AL RISALAH: Jurnal Ilmu Syariah dan Hukum

VOLUME 26 NO 1, MAY 2026
P-ISSN: 2252-8334 / E-ISSN: 2550-0309
This work is licensed under a Creative Commons Attribution 4.0 International License
https://doi.org/10.24252/al-risalah.vi.67932

Banking Legal Liability of Cybercrime for the Loss of Customer Funds in Indonesian Digital Banks

Fatur Rezqy Permana[1*], Rianda Dirkareshza[2]
[1]*E-mail : 2210611323@mahasiswa.upnvj.ac.id*
[2]*E-mail : riandadirkareshza@upnvj.ac.id*
[1,2]*Universitas Pembangunan Nasional Veteran Jakarta, Indonesia*
*corresponding author

Article history:
Received in revised form: 28 April 2026
Acceptance date: 14 May 2026
Available online: 31 May 2026

Keywords:
Digital Banking, Cybercrime, Legal Liability, Consumer Protection.

How to Cite:
Permana, F. R., & Dirkareshza , R. (2026). Banking Legal Liability of Cybercrime for the Loss of Customer Funds in Indonesian Digital Banks. Al-Risalah Jurnal Ilmu Syariah Dan Hukum.
https://doi.org/10.24252/al-risalah.vi.67932

License:
Copyright (c) The authors (2026)
This work is licensed under a Creative Commons Attribution 4.0 International License.

Abstract
The rapid transformation of financial services into the digital realm poses serious threats in the form of cybercrimes, which frequently lead to massive losses of customer funds. This phenomenon triggers disputes and a liability gap between banks and customers. This research aims to analyze the current legal liability framework of digital banking in Indonesia and formulate a more equitable ideal model. Utilizing a normative legal research method supplemented by in-depth interviews, the approaches applied include statutory, case, and conceptual approaches. The results indicate that although recent regulations, such as the Consumer Protection Law and POJK No. 22 of 2023, have obliged banks to actively manage cyber risks, in practice, banks still frequently hide behind the pretext of customer negligence. The conclusion of this study offers a solution by adopting the UK-style shared liability model, which applies the shifting burden of proof to the bank. Therefore, it is recommended that the Financial Services Authority (OJK) revise the aforementioned POJK and issue a lex specialis technical regulation regarding compensation procedures and the proportional distribution of loss burdens among banks.

INTRODUCTION

Banks are business entities engaged in the mobilization of funds from the public, the distribution thereof, and the provision of other financial services. Along with rapid technological advancements, significant changes have occurred in various aspects of life, including the financial services sector, which is currently undergoing a transformation into the digital realm. The public's demand for fast, practical, and accessible services at any time and in any location has significantly altered the landscape of the banking world. Nowadays, banking institutions no longer rely solely on physical branch operations but have begun a massive transition toward digital-based services to meet the demands of an increasingly modern customer base. One form of rapidly evolving innovation resulting from this phenomenon is the birth and proliferation of various digital banking entities in Indonesia.[1]

However, behind the various conveniences offered, digital banking services also face serious challenges, particularly regarding the high perception of risk among users. Transaction security, personal data protection, and vulnerability to cybercrime have become crucial aspects frequently highlighted, given that the majority of current attacks operate in a decentralized manner and directly target the weakest point in the banking ecosystem, namely the customers themselves.[2] Criminal threats such as phishing, digital fraud via the transmission of malicious files, the manipulation of artificial intelligence for deepfakes, and unauthorized number takeovers through SIM Swap Fraud have become real threats that often lead to massive financial losses.[3] As a tangible and relevant case in Indonesia, in mid-2023, a businessman from Malang, East Java, named Silvia Yap, suffered financial losses amounting to IDR 1.4 billion overnight. The funds in her bank account were completely drained after she inadvertently clicked and downloaded an APK-formatted file sent via WhatsApp from an unknown number,[4] wherein the malicious file (malware) was disguised as a digital wedding invitation application. This case serves as empirical evidence demonstrating how dangerous social engineering

[1] Irinwantin, *Mengenal Bank Digital* (Jakarta: Fastindo, 2023).
[2] Tri Sulistiawati, Deri Yansyah, and Nova Yanti Maleha, "Analisis Persepsi Risiko Dalam Layanan Digital Banking Di Indonesia: Tantangan Dan Solusi," *Jurnal Ekonomi Bisnis, Manajemen Dan Akuntansi (JEBMAK)* 4, no. 1 (2025): 212–23.
[3] Hendarto, "Tanggung Jawab Bank Dalam Mengantisipasi Dan Menangani Kerugian Nasabah Akibat Scam Melalui Link Phising Pada Mobile Banking," *Iuris Studia: Jurnal Kajian Hukum*, 2023, 760.
[4] Muhammad Aminudin, "Warga Malang Kehilangan Uang Rp 1,4 M Di Rekening Usai Klik Undangan Palsu," *DetikNews*, 2023, https://news.detik.com/berita/d-6811004/warga-malang-kehilangan-uang-rp-1-4-m-di-rekening-usai-klik-undangan-palsu.

modes are in exploiting customer oversight in the current digital banking era.[5]

This phenomenon gives rise to complex juridical implications and triggers a liability gap between the bank and the customer. When customer funds are lost due to a cyberattack, disputes regarding responsibility frequently arise. On one hand, banks tend to argue that losses are caused by the customer's negligence in maintaining the confidentiality of authentication data such as PINs and OTPs (One-Time Passwords). On the other hand, customers feel victimized by the failure of the bank's security system to protect their funds, which should be grounded in the prudential principle as mandated by law. The current legal framework, such as Law Number 10 of 1998 concerning the Amendment to Law Number 7 of 1992 concerning Banking (Banking Law) and Law Number 8 of 1999 concerning Consumer Protection (Consumer Protection Law),[6] whose regulation was reaffirmed through Law Number 4 of 2023 concerning the Development and Strengthening of the Financial Sector (P2SK Law),[7] These regulations were essentially established in an era when cybercrime was not as complex as it is today, resulting in many gaps that cannot yet address various forms of online fraud and evolving crimes. This condition indicates the need for legal updates that are clearer, more adaptive, and capable of adjusting to the realities of modern financial technology.[8]

