reports, and relevant scientific publications concerning cyber banking fraud and digital financial protection. The study particularly reviewed recent scholarly discussions related to phishing, hacking, unauthorized digital transactions, and consumer financial rights within banking systems. Data collection was conducted through library research by systematically identifying, reviewing, and classifying legal materials relevant to the research problem. Sugiyono (2016) explains that qualitative research emphasizes the exploration of meanings, interpretations, and contextual understanding of social phenomena through systematic data collection and analysis processes.

The collected data were analyzed descriptively and analytically using qualitative analysis techniques. The analysis process involved interpreting legal norms, comparing existing regulatory frameworks, and evaluating the extent of bank liability in customer financial loss cases caused by cybercrime. Furthermore, the study developed a legal reconstruction framework aimed at strengthening customer financial protection through responsive banking regulations, enhanced cybersecurity obligations, and proportional institutional accountability within digital banking systems. Through this analytical framework, the research is expected to contribute both theoretically and practically to the development of economic law in addressing increasingly sophisticated cyber banking fraud.

RESULTS AND DISCUSSION

Legal Framework and Emerging Patterns of Cyber Banking Fraud

The rapid development of digital banking systems has fundamentally transformed the structure of financial transactions and customer interaction within modern banking institutions. The emergence of mobile banking, internet banking, electronic payment systems, and financial technology integration has accelerated economic efficiency and expanded public access to banking services across various regions of the world. Aker and Mbiti (2010) explained that digital communication technology, particularly mobile-based financial access, significantly contributes to economic development by increasing transaction efficiency and financial accessibility. In the banking sector, digital transformation has encouraged financial institutions to adopt more sophisticated service systems capable of responding to the demands of fast, flexible, and technology-oriented financial transactions. Buchi et al. (2019) further emphasized that banking institutions in the era of the Fourth Industrial Revolution are increasingly dependent on digital infrastructures, algorithmic systems, and integrated online services that reshape traditional banking operations into technology-driven financial ecosystems.

Despite these advantages, the rapid expansion of digital banking has simultaneously generated new legal and cybersecurity vulnerabilities. The increasing dependence on electronic transaction systems has exposed customers to various forms of cyber banking fraud, including phishing, hacking, malware attacks, identity theft, social engineering, unauthorized account access, and OTP theft. Kaur and Ramachandran (2021) argued that the evolution of cybersecurity threats has become increasingly complex due to the sophistication of digital technologies and the growing interconnectivity between users, financial institutions, and online systems. This condition creates broader opportunities for cybercriminals to exploit weaknesses in digital financial systems. The Bangladesh Cyber Threat Landscape Report 2024 identified phishing attacks and credential theft as dominant threats affecting banking consumers and digital financial institutions in contemporary cyber environments (BGD e-GOV CIRT, 2024). Similarly, the study entitled Cyber Fraud and Identity Theft in Bangladesh: A Rising Concern (2025) highlighted that identity theft and unauthorized banking transactions continue to increase due to weak cybersecurity awareness and insufficient preventive mechanisms within digital financial services.

Phishing has become one of the most dominant forms of cyber banking fraud because it manipulates customers psychologically to disclose confidential financial information such as passwords, PINs, and one-time passwords. Agusthin et al. (2024) explained that phishing crimes in digital banking services in Indonesia have evolved from simple deception into highly organized cyber manipulation involving fake websites, fraudulent communication channels, and social engineering strategies. Likewise, Chairunnisa et al. (2024) argued that hacking and phishing attacks against digital banking customers reveal serious weaknesses in legal protection mechanisms because many victims experience financial losses without obtaining adequate legal remedies. In practice, customers are frequently placed in vulnerable positions because banks tend to categorize fraud incidents as customer negligence rather than institutional failure in maintaining digital security systems.

The increasing pattern of cyber banking fraud also reflects the growing gap between technological innovation and legal adaptation. Brici and Achim (2023) observed that the digitalization of public and financial services contributes not only to economic modernization but also to the escalation of economic and financial crimes in cyberspace. This indicates that regulatory systems often fail to keep pace with rapidly evolving cyber threats. Modi et al. (2021), in their analysis of e-banking fraud and legal systems in India, found that legal regulations concerning electronic banking frequently remain fragmented and reactive, thereby creating uncertainty regarding institutional accountability in unauthorized transaction cases. Similar conditions are evident in Indonesia, where legal protection for digital banking customers remains dispersed across banking regulations, electronic transaction laws, and consumer protection frameworks without a comprehensive mechanism specifically addressing cyber banking fraud.

