Walisongo Law Review (Walrev), Vol 8 No. 1 (2026)
DOI: https://doi.org/10.21580/walrev.2026.8.1.31550
P-ISSN: 2715-3347 E-ISSN: 2722-0400

RECONSTRUCTION OF BANK LIABILITY IN BANKING SKIMMING CRIMES IN INDONESIA

Mohammad Choirul Anam,[1*] Dien Nufitasari,[2] Retno Catur Kusuma Dewi,[3]
[1,2,3] Universitas Merdeka Madiun, Indonesia

[*]Correspondence: *mohammadchoirulanam@unmer-madiun.ac.id*

Citation: Mohammad Choirul Anam, Dien Nufitasari, and Retno Catur Kusuma Dewi. 2026. "Reconstruction of Bank Liability in Banking Skimming Crimes in Indonesia". *Walisongo Law Review (Walrev)* 8 (1):151-69. https://doi.org/10.21580/walrev.2026.8.1.31550.

Abstract: This study examines the legal ambiguity surrounding bank liability toward customers who become victims of skimming crimes within the Indonesian banking system. Existing regulations impose obligations on banks; however, the implementation of compensation mechanisms and evidentiary procedures often places customers in a disadvantaged position. This research employs normative legal methods with statutory and conceptual approaches. The findings reveal a structural imbalance in risk allocation and evidentiary burden between banks and customers. This study proposes a reconstructed liability model integrating strict liability and the shifting burden of proof, requiring banks to provide preliminary compensation followed by internal verification. This model strengthens legal certainty, enhances consumer protection, and aligns liability with institutional risk control in digital banking.

Penelitian ini mengkaji ketidakpastian hukum terkait tanggung jawab bank terhadap nasabah yang menjadi korban tindak pidana skimming dalam sistem perbankan Indonesia. Peraturan yang ada saat ini memang membebankan kewajiban kepada bank; namun, implementasi mekanisme ganti rugi dan prosedur pembuktian sering kali menempatkan nasabah pada posisi yang tidak menguntungkan. Penelitian ini menggunakan metode penelitian hukum normatif dengan pendekatan perundang-undangan dan pendekatan konseptual. Hasil penelitian menunjukkan adanya ketidakseimbangan struktural dalam alokasi risiko dan beban pembuktian antara pihak bank dan nasabah. Penelitian ini mengusulkan rekonstruksi model tanggung jawab yang mengintegrasikan prinsip tanggung jawab mutlak (strict liability) dan pembalikan beban pembuktian (shifting burden of proof), yang mewajibkan bank untuk memberikan ganti rugi awal yang diikuti dengan verifikasi internal. Model ini memperkuat kepastian hukum, meningkatkan perlindungan konsumen, dan menyelaraskan tanggung jawab dengan kendali risiko institusional dalam perbankan digital.

Keywords: Bank Liability; Skimming; Strict Liability; Burden of Proof; Consumer Protection.

INTRODUCTION

The rapid digitalization of banking services has significantly increased efficiency and accessibility in financial transactions. However, this financial transactions are targeted by cybercriminals, resulting in cash withdrawals from customers' accounts (Begishev et al. 2024). One of the kind of digital crime, like skimming, which involves unauthorized duplication of customer card data. Skimming refers to the unlawful duplication of information stored in the magnetic stripe of credit cards as well as ATM/debit cards (Kartini 2022). The modus operandi involves transferring data from the customer's ATM card magnetic stripe onto a counterfeit card, which is subsequently used by perpetrators to withdraw funds from the victim's account without the knowledge of the lawful cardholder (Lestari, Muhaimin, and Mulada, 2022). This practice generates not only financial losses for customers but also erodes public trust in financial institutions and the security technologies they employ (Nafis Dwi Kartiko et al. 2024).

In Indonesia, the rise of cybercrime in the financial sector demonstrates a growing vulnerability in banking security systems. According to the Ministry of Communication and Informatics, between 2019 and 2022 approximately 486,000 fraud cases were documented, of which 405,000 were reports of online fraud, making it the most prevalent form of fraud. Online fraud or cyber-fraud refers to criminal conduct that utilizes the internet for business and commercial activities without involving traditional physical business forms. This includes the misuse of information technology platforms to deceive victims through information manipulation, fictitious transactions, or identity theft (Yunita et al. 2024). The absence of physical control over the card at the time data is stolen often leads to customers being presumed negligent, whereas in reality the perpetrators have successfully breached the bank's security system.