Rapid digitalization of banking, while encouraging financial inclusion, has exposed increasingly complex operational and security risks, leading to customer losses and triggering liability disputes. Addressing this challenge, the P2SK Law was enacted to strengthen the entire financial architecture, with a specific focus on technology risk and consumer protection. A deeper legal analysis demonstrates that if the Consumer Protection Law provides a broad legal umbrella,[9] the existence of Financial Services Authority Regulation Number 21 of 2023 concerning Digital Services by Commercial Banks (Digital Services POJK),[10] and Financial Services Authority Regulation Number 22 of 2023 on Consumer And Community Protection in the Financial Services Sector

---

[5] Y S Kristiyenda and T S Ramli, "Pelindungan Hukum Bagi Nasabah Bank Digital Terhadap Ancaman Pencurian Data Melalui BTS Palsu (Fake BTS)," *Causa: Jurnal Hukum Dan Kewarganegaraan* 13, no. 2 (2025).
[6] Republik Indonesia, "Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen," 1999.
[7] Republik Indonesia, "Undang-Undang Nomor 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan," 2023.
[8] Asmaru Amru, Naufal Adil, and Novah Patilani, "Perlindungan Hukum Terhadap Penanggulangan Kejahatan Siber Di Sektor Perbankan Digital Indonesia," *Journal of Scientech Research and Development* 7, no. 1 (2025): 587–88.
[9] E Dori et al., "Analisis Hukum Transparansi Perbankan Dan Stabilitas Keuangan Pasca Perubahan POJK No. 37/2019 Menjadi POJK No. 18/2025," *Al-Zayn: Jurnal Ilmu Sosial \& Hukum* 4, no. 1 (2026): 1028–37.
[10] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 Tentang Layanan Digital Oleh Bank Umum," 2023.

(Consumer Protection POJK),[11] as a mandate of the P2SK Law significantly clarifies and operationalizes these principles. This POJK provides a very specific technical foundation for the financial services sector, wherein the bank's obligations no longer end at providing a transaction platform but have shifted to include the obligation to actively manage, mitigate, and respond to cyber risks. This marks a shift in role from mere service providers to guardians of their digital ecosystem's security. Therefore, it is important to analyze how this new legal framework has juridical implications for the construction of digital bank legal liability when customer fund loss disputes occur.[12]

Consumer Protection Law encourages changes in the burden of proof for digital bank customer fund loss cases. The imbalance in access and technical capabilities places customers in a weak position, while banks control all data and transaction systems. Consequently, in fund loss disputes, it is difficult for customers to prove whether the cause originated from their own negligence or the bank's security weaknesses.[13] The importance of shifting the burden of proof is to create more equitable legal liability. Banks must prove that their security systems have met standards and that the losses truly occurred due to the customer's gross negligence. Effective legal protection highly depends on the interpretation of regulators and courts regarding the concept of "bank negligence" in the digital age. The focus is no longer on blaming the customer but on ensuring that banks perform their primary role in maintaining security, preventing cybercrime, and providing education to customers.[14]

Legally, urgency arises because there are still gaps or vacuums in the current applicable regulations. Although the Consumer Protection Law and the latest POJK have been issued, their implementation is still hindered by the technical complexity of cybercrime.[15] There is a mutual passing of responsibility between banks and customers because there are no clear standards regarding "negligence" and the burden of proof. This uncertainty must be immediately addressed so as not to disadvantage customers as

[11] Otoritas Jasa Keuangan, "Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan," 2023.
[12] Syukron, "Peran OJK Dalam Melindungi Konsumen Dan Masyarakat Di Sector Jasa Keuangan," *Yurisprudentia: Jurnal Hukum Ekonomi* 8, no. 2 (2022): 192.
[13] Nur Hidayah, Baidhowi, and Yustina Dhian Novita, "Perlindungan Hukum Bagi Pengguna Layanan Internet Banking Menurut Undang-Undang No. 8 Tahun 1999 Tentang Perlindungan Konsumen," *Media Hukum Indonesia* 2, no. 7 (2025): 22–28.
[14] Lies Norma Tri Utami and others, "Perlindungan Hukum Bagi Pengguna Layanan Bank Digital Di Era Globalisasi," *Journal of Multidisciplinary Inquiry in Science Technology and Educational Research* 2, no. 1 (2025): 197.
[15] B S Fithri and W S Wahyuni, *Hukum Pidana Perbankan*, 2025.

the weaker party.[16]

Therefore, writing a journal titled "Banking Legal Liability Of Cybercrime For The Loss Of Customer Funds In Indonesian Digital Banks" becomes very important and relevant to study. This research not only maps existing regulations but crucially aims to bridge these legal gaps. By deeply analyzing the practice of implementing the prudential principle and the burden of proof, this writing is expected to provide constructive thought contributions to encourage the creation of an innovative, safe, and fair digital banking ecosystem. Based on the background description, the main problems to be answered in this research are focused on two things, namely: how is the legal liability regulation of digital banks regarding customer funds lost due to cybercrime based on current laws and regulations in Indonesia and what is the ideal legal liability model to provide fairer and more effective protection for digital bank customers in the future.

METHOD

This research is normative legal research complemented by interviews, which aims to evaluate the compatibility of digital bank liability rules with the principles of justice in society.[17] The problem approaches used include the statute approach, the case approach related to cyber threats such as phishing, deepfakes, and SIM Swap Fraud, and the conceptual approach to analyze legal doctrines and principles. Data sources in this research are divided into two, namely secondary data and primary data. Secondary data consists of legal materials comprising: authoritative primary legal materials (Law No. 8 of 1999, Law No. 4 of 2023, POJK No. 21 of 2023, and POJK No. 22 of 2023); secondary legal materials (legal literature and journals); and tertiary legal materials (encyclopedias, legal dictionaries, and online news). Meanwhile, primary data were obtained directly from the field through relevant informants to complement the normative analysis.

Data collection was conducted through a combination of library research. Library research was carried out by examining various laws and regulations, legal literature, and expert views to map legal norms descriptively and systematically. As a crucial support, in-depth interviews were directed to authorized Digital Bank parties, such as representatives from the Compliance Division, Information Technology Risk Management, or the Legal Division. These interviews aim to gather practical information regarding handling procedures, the implementation of security standards, and the

[16] Melinda Putri Lutfi, Ela Kurniasari, and Fadilla Elza Aida Putri, "Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank Di Era Perkembangan Digital," *Jurnal Multidisiplin Ilmu Akademik* 1, no. 5 (2024): 211–14.
[17] Peter Mahmud Marzuki, *Penelitian Hukum: Edisi Revisi* (Prenada Media, 2017).

compensation mechanisms applied by digital banks when facing cases of customer fund loss due to cybercrime in the field.