From a legal perspective, the relationship between banks and customers within digital banking systems is increasingly complex because banking services are now highly dependent on electronic infrastructures and third-party technological integrations. Cvijovic et al. (2017) emphasized that modern banking services prioritize customer relationship management through digital interaction systems designed to improve efficiency and customer satisfaction. However, this technological dependency also increases institutional responsibility in maintaining transaction security and protecting customer financial data. Islam et al. (2020) argued that service quality in banking sectors significantly influences customer trust and loyalty, particularly regarding reliability, security, and institutional responsiveness. Consequently, when customers suffer financial losses due to unauthorized digital transactions, the issue extends beyond individual negligence and becomes a matter of institutional accountability and risk governance.

The legal framework governing cyber banking fraud therefore requires a more adaptive and responsive approach capable of balancing technological innovation with customer protection. Existing consumer protection mechanisms are often insufficient because they primarily focus on dispute resolution after losses occur rather than establishing preventive cybersecurity obligations for banking institutions. Dluha and Ariska (2021) noted that legal protection for internet banking users under consumer protection law remains largely reactive and fails to comprehensively address digital financial risks. In response to this challenge, Akinbowale et al. (2024) emphasized the importance of integrating fraud investigation, mitigation strategies, and institutional cybersecurity frameworks within banking systems to strengthen protection against emerging cyber threats.

The increasing sophistication of cyber banking fraud demonstrates the necessity of reconstructing bank accountability within digital financial systems. Malagón Medina (2023) argued that banking institutions possess strategic control over electronic transaction systems and therefore cannot entirely shift responsibility to customers in cases of fraudulent digital transactions. Banks maintain control over authentication systems, transaction monitoring, cybersecurity infrastructure, and fraud detection mechanisms, which places them in a stronger institutional position compared to customers. This perspective supports the argument that legal responsibility in cyber banking fraud should be proportionally distributed based on institutional capacity, risk management obligations, and the principle of prudential banking.

The development of digital financial systems requires stronger regulatory supervision and preventive governance mechanisms. Nababan et al. (2019) emphasized the importance of strengthening regulatory sandbox mechanisms and prudential principles within financial technology systems to ensure institutional accountability and consumer protection. This principle is equally relevant within digital banking services because financial institutions operating in cyberspace must adopt enhanced security standards and adaptive regulatory compliance measures. Therefore, the legal framework concerning cyber banking fraud should not merely focus on criminal punishment but must also emphasize preventive legal protection, institutional accountability, cybersecurity governance, and customer financial justice within increasingly complex digital banking ecosystems.

Regulatory Weaknesses and Bank Accountability in Customer Financial Loss Cases

The rapid expansion of digital banking services has created significant legal and regulatory challenges concerning customer financial protection and institutional accountability in cyber banking fraud cases. Digital transformation in the banking sector has undoubtedly increased efficiency, accessibility, and financial inclusion, yet it has simultaneously intensified vulnerabilities associated with cybercrime, unauthorized transactions, and electronic fraud. Wahyudi and Nugroho (2022) explained that the digital transformation of banking institutions generates both opportunities and risks because financial services increasingly depend on interconnected technological systems that are susceptible to cyberattacks. Similarly, Prasetyo and Hidayat (2021) argued that digital banking development in Indonesia has outpaced the evolution of legal and cybersecurity frameworks, thereby creating gaps in customer protection mechanisms and institutional supervision.

One of the major regulatory weaknesses in digital banking systems lies in the fragmented nature of legal protection governing electronic financial transactions. Existing regulations concerning banking law, electronic transactions, consumer protection, and cybersecurity often operate separately without comprehensive integration capable of addressing complex cyber banking fraud cases. Ningrum and Robekha (2023) noted that cybercrime involving internet banking in Indonesia demonstrates the inadequacy of existing legal regulations in responding to rapidly evolving technological crimes. This fragmentation creates uncertainty regarding institutional liability, especially in cases where customers lose funds through phishing, hacking, or unauthorized account access. In practice, customers frequently encounter difficulties in proving whether financial losses resulted from personal negligence or weaknesses within banking security systems.