All collected data were subsequently analyzed using qualitative data analysis techniques. The analysis process was conducted inductively by interpreting and elaborating on legal data (library) and field data (interviews) in detail. Library data were analyzed to formulate the ideal concept of fair digital bank legal liability, while interview data were used to understand the reality of implementing such liability. Through this comparative and comprehensive analysis between normative rules and empirical reality, the researcher will draw conclusions that systematically answer the main problems regarding banking legal protection and liability for the loss of customer funds in Indonesian digital banks.

RESULTS AND DISCUSSIONS

1. Regulation of Digital Bank Legal Liability for Customer Funds Lost Due to Cybercrime Based on Current Laws and Regulations in Indonesia

Construction of digital bank liability for the loss of customer funds in Indonesia is regulated in a multi-layered manner, with the Consumer Protection Law as the primary legal umbrella and financial sector regulations as specific rules (*lex specialis*). Pursuant to the Consumer Protection Law, banks as business actors bear strict liability to provide compensation for every loss experienced by consumers resulting from the use of their services.[18] However, in the dynamic context of cybercrime, these provisions are reinforced and expanded by the P2SK Law and its derivative regulations, namely POJK No. 22 of 2023 concerning Consumer Protection and POJK No. 21 of 2023 concerning Digital Services. This latest regulation fundamentally transforms the bank's liability paradigm, shifting from a mere platform provider to a party obligated to actively implement cyber risk management.[19] This implies that the law mandates banks to possess reliable fraud detection systems and conduct real-time monitoring of suspicious transactions. Consequently, a bank's failure to mitigate risks or detect transaction anomalies can be qualified as an unlawful act (*tort*) that necessitates compensation, regardless of whether the customer contributed to the incident or not.[20]

From a doctrinal perspective, the construction of digital banking liability outlined

[18] T Tasman and U Ulfanora, "Perlindungan Hukum Terhadap Nasabah Bank Digital," *UNES Law Review* 6, no. 1 (2023): 1624–35.
[19] F U Rianda, "Urgensi Pengaturan Central Bank Digital Currency Untuk Melindungi Data Pribadi Dari Cybercrime Di Indonesia" (Universitas Islam Negeri Maulana Malik Ibrahim, 2025).
[20] M Ghozali et al., "Kejahatan Siber (Cyber Crime) Dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)," *Cendekia: Jurnal Hukum, Sosial Dan Humaniora* 2, no. 4 (2024): 797–809.

above can be theoretically situated within several mutually reinforcing legal frameworks. First, Hans Kelsen's theory of legal responsibility (*theorie der Verantwortlichkeit*) distinguishes between liability premised on fault (*Schuldhaftung*) and liability attached to the mere occurrence of a particular result (*Erfolgshaftung*).[21] The architecture of POJK Number 22 of 2023, by obliging banks to actively manage cyber risk irrespective of customer behaviour, demonstrates a normative gravitation toward the latter paradigm in the digital banking context. Second, the theory of legal protection developed by Philipus M. Hadjon distinguishes between preventive legal protection—directed at averting disputes through clear normative standards and adequate institutional safeguards—and repressive legal protection—directed at the *ex post* resolution of disputes through compensation and adjudication.[22] The dual obligation imposed upon banks to operate robust fraud detection systems (preventive) and to provide accessible complaint and compensation mechanisms (repressive) reflects the integration of both dimensions within Indonesia's current regulatory framework.

Third, the prudential banking principle, codified in Article 2 of the Banking Law, requires banks to conduct their business with the utmost prudence; in the digital era, this principle has expanded to encompass the affirmative obligation to invest in adaptive cybersecurity infrastructure capable of detecting and intercepting transactional anomalies in real time.[23] Fourth, the doctrine of strict liability, originally developed in the context of hazardous activities and environmental protection, finds analogical application in the digital banking sector because the asymmetry of information and technical capacity between banks and customers renders the conventional fault-based regime structurally inadequate to safeguard the weaker party. Read in concert, these four theoretical lenses converge on a single normative conclusion: the legitimate construction of digital banking liability in Indonesia must shift away from a fault-centric model that places the evidentiary and substantive burden on the customer toward a model of institutional accountability in which the bank, as the controller of the technological

[21] Ridwan HR, "Pertanggungjawaban Publik Pemerintah Dalam Perspektif Hukum Administrasi Negara," *Jurnal Hukum IUS QUIA IUSTUM* 10, no. 22 (2003): 27–38, https://doi.org/10.20885/iustum.vol10.iss22.art3; Shofiy Zulfah, Bunga Jasmine Puji Hapsari, and Faza Rusda, "Legal Responsibility of Digital Commerce Platforms for Seller Content That Violates Public Ethics," *Indonesia Media Law Review* 4, no. 1 (2025).

[22] Zennia Almaida and Moch Najib Imanullah, "Perlindungan Hukum Preventif Dan Represif Bagi Pengguna Uang Elektronik Dalam Melakukan Transaksi Tol Nontunai," *Privat Law* 9, no. 1 (2021): 218–26; Philippus M Hadjon, *Perlindungan Hukum Bagi Rakyat Indonesia* (Surabaya: PT. Bina Ilmu, 1999).

[23] Marc Lacoursière, "Les Méthodes Alternatives de Résolution Des Conflits Au Service de La Protection Des Consommateurs de Services Bancaires En Ligne Dans Les Amériques," *Banking & Finance Law Review* 21 (2005): 357.

infrastructure, bears the primary duty to prevent loss and to demonstrate the absence of fault when loss occurs.

Referring to the realities occurring in the field as explored through in-depth interviews with the banking sector, it is emphasized that banks as institutions of trust have a fundamental obligation to provide excellent service and guarantee the security of customer funds. In the context of legal liability, the banks expressed their commitment to be fully liable if the loss of funds or customer data is proven to be caused by internal factors, such as procedural negligence by officers or operational errors by the bank.[24] However, realization of this liability is not necessarily carried out solely based on a unilateral report from the customer.[25] Banks implement strict standard procedures through a series of investigation and evidentiary processes to ensure claim validity and to determine the actual location of fault objectively.

On the other hand, digital banks emphasize the limits of their liability, particularly regarding incidents arising from the customer's own negligence. Banks will not assume the responsibility for compensation if the financial loss is proven to be caused by the customer's error. Nevertheless, as a form of consumer protection, banks continue to provide reporting space and responsive complaint mechanisms to assist customers who experience a loss of money. This demonstrates that although banks reject liability for customer errors, they continue to perform administrative functions to facilitate the handling of problems experienced by consumers.

Furthermore, based on the experience of handling disputes in the field, there are specific scenarios that require banks to be willing to provide liability in the form of compensation. Such scenarios include incidents where hackers succeed in stealing data directly from the bank's system, the existence of fraudulent acts intentionally committed by internal banking personnel, and the occurrence of technical failures in the system infrastructure, such as system freeze errors or technical faults detrimental to customer funds. In these three conditions, the bank acknowledges a failure in its security or oversight system; thus, the restoration of customer rights becomes an absolute obligation that must be fulfilled.

When the theoretical frameworks set out earlier are read against this empirical reality, a critical disjunction becomes visible. Although the statutory architecture has formally

[24] John Bert Christian et al., "Analisis Hukum Atas Penerapan Rahasia Bank Di Indonesia Terkait Dengan Perlindungan Data Nasabah Berdasarkan Prinsip Kepercayaan Kepada Bank (Studi Pada Pt. Bank Cimb Niaga Tbk Cabang Medan)," *USU Law Journal* 4, no. 4 (2016): 164935.
[25] Hidayah, Baidhowi, and Novita, "Perlindungan Hukum Bagi Pengguna Layanan Internet Banking Menurut Undang-Undang No. 8 Tahun 1999 Tentang Perlindungan Konsumen."

elevated the bank's position to that of an active risk manager bound by the prudential principle and exposed to a strict-liability-oriented regime, the operational practice disclosed through the interviews indicates that banks continue to anchor their liability determinations on a fault-based paradigm centred on customer negligence outside the three narrow scenarios acknowledged above. The structural imbalance described by Hadjon—in which the consumer occupies a weaker bargaining and evidentiary position vis-à-vis the bank—remains insufficiently addressed in practice, because customers are institutionally burdened with proving the bank's security failure despite lacking access to the bank's internal systems and forensic data. This implementation gap demonstrates that doctrinal reform alone is insufficient that is required a regulatory mechanism capable of operationalising the theoretical commitment to consumer protection through concrete shifts in the burden of proof and the proportional distribution of loss, which constitutes the analytical premise for the discussion that follows.

2. Ideal Legal Liability Model to Provide Fairer and More Effective Protection for Digital Bank Customer in the Future

Currently, a phenomenon of mutual shifting of responsibility between customers and digital banks frequently occurs when financial losses arise due to cybercrime. Criminal actors continue to innovate using increasingly sophisticated modes, ranging from fraud through the transmission of malicious files, psychological manipulation using artificial intelligence (deepfake), to authorization takeover through SIM Swap Fraud. In facing such incidents,[26] banks tend to hide behind the argument that the loss was purely caused by the customer's negligence in maintaining the confidentiality of authentication data, such as PINs and OTPs. Conversely, customers feel victimized by the fragility of the bank's security system. In reality, these losses often do not stand alone as mere customer fault. Although a customer may unknowingly open a hacking gap, the bank also shares culpability if it is proven not to have implemented multi-layered security systems and lacks a sufficiently robust Fraud Detection System (FDS) to detect such transaction anomalies in real-time. This deadlock condition is what triggers the complexity of resolving liability issues.[27]

From a theoretical standpoint, the impasse described above is a paradigmatic illustration of the limitations of formal corrective justice when applied to digitally mediated and structurally asymmetric relationships. John Rawls's theory of justice as

[26] M K Faridi, "Kejahatan Siber Dalam Bidang Perbankan," *Cyber Security Dan Forensik Digital* 1, no. 2 (2018): 57–61.
[27] Rudi Margono, *Kejahatan Perbankan: Teknis Pembuktian Dan Perlindungan Nasabah* (Profesor Rudi Margono, 2026).

fairness furnishes a normative foundation for redesigning the liability framework:[28] in a context where one party (the bank) controls the entire informational and technological infrastructure while the other (the customer) controls neither, the principles of equal liberty and the fair distribution of social burdens cannot be realised through formal equality alone; rather, they demand a structural reallocation of risk that systematically favours the more vulnerable party, in a manner analogous to the operation of the difference principle. Complementarily, the theory of responsive law advanced by Philippe Nonet and Philip Selznick posits that legal systems mature when they evolve from autonomous rule-based legality toward a responsive orientation that integrates substantive purposes and adaptive problem-solving capability;[29] the rigidity of fault-based liability in the face of digital cybercrime is precisely the form of legal formalism that responsive law is designed to transcend. Furthermore, although the doctrine of *res ipsa loquitur* is traditionally associated with common law negligence, it offers a useful conceptual scaffold for the shifting burden of proof in digital banking contexts, since the occurrence of an unauthorised transaction within a closed banking system controlled exclusively by the bank gives rise to a reasonable, rebuttable presumption of inadequate institutional safeguards.

In addition to these substantive theories, the comparative discussion that follows between the United Kingdom and Indonesia must be situated within the framework of legal transplantation theory developed by Alan Watson and refined by subsequent comparative scholars.[30] Watson's thesis—that legal rules can be transplanted across jurisdictions notwithstanding differences in socio-legal context—provides the methodological warrant for the comparison undertaken here.[31] However, the more nuanced position advanced by Pierre Legrand and Otto Kahn-Freund cautions that legal transplants are rarely mechanical and that the receiving system must creatively adapt the imported norm to its own institutional matrix, otherwise the transplant risks rejection or distortion. This theoretical reservation is especially pertinent for Indonesia, whose civil law tradition, regulator-led financial supervision architecture, and unique cybercrime typology demand a contextualised rather than literal adoption of the United Kingdom model. The comparative analysis that follows therefore proceeds not as an exercise in

[28] John Rawls, *Justice as Fairness: A Restatement* (Harvard University Press, 2001).
[29] Philippe Nonet and Philip Selznick, *Hukum Responsif* (Bandung: Nusa Media, 2018).
[30] Alan Watson, "From Legal Transplants to Legal Formants," *Am. J. Comp. L.* 43 (1995): 469.
[31] Alan Watson, "The Birth of Legal Transplants," *Ga. J. Int'l \& Comp. L.* 41 (2012): 605; Przemyslaw Kusik, "The Legal Transplant Theory as a Paradigm of Comparative Law: An Attempt at a Summary on the 50th Anniversary of the Publication of Legal Transplants: An Approach to Comparative Law by Alan Watson," in *Forum Prawnicze*, 2024, 42.

legal mimicry but as a structured search for transplantable normative components that can be re-engineered to address the specific contours of the Indonesian legal and institutional landscape.