The problem becomes more complex because cyber banking fraud increasingly relies on sophisticated manipulation techniques targeting customer psychology and digital behavior. Ramadhanti et al. (2024) explained that phishing operations in cyberspace involve deceptive methods such as fake banking websites, fraudulent text messages, manipulated communication channels, and social engineering practices designed to obtain sensitive customer information. Consequently, cyber fraud is no longer merely a technical cybersecurity issue but also a broader legal problem involving institutional responsibility, customer vulnerability, and digital risk governance. Despite this reality, banking institutions often argue that customers bear full responsibility for losses caused by disclosure of passwords, OTP codes, or personal information. Such arguments demonstrate the imbalance of legal power between customers and financial institutions within digital banking relationships.

Current regulatory systems tend to emphasize reactive dispute resolution mechanisms rather than preventive institutional obligations. Sitorus (2023) observed that legal protection for customers experiencing fraud in digital banking transactions remains limited because regulatory approaches largely focus on complaint handling after losses occur instead of strengthening preventive cybersecurity systems. Similarly, Putrianda (2023) found that customers using internet banking services in Indonesia often face procedural difficulties when seeking compensation for unauthorized transactions. Banks frequently rely on standard contractual clauses and transaction records to reject customer claims, even though customers generally possess weaker bargaining positions and limited technological understanding compared to financial institutions.

This situation reveals significant weaknesses in the implementation of the prudential principle within digital banking governance. Nababan et al. (2019)

emphasized the importance of strengthening regulatory sandbox mechanisms and scoring systems to ensure prudential supervision in digital financial services. However, in practice, many banking institutions continue prioritizing service expansion and technological innovation without adequately balancing cybersecurity investment and customer protection standards. Setyawan (2021) argued that cybersecurity within Indonesian digital banking systems still faces substantial challenges due to insufficient monitoring mechanisms, weak authentication systems, and limited institutional preparedness against sophisticated cyber threats. Consequently, when cyber banking fraud occurs, customers frequently become the primary victims of institutional vulnerabilities embedded within digital banking infrastructures.

The issue of bank accountability in customer financial loss cases therefore becomes increasingly significant within modern financial systems. Malagón Medina (2023) argued that banking institutions possess strategic control over electronic transaction systems and should therefore bear proportional civil responsibility for fraudulent transactions conducted through digital banking channels. Banks control authentication technologies, transaction verification systems, cybersecurity infrastructures, and customer data management processes. Consequently, shifting full responsibility to customers in cases of cyber fraud reflects an imbalance in legal responsibility and contradicts the principle of fairness within consumer protection law. This perspective supports the argument that banks should not merely function as passive intermediaries but must actively ensure transaction security and fraud prevention within digital financial ecosystems.

The growing number of cyber banking fraud cases across various countries further demonstrates the urgency of regulatory reform. Reports from Bangladesh indicate that digital financial fraud has become increasingly widespread within mobile banking and online transaction systems. The Digital Financial Fraud Report published by Prothom Alo (2025) revealed a significant increase in unauthorized digital transactions involving banking and mobile financial services. Similarly, The Daily Star (2025) reported that scammers successfully targeted dozens of bank credit cards and caused substantial financial losses through cyber manipulation techniques. These cases illustrate that cyber banking fraud is not confined to isolated incidents but constitutes a transnational financial crime problem requiring stronger regulatory coordination and institutional accountability.

The expansion of mobile financial services has also intensified cybersecurity concerns within digital banking systems. Rashid (2025) explained that mobile financial services contribute significantly to financial accessibility and economic activity, particularly in developing countries. Sharif et al. (2024) similarly emphasized that mobile financial systems provide substantial economic benefits while simultaneously increasing risks associated with data breaches, fraud, and cyber exploitation. Transparency International Bangladesh (2025) further highlighted that weaknesses in institutional governance and insufficient cybersecurity supervision contribute to rising financial vulnerabilities within digital transaction ecosystems. These findings demonstrate that digital financial inclusion without adequate cybersecurity governance may ultimately expose customers to greater financial risks.

Another regulatory weakness concerns the imbalance between financial literacy development and technological expansion. Rahayu and Santoso (2022) argued that financial literacy plays a crucial role in strengthening financial inclusion and customer awareness regarding digital financial risks. Likewise, Wijaya and Hardianto (2023) emphasized that digital banking education is essential for bridging financial literacy and secure financial participation. However, despite increasing public access to digital banking services, customer understanding regarding cybersecurity risks often remains limited. Banking institutions frequently promote digital convenience and transaction speed without sufficiently educating customers about fraud prevention and cybersecurity awareness. This imbalance contributes to the increasing vulnerability of customers within digital banking environments.