To overcome the polemic of shifting responsibility, a regulatory breakthrough is required through the development of a more equitable liability model. As a comparative reference, Indonesia can adapt the protection model implemented in the United Kingdom, namely the Mandatory Reimbursement regulation for Authorised Push Payment (APP) Fraud cases.[32] This regulatory model is designed in a measured manner so as not to unilaterally impose the burden of loss on one party only.[33] In its application, the most relevant approach to be implemented is a shared liability scheme, where the burden of loss is distributed proportionally.[34]

In practice, this British model totally transforms the way cases are handled through a system of shifting the burden of proof. If previously customers had to struggle to prove that the bank's security system was weak, under this rule, it is actually the bank that is obligated to reimburse the customer's lost money. The bank can only refuse such compensation if they are able to legally prove that the customer committed "gross negligence," for example, by being proven to have intentionally ignored emergency warnings displayed by the bank's application system. Interestingly, this model applies a 50:50 loss-sharing scheme.[35] However, this division is not imposed between the bank and the customer but is divided fairly between the sending bank and the receiving bank of the fund flow. This means 50% of the loss is borne by the originating bank because it is deemed to have failed to detect its customer's transaction anomalies, and the remaining 50% is borne by the receiving bank because it is considered negligent in allowing the creation of a fraudulent account (mule account) used by the criminal.[36]

For reference, the United Kingdom has implemented the Mandatory Reimbursement scheme through the Payment Systems Regulator (PSR) with the Specific Direction 20

[32] Kusik, "The Legal Transplant Theory as a Paradigm of Comparative Law: An Attempt at a Summary on the 50th Anniversary of the Publication of Legal Transplants: An Approach to Comparative Law by Alan Watson."
[33] Jo Braithwaite, "'Authorized Push Payment'Bank Fraud: What Does an Effective Regulatory Response Look Like?," *Journal of Financial Regulation* 10, no. 2 (2024): 174–93.
[34] Chen Yang, "Protecting Financial Consumers from Authorized Push Payment Fraud: Is Reimbursement an Optimal Solution?," *Journal of Financial Regulation and Compliance* 33, no. 4 (2025): 642–53; Garrett S Grewal, "Combating Authorized Push Payment Fraud: Which Regulatory Approach Should the United States Adopt?," *NC Bank. Inst.* 30 (2026): 385.
[35] Katelyn Wan Fei Ma, Tarundeep Dhot, and Mohsen Raza, "Considerations for Using Artificial Intelligence to Manage Authorized Push Payment (APP) Scams," *IEEE Engineering Management Review* 51, no. 3 (2023): 166–79.
[36] UK Parliament, "Financial Services and Markets Act 2023," 2023.

(SD20) instrument, which is a direct derivative rule of the Financial Services and Markets Act 2023.[37] This Mandatory Reimbursement constitutes a 50:50 loss-sharing between banks. If this model is adopted in Indonesia, the Financial Services Authority (OJK) needs to take two strategic steps concurrently. First, revising POJK Number 22 of 2023 to overhaul its legal foundation, namely by removing standard clauses that exempt banks from liability and replacing them with norms for the shifting of the burden of proof and absolute compensation so that no legal conflict occurs in the future. Second, once the umbrella rule is improved, OJK must issue a new technical regulation that is *lex specialis* in nature, similar to SD20 in the UK.[38] This new rule will subsequently detail binding operational procedures, ranging from the deadline for fund returns, indicators of customer "gross negligence," to the execution of proportional loss sharing between the sending bank and the receiving bank.

Presence of regulations regarding this cross-sector liability is believed to bring a comprehensive positive impact.[39] Banking institutions will be increasingly encouraged to prioritize investment in improving their digital security infrastructure, while simultaneously being more active in performing educational functions so that the cyber security literacy of customers increases.[40] In the future, the implementation of this adaptive regulation is expected to be able to massively minimize cybercrime rates, while providing complete legal protection and certainty of fund returns for customers in the digital banking ecosystem.

The contextualisation of the United Kingdom's Mandatory Reimbursement scheme into the Indonesian legal system requires careful structural adaptation rather than wholesale transplantation, because the two jurisdictions differ in three legally significant respects. First, the United Kingdom operates within a common law tradition in which the Payment Systems Regulator (PSR) exercises a market-conduct supervisory mandate over an interbank Faster Payments Scheme administered by Pay.UK, whereas Indonesia operates within a civil law framework in which the Financial Services Authority (OJK) functions as a unified prudential and conduct-of-business regulator, while real-time interbank transfers are channelled through the centralised BI-FAST system administered