From a broader legal perspective, customer financial protection constitutes an integral component of human rights protection and legal justice. Setiawan (2015) argued that legal protection reflects the state's obligation to ensure justice, security, and equality before the law. In the context of digital banking fraud, this principle implies that customers suffering financial losses due to institutional weaknesses should receive adequate legal protection and effective compensation mechanisms. Furthermore, the relationship between financial supervision institutions and banking regulators also significantly influences the effectiveness of customer protection systems. Zaini (2013) explained that the relationship between Bank Indonesia and the Financial Services Authority (OJK) after the transfer of banking supervisory functions requires effective institutional coordination to ensure financial system stability and consumer protection. Weak coordination between regulatory institutions may ultimately hinder effective supervision of digital banking security and institutional accountability.

The current regulatory framework governing cyber banking fraud remains insufficient to address increasingly sophisticated digital financial crimes. Existing legal systems still tend to prioritize formal transaction verification rather than substantive customer protection and institutional cybersecurity responsibility. Consequently, reconstructing bank accountability within digital banking systems becomes necessary to establish a more balanced legal framework capable of integrating prudential principles, cybersecurity governance, consumer protection, and institutional responsibility in responding to customer financial loss cases caused by cybercrime.

Reconstructing Customer Financial Protection and Bank Liability in Digital Banking Systems

The reconstruction of customer financial protection and bank liability within digital banking systems has become increasingly urgent due to the rapid escalation of cyber banking fraud and the growing dependence of society on electronic financial transactions. Digital banking services have transformed the traditional relationship between banks and customers into a highly technology-dependent interaction in which financial transactions are conducted through mobile applications, internet banking platforms, electronic payment systems, and integrated financial technologies. This transformation has generated substantial economic benefits by improving transaction efficiency, financial accessibility, and customer convenience. Aker and Mbiti (2010) explained that digital communication technologies significantly contribute to economic development by expanding financial access and increasing economic participation within modern societies. Similarly, Rashid (2025) emphasized that mobile financial services have strengthened economic activities and financial inclusion in developing countries by facilitating faster and more accessible financial transactions. However, these technological advancements simultaneously expose customers to increasingly sophisticated cyber risks, including phishing, identity theft, hacking, and unauthorized electronic transactions, thereby requiring stronger legal protection and institutional accountability frameworks. (Aker & Mbiti, 2010; Rashid, 2025).

The existing legal framework governing digital banking systems remains insufficient to address the complexity of cyber financial crimes because current regulations are predominantly reactive rather than preventive. Existing legal systems often focus on dispute settlement after customer losses occur instead of establishing comprehensive obligations for banks to prevent cyber fraud through advanced cybersecurity governance. Agusthin et al. (2024) argued that legal protection for customers against phishing crimes in digital banking services remains weak because regulatory systems have not fully adapted to evolving cybercrime methods. Likewise, Az-Zahra and Labib (2025) observed that customers experiencing losses from phishing and cyber fraud frequently encounter difficulties in obtaining compensation due to the absence of clear standards concerning institutional liability in digital financial transactions. This regulatory weakness demonstrates the need to reconstruct legal principles governing bank responsibility by shifting from a customer-burdened liability model toward a proportional institutional accountability approach capable of reflecting the realities of contemporary digital banking systems. (Agusthin et al., 2024; Az-Zahra & Labib, 2025).

A reconstructed framework of customer financial protection should therefore place cybersecurity governance as a central legal obligation of banking institutions. In digital banking environments, banks possess strategic control over authentication systems, transaction monitoring infrastructures, customer data management, and fraud detection mechanisms. Consequently, banks cannot merely position themselves as passive service providers while transferring cybersecurity risks entirely to customers. Malagón Medina (2023) emphasized that banking institutions maintain substantial control over electronic transaction channels and therefore should bear proportional civil responsibility for fraudulent transactions occurring within their systems. This perspective is reinforced by Setyawan (2021), who argued that cybersecurity within digital banking systems requires continuous institutional supervision, sophisticated security infrastructure, and adaptive technological responses to emerging cyber threats. Accordingly, the reconstruction of bank liability should integrate the principle of enhanced cybersecurity duty, which obligates banks to actively prevent, detect, and mitigate cyber fraud risks affecting customers. (Malagón Medina, 2023; Setyawan, 2021).

The reconstruction of customer protection must also involve the transformation of prudential principles within digital financial governance. Traditional prudential principles primarily emphasize financial stability and institutional solvency, whereas contemporary digital banking systems require prudential standards that additionally prioritize cybersecurity resilience and customer data protection. Nababan et al. (2019) highlighted the importance of strengthening regulatory sandbox mechanisms and prudential supervision within financial technology systems to ensure institutional accountability and customer security. Similarly, Suryanto (2022) explained that data security constitutes a fundamental component of digital banking governance because financial institutions increasingly rely on interconnected technological systems vulnerable to cyber exploitation. Therefore, prudential principles in digital banking should be expanded to include mandatory cybersecurity audits, transaction anomaly monitoring, fraud detection systems, and preventive customer protection mechanisms as integral legal obligations of financial institutions. (Nababan et al., 2019; Suryanto, 2022).

In addition to institutional reform, the reconstruction of customer financial protection also requires stronger regulatory coordination among supervisory authorities responsible for digital financial governance. Zaini (2013) explained that the relationship between Bank Indonesia and the Financial Services Authority (OJK) plays a crucial role in ensuring banking supervision and consumer protection within Indonesia's financial system. However, the rapid evolution of cyber banking fraud demonstrates that institutional coordination among banking regulators, cybersecurity agencies, and law enforcement authorities remains insufficient to address increasingly transnational and technologically sophisticated financial crimes. Rahman et al. (2025), in their comparative study between Bangladesh and Singapore, found that countries with stronger interinstitutional coordination and integrated cybersecurity governance tend to possess more effective mechanisms for preventing online financial scams. Consequently, reconstructing digital banking governance requires the establishment of collaborative regulatory frameworks integrating banking supervision, cybersecurity monitoring, digital forensic investigation, and consumer financial protection into a unified institutional mechanism. (Zaini, 2013; Rahman et al., 2025).

The reconstruction of customer protection should also recognize the importance of balancing technological innovation with customer rights and legal justice. The rapid digitalization of banking systems has increased customer dependence on electronic financial services, yet many customers still possess limited understanding regarding cybersecurity risks and digital transaction vulnerabilities. Rahayu and Santoso (2022) explained that financial literacy significantly influences public participation and security awareness within digital financial ecosystems. Likewise, Wijaya and Hardianto (2023) argued that digital banking education is essential for bridging financial inclusion and secure financial participation. Nevertheless, despite the expansion of digital banking services, many financial institutions continue prioritizing service efficiency and market expansion without adequately strengthening customer cybersecurity awareness. Therefore, reconstructed customer protection frameworks should require banks to implement mandatory digital literacy programs, cybersecurity education initiatives, and transparent fraud prevention guidance as part of their institutional obligations toward customers. (Rahayu & Santoso, 2022; Wijaya & Hardianto, 2023).

Another important aspect of reconstructing bank liability concerns the adoption of proportional liability principles capable of balancing customer responsibility and institutional accountability. Current banking practices frequently rely on standard contractual clauses to deny liability whenever customers disclose passwords, OTP codes, or personal information to third parties. However, this approach fails to recognize the increasingly sophisticated nature of cyber manipulation techniques targeting customer psychology and digital behavior. Ramadhanti et al. (2024) explained that phishing operations increasingly involve highly organized social engineering strategies designed to deceive customers through manipulated communication systems and fake digital interfaces. Similarly, Kaushik (2025) found that online banking scams in India continue to increase because cybercriminals exploit customer trust and institutional security weaknesses simultaneously. These findings indicate that customer negligence cannot be interpreted narrowly because cyber fraud often involves systemic vulnerabilities beyond individual customer control. Consequently, reconstructed liability frameworks should adopt a risk-based accountability model in which banks bear greater responsibility proportional to their technological capacity and institutional control over digital transaction systems. (Ramadhanti et al., 2024; Kaushik, 2025).