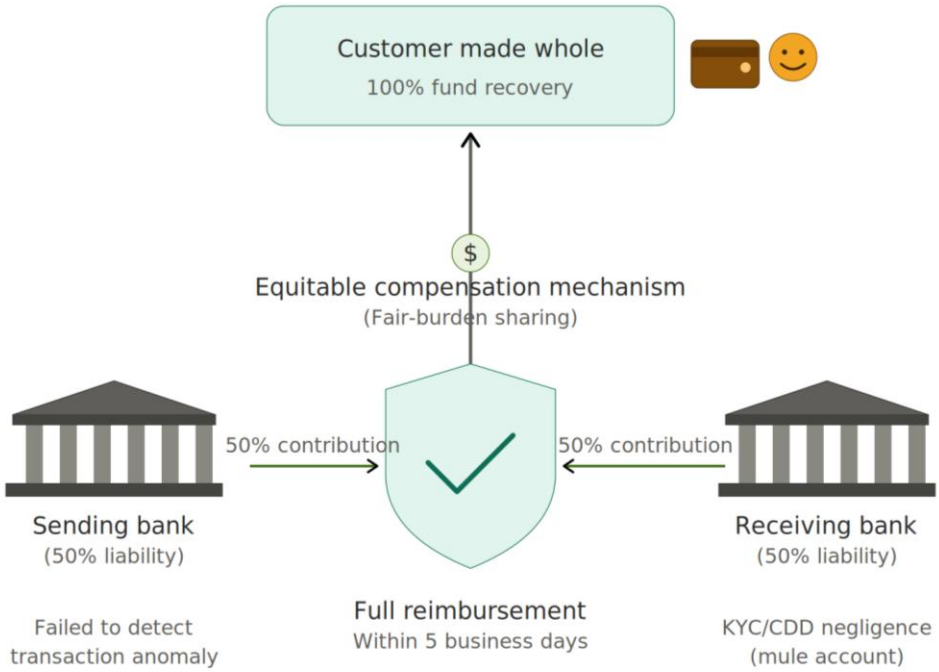
[37] Payment Systems Regulator, "Authorised Push Payment (APP) Scams: Mandatory Reimbursement Requirement" (London, 2023).
[38] Oluwadamilola Lola Fajinmi, "Innovation and Device Reimbursement: United States vs United Kingdom," *Chest* 163, no. 1 (2023): 36–37.
[39] Fikry Latukau and Syah Awaluddin Uar, "Penerapan Prinsip Strict Liability Dalam Hukum Lingkungan Internasional Dan Nasional Terkait Lingkungan Laut," *Jurnal Ilmu Hukum Kyadiren* 3, no. 1 (2021): 45–54.
[40] Zoubida Mesbahi et al., "Pharmacists as Independent Prescribers in Community Pharmacy: A Scoping Review," *Research in Social and Administrative Pharmacy* 21, no. 3 (2025): 142–53.

by Bank Indonesia.[41] Second, the United Kingdom's SD20 instrument is calibrated primarily against a single fraud typology—Authorised Push Payment fraud—whereas the Indonesian threat landscape encompasses a broader spectrum of cyber modalities, including malware-laden APK distribution, deepfake-assisted social engineering, and SIM Swap Fraud, each of which requires distinct evidentiary indicators of negligence and causation.[42] Third, the United Kingdom regime presupposes a relatively mature consumer protection ecosystem with established Alternative Dispute Resolution institutions such as the Financial Ombudsman Service, while Indonesia's equivalent institutional infrastructure, namely the Lembaga Alternatif Penyelesaian Sengketa Sektor Jasa Keuangan (LAPS SJK), is still consolidating its jurisdictional reach and procedural capacity. These structural differences mean that the United Kingdom model cannot be mechanically imported; it must instead be re-engineered to fit the Indonesian institutional matrix.

Through this contextualised adaptation, the Indonesian legal system would not merely import a foreign rule but would generate an indigenous regulatory innovation responsive to the specific contours of the national financial architecture, the civil law tradition, the OJK's unified supervisory mandate, and the distinctive cybercrime threat landscape. This contextualised novelty thus advances the comparative-law discourse beyond the binary of acceptance or rejection of legal transplants, demonstrating instead that comparative law can serve as a generative resource for jurisdiction-specific reform when accompanied by a rigorous structural analysis of the receiving legal system. In substantive terms, the proposed framework operationalises the theoretical commitments identified earlier—Rawls's requirement of fair distribution under structural asymmetry, the responsive-law orientation of Nonet and Selznick, the evidentiary logic of res ipsa loquitur, and the contextual sensitivity demanded by post-Watson legal transplantation theory—and translates them into concrete regulatory instruments capable of being deployed by the OJK within the existing Indonesian legal hierarchy.

[41] Christopher M. Raymond et al., "Integrating Local and Scientific Knowledge for Environmental Management," *Journal of Environmental Management* 91, no. 8 (2010): 1766–77, https://doi.org/10.1016/j.jenvman.2010.03.023.
[42] Li Huang and Henry N. Pontell, "Crime and Crisis in China's P2P Online Lending Market: A Comparative Analysis of Fraud," *Crime, Law and Social Change* 79, no. 4 (2023).

Graphic 1. Compensation Mechanism



Graphic 1 visualises the operational architecture of the compensation mechanism proposed in this study, which results from the contextualised adaptation of the United Kingdom's Mandatory Reimbursement scheme into the Indonesian regulatory framework. The diagram should be read in three sequential layers that correspond to the substantive arguments developed in the preceding paragraphs. The first layer, situated at the customer–bank interface and depicted at the apex of the diagram, depicts the customer's submission of a complaint to the originating (sending) bank following an unauthorised transaction caused by cybercrime, and the consequent full reimbursement of the customer—denoted in the diagram as "Customer made whole / 100% fund recovery"—within a maximum period of five business days. Pursuant to the proposed lex specialis OJK regulation, the originating bank is statutorily obliged to provide this preliminary reimbursement to the customer, subject only to the bank's evidentiary opportunity to demonstrate, on the balance of probabilities, that the customer committed gross negligence as exhaustively defined in the regulation. This first layer therefore captures the protection-oriented dimension of the model: the shifting of the burden of proof to the bank, the certainty of timely fund restoration for the customer, and the elimination of the customer's exposure to inter-institutional disputes.

The second layer, situated at the interbank level and depicted at the base of the diagram with horizontal arrows of equal magnitude flowing from the sending bank and

the receiving bank into the central "equitable compensation mechanism (fair-burden sharing)" node, illustrates the proportional loss-sharing that follows once the customer has been reimbursed. Fifty per cent of the loss is attributed to the originating bank for its failure to detect the transaction anomaly through its Fraud Detection System (FDS), as indicated in the diagram by the legend "Sending bank (50% liability) – Failed to detect transaction anomaly"; the remaining fifty per cent is attributed to the receiving bank for its KYC/CDD negligence in permitting the activation, maintenance, or operation of the mule account through which the criminal proceeds were channelled, as indicated by the legend "Receiving bank (50% liability) – KYC/CDD negligence (mule account)". Where the receiving account exhibits prior indicators of mule activity identifiable through the Sistem Layanan Informasi Keuangan (SLIK) database, the proportional liability of the receiving bank is intensified above the default fifty per cent threshold, in line with the graduated proportionality calibrated to the BI-FAST settlement architecture. This second layer therefore captures the accountability-distribution dimension of the model, by which both banks are incentivised to invest in their respective preventive infrastructures.