From a broader legal perspective, reconstructing customer financial protection in digital banking systems also reflects the realization of legal justice and human rights principles within modern financial governance. Setiawan (2015) argued that legal protection constitutes a manifestation of state responsibility to ensure justice, security, and equality before the law for all individuals. In digital banking contexts, this principle requires states and financial institutions to provide effective legal remedies, fair compensation mechanisms, and adequate institutional safeguards for customers experiencing financial losses due to cybercrime. Furthermore, Islamic legal perspectives concerning social justice and protection of property rights may also strengthen the ethical foundation of customer financial protection within digital banking systems. Riyani (2016) explained that Islamic legal development historically emphasized the formation of social order based on justice and collective protection of community interests. Similarly, Abdur et al. (2022) demonstrated that legal enforcement within Islamic legal systems prioritizes the protection of public welfare and legal certainty. These principles are relevant in constructing modern financial protection systems that emphasize institutional responsibility, fairness, and the protection of customer property rights within increasingly complex digital economies. (Setiawan, 2015; Riyani, 2016; Abdur et al., 2022).

Reconstructing customer financial protection and bank liability within digital banking systems requires a comprehensive legal transformation capable of integrating cybersecurity governance, prudential banking principles, institutional accountability, financial literacy development, and customer rights protection into a unified regulatory framework. Banking institutions should no longer rely solely on formal transaction verification and standard contractual defenses when responding to customer financial losses caused by cyber fraud. Instead, banks must be legally obligated to implement proactive cybersecurity systems, transparent risk mitigation mechanisms, effective fraud detection technologies, and fair compensation procedures reflecting their institutional control over digital financial infrastructures. Through this reconstruction, customer financial protection can evolve from a reactive dispute-resolution model into a preventive and justice-oriented legal framework capable of responding to increasingly sophisticated cyber banking fraud within modern digital financial ecosystems.

CONCLUSION

This study concludes that the rapid development of digital banking systems has significantly increased customer vulnerability to cyber banking fraud, including phishing, hacking, identity theft, and unauthorized electronic transactions. Existing legal frameworks governing customer financial protection and bank accountability remain fragmented, reactive, and insufficiently responsive to the complexity of contemporary cybercrime. The findings demonstrate that current regulations frequently place a disproportionate burden on customers by emphasizing customer negligence while failing to adequately recognize institutional weaknesses in cybersecurity governance and digital transaction systems. As a result, customers who experience financial losses often encounter legal uncertainty and difficulties in obtaining effective remedies and compensation. The study further reveals that the increasing sophistication of cyber fraud requires a more adaptive legal framework capable of integrating banking law, consumer protection law, and cybersecurity governance within digital financial ecosystems.

This research also concludes that reconstructing customer financial protection and bank liability in digital banking systems is necessary to establish a more balanced and justice-oriented regulatory framework. Banks should not merely function as passive financial intermediaries but must bear proportional responsibility for ensuring transaction security, protecting customer data, and preventing cyber fraud through enhanced cybersecurity obligations and proactive risk management systems. The reconstruction of bank accountability should therefore incorporate stronger prudential principles, integrated regulatory supervision, mandatory cybersecurity governance, and customer financial literacy programs as essential components of digital banking regulation. Through this approach, the legal framework for digital banking can provide more effective customer protection, strengthen public trust in financial institutions, and create a more secure and accountable digital financial environment in the era of cybercrime.

REFERENCES

Abdur, S., Agama, P., & Balai, P. (2022). Penegakan Hukum Jinayat bagi Non-Muslim di Aceh. Jurnal Hukum Islam, 11(1), 21–42.

Agusthin, I. D., Nada, D. C., & Putri, N. A. (2024). Perlindungan Hukum Nasabah dari Kejahatan Phising dalam Layanan Perbankan Digital di Indonesia. In Kajian Hukum Siber dan Perlindungan Konsumen (pp. 132–148).

Aker, J., & Mbiti, I. (2010). Mobile Phones and Economic Development in Africa. Journal of Economic Perspectives, 24(3), 207–232. https://doi.org/10.1257/jep.24.3.207

Akinbowale, O., Mashigo, P., & Zerihun, M. (2024). Fraud Investigation and Mitigation. AOSIS. https://doi.org/10.4102/aosis.2024.BK485.02

Az-Zahra, I., & Labib, Z. M. (2025). Perlindungan Hukum bagi Nasabah dalam Kasus Phising dan Siber Perbankan di Indonesia. Yurisprudentia: Jurnal Hukum Ekonomi, 10(2), 405–425. https://doi.org/10.24952/yurisprudentia.v10i2.13952

BGD e-GOV CIRT. (2024). Bangladesh Cyber Threat Landscape 2024. https://www.cirt.gov.bd/documents/bd-cyber-landscape-2024

Brici, I., & Achim, V. (2023). Does the Digitalization of Public Services Influence Economic and Financial Crime? Studies in Business and Economics, 18(2), 67–85. https://doi.org/10.2478/sbe-2023-0025

Buchi, G., Fasolo, L., & Cugna, M. (2019). New Banks in the 4th Industrial Revolution: A Review and Typology. Excellence in Service International Conference Proceedings.