The third layer, situated at the supervisory level, depicts the role of the Financial Services Authority (OJK) as the institutional anchor of the entire reimbursement ecosystem. In the event of disagreement between the originating and receiving banks regarding the apportionment of loss—for instance, where one bank disputes the existence or significance of the mule-account indicators—the OJK exercises an adjudicatory function through structured arbitration, thereby ensuring the timely settlement of interbank disputes without affecting the customer's already-completed reimbursement. The OJK's role thus operates concurrently as the rule-setter (through the revised POJK Number 22 of 2023 and the proposed lex specialis), the supervisor of operational compliance, and the adjudicator of interbank disagreements, mirroring its unified mandate within the Indonesian financial supervisory architecture. Read together, the three layers of Graphic 1 illustrate that the proposed mechanism is not a single procedural step but an integrated regulatory ecosystem in which consumer protection, interbank accountability, and supervisory oversight operate as mutually reinforcing components.

CONCLUSION

Regulation of digital bank legal liability for customer funds lost due to cybercrime in Indonesia is currently regulated in layers through the Consumer Protection Law, the P2SK Law, and specific provisions in POJK Numbers 21 and 22 of 2023. Although the legal framework has shifted the paradigm of bank obligations to be a party required to actively manage cyber risks and detect transaction anomalies, implementation in the field

still shows an imbalance of position. Banking parties still tend to hide behind arguments of customer negligence over the leakage of authentication data, thereby triggering the phenomenon of mutual shifting of responsibility. To break this deadlock, the ideal legal liability model to be applied in the future is the shared liability model by adapting Mandatory Reimbursement regulations. This model fundamentally changes the legal construction through the shifting of the burden of proof, where banks are obligated to reimburse lost customer funds unless they can prove the existence of gross negligence on the part of the customer. Furthermore, such compensation liability is not borne unilaterally, but is distributed proportionally between the sending bank that failed to detect the fraud and the receiving bank that was negligent in allowing the criminal account.

Based on these conclusions, it is recommended to Financial Services Authority (OJK), as the regulatory and supervisory authority for the financial services industry, to immediately revise POJK Number 22 of 2023 by explicitly including norms for the shifting of the burden of proof and minimizing clauses that can exempt banking from absolute liability. Furthermore, OJK is advised to immediately issue a new technical regulation that is *lex specialis* in nature as a binding operational derivative. This technical regulation from OJK needs to regulate in detail regarding the mandatory reimbursement mechanism, the deadline for the disbursement of fund returns for customers who are victims, clear indicators regarding the limits of customer "gross negligence," and the technical basis regarding the procedure for proportional loss sharing between banks.

REFERENCES

Almaida, Zennia, and Moch Najib Imanullah. "Perlindungan Hukum Preventif Dan Represif Bagi Pengguna Uang Elektronik Dalam Melakukan Transaksi Tol Nontunai." *Privat Law* 9, no. 1 (2021): 218–26.

Aminudin, Muhammad. "Warga Malang Kehilangan Uang Rp 1,4 M Di Rekening Usai Klik Undangan Palsu." *DetikNews*, 2023. https://news.detik.com/berita/d-6811004/warga-malang-kehilangan-uang-rp-1-4-m-di-rekening-usai-klik-undangan-palsu.

Amru, Asmaru, Naufal Adil, and Novah Patilani. "Perlindungan Hukum Terhadap Penanggulangan Kejahatan Siber Di Sektor Perbankan Digital Indonesia." *Journal of Scientech Research and Development* 7, no. 1 (2025): 587–88.

Braithwaite, Jo. "'Authorized Push Payment'Bank Fraud: What Does an Effective Regulatory Response Look Like?" *Journal of Financial Regulation* 10, no. 2 (2024): 174–93.

Christian, John Bert, Bismar Nasution, Suhaidi Suhaidi, and Mahmul Siregar. "Analisis Hukum Atas Penerapan Rahasia Bank Di Indonesia Terkait Dengan Perlindungan Data Nasabah Berdasarkan Prinsip Kepercayaan Kepada Bank (Studi Pada Pt. Bank Cimb Niaga Tbk Cabang Medan)." *USU Law Journal* 4, no. 4 (2016): 164935.

Dori, E, J Baransano, J A Ibran, and D D Y Tarina. "Analisis Hukum Transparansi Perbankan Dan Stabilitas Keuangan Pasca Perubahan POJK No. 37/2019 Menjadi POJK No. 18/2025." *Al-Zayn: Jurnal Ilmu Sosial \& Hukum* 4, no. 1 (2026): 1028–37.

Fajinmi, Oluwadamilola Lola. "Innovation and Device Reimbursement: United States vs United Kingdom." *Chest* 163, no. 1 (2023): 36–37.

Faridi, M K. "Kejahatan Siber Dalam Bidang Perbankan." *Cyber Security Dan Forensik Digital* 1, no. 2 (2018): 57–61.

Fithri, B S, and W S Wahyuni. *Hukum Pidana Perbankan*, 2025.

Ghozali, M, N Liana, C Afra, Z Siregar, and M Hatta. "Kejahatan Siber (Cyber Crime) Dan Implikasi Hukumnya: Studi Kasus Peretasan Bank Syariah Indonesia (BSI)." *Cendekia: Jurnal Hukum, Sosial Dan Humaniora* 2, no. 4 (2024): 797–809.

Grewal, Garrett S. "Combating Authorized Push Payment Fraud: Which Regulatory Approach Should the United States Adopt?" *NC Bank. Inst.* 30 (2026): 385.

Hadjon, Philippus M. *Perlindungan Hukum Bagi Rakyat Indonesia*. Surabaya: PT. Bina Ilmu, 1999.

Hendarto. "Tanggung Jawab Bank Dalam Mengantisipasi Dan Menangani Kerugian Nasabah Akibat Scam Melalui Link Phising Pada Mobile Banking." *Iuris Studia: Jurnal Kajian Hukum*, 2023, 760.

Hidayah, Nur, Baidhowi, and Yustina Dhian Novita. "Perlindungan Hukum Bagi Pengguna Layanan Internet Banking Menurut Undang-Undang No. 8 Tahun 1999 Tentang Perlindungan Konsumen." *Media Hukum Indonesia* 2, no. 7 (2025): 22–28.