Chairunnisa, S., Murwadji, T., & Harrieti, N. (2024). Perlindungan Hukum Terhadap Nasabah atas Kejahatan Phising dan Hacking pada Layanan Bank Digital Ditinjau Berdasarkan Hukum Positif Indonesia. Hakim: Jurnal Ilmu Hukum Dan Sosial, 2(1), 1–16.

Cvijovic, J., Stankovic, M. K., & Reljic, M. (2017). Customer Relationship Management in Banking Industry: Modern Approach. Industrija Journal, 45(3).

Cyber Fraud and Identity Theft in Bangladesh: A Rising Concern. (2025). IJEDR - International Journal of Engineering Development and Research, 13(2), 193–210. https://rjwave.org/IJEDR/papers/IJEDR2502027.pdf

Dluha, M., & Ariska, Y. I. (2021). Bentuk Perlindungan Hukum Terhadap Nasabah Bank Pengguna Layanan Internet Banking Menurut Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Justness Journal, 1(2), 85–121. https://doi.org/10.61974/justness.v1i2.9

Hakim, R. (2006). Meruy Jenis, Metode dan Pendekatan dalam Penelitian Hukum. Law Review, 5(3).

Islam, R., Ahmed, S., Rahman, M., & Al Asheq, A. (2020). Determinants of Service Quality and Its Effect on Customer Satisfaction and Loyalty: An Empirical Study of Private Banking Sector. The TQM Journal. https://doi.org/10.1108/TQM-05-2020-0119

Kaelan. (2010). Metode Penelitian Agama Kualitatif Interdisipliner. Paradigma.

Kaur, J., & Ramachandran, R. (2021). The Recent Trends in CyberSecurity: A Review. Journal of King Saud University - Computer and Information Sciences, 34(8). https://doi.org/10.1016/j.jksuci.2021.01.018

Kaushik, K. R. (2025). Online Banking Scams with Bank Customers in India: Reasons \& Resolutions. IJSRED - International Journal of Scientific Research and Engineering Development, 8(5), 1070–1073. https://doi.org/10.5281/zenodo.17275581

Malagón Medina, J. A. (2023). Responsabilidad Civil de los Establecimientos Bancarios por la Utilización Fraudulenta de Canales Electrónicos de Disposición de Depósitos y su Relación con los Hábitos Transaccionales de los Consumidores Financieros [Universidad Externado de Colombia]. https://doi.org/10.57998/bdigital/handle.001.169

Modi, S., Premani, V., & Kaur, M. (2021). A Critical Analysis of E-Banking Frauds and Laws in India. International Journal of Health Sciences, 931–938. https://doi.org/10.53730/ijhs.v5nS2.13925

Nababan, M. G., & others. (2019). Penguatan Regulatory Sandbox dan Scoring System dalam Penerapan Prinsip Kehati-Hatian pada Peer-to-Peer Lending. Legislatif, 3(1).

Ningrum, D. P. S., & Robekha, J. (2023). Analisa Yuridis dalam Kasus Kejahatan Siber terhadap Internet Banking di Indonesia. PESHUM: Jurnal Pendidikan, Sosial Dan Humaniora, 2(4), 765–776. https://doi.org/10.56799/peshum.v2i4.2115

Prasetyo, T. A., & Hidayat, R. (2021). Digital Banking in Indonesia: Opportunities and Challenges. Journal of Financial Innovation and Technology, 15(3), 250–270.

Prothom Alo. (2025). Digital Financial Fraud Report. https://en.prothomalo.com/business/local/5oi7ncs555

Putrianda, S. (2023). Analisis Hukum terhadap Perlindungan Nasabah dalam Menggunakan Internet Banking di Indonesia (Studi Kasus Bank X). Dharmasisya: Jurnal Program Magister Hukum, 2(1).