HR, Ridwan. "Pertanggungjawaban Publik Pemerintah Dalam Perspektif Hukum Administrasi Negara." *Jurnal Hukum IUS QUIA IUSTUM* 10, no. 22 (2003): 27–38. https://doi.org/10.20885/iustum.vol10.iss22.art3.

Huang, Li, and Henry N. Pontell. "Crime and Crisis in China's P2P Online Lending Market: A Comparative Analysis of Fraud." *Crime, Law and Social Change* 79, no. 4 (2023).

Irinwantin. *Mengenal Bank Digital*. Jakarta: Fastindo, 2023.

Kristiyenda, Y S, and T S Ramli. "Pelindungan Hukum Bagi Nasabah Bank Digital Terhadap Ancaman Pencurian Data Melalui BTS Palsu (Fake BTS)." *Causa: Jurnal Hukum Dan Kewarganegaraan* 13, no. 2 (2025).

Kusik, Przemyslaw. "The Legal Transplant Theory as a Paradigm of Comparative Law: An Attempt at a Summary on the 50th Anniversary of the Publication of Legal

Transplants: An Approach to Comparative Law by Alan Watson." In *Forum Prawnicze*, 42, 2024.

Lacoursière, Marc. "Les Méthodes Alternatives de Résolution Des Conflits Au Service de La Protection Des Consommateurs de Services Bancaires En Ligne Dans Les Amériques." *Banking & Finance Law Review* 21 (2005): 357.

Latukau, Fikry, and Syah Awaluddin Uar. "Penerapan Prinsip Strict Liability Dalam Hukum Lingkungan Internasional Dan Nasional Terkait Lingkungan Laut." *Jurnal Ilmu Hukum Kyadiren* 3, no. 1 (2021): 45–54.

Lutfi, Melinda Putri, Ela Kurniasari, and Fadilla Elza Aida Putri. "Urgensi Perlindungan Hukum Terhadap Data Privasi Nasabah Bank Di Era Perkembangan Digital." *Jurnal Multidisiplin Ilmu Akademik* 1, no. 5 (2024): 211–14.

Ma, Katelyn Wan Fei, Tarundeep Dhot, and Mohsen Raza. "Considerations for Using Artificial Intelligence to Manage Authorized Push Payment (APP) Scams." *IEEE Engineering Management Review* 51, no. 3 (2023): 166–79.

Margono, Rudi. *Kejahatan Perbankan: Teknis Pembuktian Dan Perlindungan Nasabah*. Profesor Rudi Margono, 2026.

Marzuki, Peter Mahmud. *Penelitian Hukum: Edisi Revisi*. Prenada Media, 2017.

Mesbahi, Zoubida, Celia Piquer-Martinez, Shalom I Benrimoj, Fernando Martinez-Martinez, Noelia Amador-Fernandez, Maria Jose Zarzuelo, Sarah Dineen-Griffin, and Victoria Garcia-Cardenas. "Pharmacists as Independent Prescribers in Community Pharmacy: A Scoping Review." *Research in Social and Administrative Pharmacy* 21, no. 3 (2025): 142–53.

Nonet, Philippe, and Philip Selznick. *Hukum Responsif*. Bandung: Nusa Media, 2018.

Otoritas Jasa Keuangan. "Peraturan Otoritas Jasa Keuangan Nomor 21 Tahun 2023 Tentang Layanan Digital Oleh Bank Umum," 2023.

———. "Peraturan Otoritas Jasa Keuangan Nomor 22 Tahun 2023 Tentang Pelindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan," 2023.

Payment Systems Regulator. "Authorised Push Payment (APP) Scams: Mandatory Reimbursement Requirement." London, 2023.

Rawls, John. *Justice as Fairness: A Restatement*. Harvard University Press, 2001.

Raymond, Christopher M., Ioan Fazey, Mark S. Reed, Lindsay C. Stringer, Guy M. Robinson, and Anna C. Evely. "Integrating Local and Scientific Knowledge for Environmental Management." *Journal of Environmental Management* 91, no. 8 (2010): 1766–77. https://doi.org/10.1016/j.jenvman.2010.03.023.

Republik Indonesia. "Undang-Undang Nomor 4 Tahun 2023 Tentang Pengembangan Dan Penguatan Sektor Keuangan," 2023.

———. "Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen,"

1999.

Rianda, F U. "Urgensi Pengaturan Central Bank Digital Currency Untuk Melindungi Data Pribadi Dari Cybercrime Di Indonesia." Universitas Islam Negeri Maulana Malik Ibrahim, 2025.

Sulistiawati, Tri, Deri Yansyah, and Nova Yanti Maleha. "Analisis Persepsi Risiko Dalam Layanan Digital Banking Di Indonesia: Tantangan Dan Solusi." *Jurnal Ekonomi Bisnis, Manajemen Dan Akuntansi (JEBMAK)* 4, no. 1 (2025): 212–23.

Syukron. "Peran OJK Dalam Melindungi Konsumen Dan Masyarakat Di Sector Jasa Keuangan." *Yurisprudentia: Jurnal Hukum Ekonomi* 8, no. 2 (2022): 192.

Tasman, T, and U Ulfanora. "Perlindungan Hukum Terhadap Nasabah Bank Digital." *UNES Law Review* 6, no. 1 (2023): 1624–35.

UK Parliament. "Financial Services and Markets Act 2023," 2023.

Utami, Lies Norma Tri, and others. "Perlindungan Hukum Bagi Pengguna Layanan Bank Digital Di Era Globalisasi." *Journal of Multidisciplinary Inquiry in Science Technology and Educational Research* 2, no. 1 (2025): 197.

Watson, Alan. "From Legal Transplants to Legal Formants." *Am. J. Comp. L.* 43 (1995): 469.

———. "The Birth of Legal Transplants." *Ga. J. Int'l \& Comp. L.* 41 (2012): 605.

Yang, Chen. "Protecting Financial Consumers from Authorized Push Payment Fraud: Is Reimbursement an Optimal Solution?" *Journal of Financial Regulation and Compliance* 33, no. 4 (2025): 642–53.

Zulfah, Shofiy, Bunga Jasmine Puji Hapsari, and Faza Rusda. "Legal Responsibility of Digital Commerce Platforms for Seller Content That Violates Public Ethics." *Indonesia Media Law Review* 4, no. 1 (2025).