Rahayu, S., & Santoso, D. (2022). Peran Literasi Keuangan dalam Meningkatkan Inklusi Keuangan di Indonesia. Jurnal Ekonomi Dan Bisnis Indonesia, 10(2), 120–140.

Rahman, K., Jiow, H. J., & Lee, B. (2025). Preventing Crimes of Online Scams Across Countries: A Comparative Study Between Bangladesh and Singapore. Social Science Review, 42(1), 45–62. https://doi.org/10.3329/ssr.v42i1.85321

Ramadhanti, A. N., Tias, T. A., Lestari, E. D., & Hosnah, A. U. I. (2024). Cara Operasi Kejahatan Phising di Ranah Siber yang Diatur oleh Hukum Positif Indonesia. Jurnal Pendidikan Tambusai, 8(1), 1299–1305.

Rashid, M. M. (2025). The Impact of Mobile Financial Services in Bangladesh: Usage, Benefits, and Challenges. World Journal of Advanced Engineering Technology and Sciences, 16(2), 271–277. https://doi.org/10.30574/wjaets.2025.16.2.1290

Rasyid, A., & Siregar, S. (2022). Fenomena Menarik Perkawinan Dibawah Umur Menjadi Trend Masa Kini di Bittuju Tapanuli Selatan. AL-MANHAJ: Jurnal Hukum Dan Pranata Sosial Islam, 4(1), 61–68. https://doi.org/10.37680/almanhaj.v4i1.1571

Riyani, I. (2016). Menelusuri Latar Historis Turunnya Alquran dan Proses Pembentukan Tatanan Masyarakat Islam. Al-Bayan: Jurnal Studi Ilmu Al-Qur'an Dan Tafsir, 1(1), 27–34. https://doi.org/10.15575/al-bayan.v1i1.873

Setiawan, A. (2015). Perlindungan Hukum dalam Perspektif Hak Asasi Manusia. Jurnal Ilmu Hukum, 7(2), 123–135.

Setyawan, D. (2021). Cybersecurity in Digital Banking: A Case Study in Indonesia. International Journal of Banking Technology, 12(4), 389–402.

Sharif, J. B., Hasan, M., Kwosar, M., Ahmed, M. F., & Mandal, P. (2024). A Short Review of Mobile Financial Services in Bangladesh. World Journal of Advanced Research and Reviews, 23(2), 2479–2485. https://doi.org/10.30574/wjarr.2024.23.2.2610

Siregar, S., & Mardiah, M. (2021). Relevansi Term Kafa'ah pada Pernikahan Adat Batak Mandailing Natal. Jurnal Al-Maqasid: Jurnal Ilmu-Ilmu Kesyariahan Dan Keperdataan, 7(2), 290–302.

Sitorus, H. A. M. (2023). Perlindungan Hukum terhadap Nasabah atas Fraud pada Transaksi Bank Digital. JISIP (Jurnal Ilmu Sosial Dan Pendidikan), 7(1). https://doi.org/10.58258/jisip.v7i1.4428

Sugiono. (2016). Metode Penelitian Kuantitatif, Kualitatif Dan R & D (Bandung: Alfabeta).

Suryanto, D. (2022). Keamanan Data dalam Era Digitalisasi Perbankan. Gadjah Mada University Press.

The Daily Star. (2025). Scammers Target 50 SCB Credit Cards, Steal BDT 27 Lakh: Report. https://www.thedailystar.net/tech-startup/news/scammers-target-50-scb-credit-cards-steal-bdt-27-lakh-report-3992241

Transparency International Bangladesh. (2025). Executive Summary: Mobile Financial Services Sector in Bangladesh. https://www.ti-bangladesh.org/images/2025/report/mfs/Executive-Summary-Mobile-Financial-Services-Sector-En.pdf

Wahyudi, T., & Nugroho, A. (2022). Transformasi Digital di Sektor Perbankan: Peluang dan Tantangan. Jurnal Transformasi Digital, 8(1), 45–60.

Wijaya, B., & Hardianto, F. (2023). Digital Banking Education: Bridging Financial Literacy and Inclusion. International Journal of Financial Studies, 11(1), 75–90.

Zaini, Z. D. (2013). Hubungan Hukum Bank Indonesia sebagai Bank Sentral dengan Otoritas Jasa Keuangan (OJK) Pasca Pengalihan Fungsi Perbankan. Jurnal Media Hukum, 20(2).