Statistical data indicate that the escalation of cybercrime in the financial sector, particularly in relation to card fraud and skimming, has reached an alarming level in recent years. In Indonesia, the National Cyber and Crypto Agency (BSSN) recorded more than 361 million traffic anomalies or cyberattacks throughout 2023, with the financial sector identified as one of the primary targets of data theft attacks (Otoritas Jasa Keuangan 2024). Reports from the Indonesian National Police have repeatedly uncovered international skimming syndicates operating in Bali, causing customer losses amounting to billions of rupiah within a short period due to weaknesses in ATM protection systems (Tribratanews 2021). Digital threats in Indonesia have once again drawn significant attention. A recent study released by AwanPintar.id, the national cyber threat intelligence platform of Prosperita Group, revealed that during the first semester of 2025 (January–June), 133.4 million cyberattacks were detected nationwide (Sari, 2025). Existing protection mechanisms have proven insufficient to curb the financial losses suffered by the broader public as a consequence of banking-related crimes. The magnitude of these losses underscores the

urgent necessity for the state to intervene through stronger legal instruments to ensure the security of its citizens' financial assets.

In Indonesia, despite the existence of various regulatory frameworks governing the protection of customers who fall victim to banking crimes including Law Number 10 of 1998 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection, and Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law, 2008), as amended by Law Number 19 of 2016 (ITE Law 2016) and most recently by Law Number 1 of 2024 (ITE Law, 2024) legal protection for customers remains inadequate. In practice, customers frequently encounter complex evidentiary bureaucracies. Banks often impose the burden of proof upon the customer by requiring evidence that the customer was not negligent in maintaining the confidentiality of their PIN or card data (Malawai and Jamal 2021). Such conditions give rise to legal uncertainty and expose customers to potential harm, particularly as most customers lack an understanding of the technical dimensions of digital security. Consequently, the resolution of disputes frequently depends on internal interpretations adopted by banks, while customers are left without meaningful bargaining power or access to the technical evidence underlying transaction examinations (Hakim, Rizqi, and Putra 2025). This situation creates structural injustice, whereby the risks arising from failures in banking security systems are ultimately borne by customers who, in principle, entrust their funds to banks for safekeeping.

Several previous studies have examined bank liability for customer losses resulting from skimming crimes. Research conducted by Wicaksana and Baidhowi (2025) analyzed the legal aspects of bank responsibility in skimming cases by reviewing existing statutory regulations and customer legal protection frameworks (Wicaksana and Baidhowi 2025). Their findings indicate that banks are obliged to compensate customers' losses under consumer protection law. Although the study focuses on bank liability, it also acknowledges the practical difficulties customers face in proving losses during litigation. Furthermore, research by Lestari, Muhaimin, and Mulada (2022) explored forms of bank liability through compensation mechanisms based on OJK regulations and the Consumer Protection Law. Nevertheless, their analysis primarily addressed the normative position of legal provisions without mapping weaknesses in the implementation of liability mechanisms in practice (Lestari, Muhaimin, and Mulada 2022). Another study by Malawai and Jamal (2021) emphasized banks' obligation to provide compensation, subject to evidentiary requirements such as CCTV recordings and the absence of customer negligence (Malawai and Jamal, 2021). However, the study did not sufficiently explore the evidentiary controversies within the context of skimming crimes, which are often perpetrated through complex and concealed methods. In addition, a juridical analysis by Yusnita, Pratiwi, and Citra (2025) highlighted that banking contracts frequently contain clauses that effectively place the burden of proof upon customers, thereby positioning consumers in a disadvantaged

situation when claiming losses arising from skimming incidents (Yusnita, Aprilia Pratiwi, and Citra 2025).

Previous research has examined bank liability in skimming cases; however, it tends to focus on normative obligations without addressing structural issues within evidentiary mechanisms and compensation procedures. Consequently, this study identifies a critical gap, namely the absence of a fair and balanced liability model that reflects technological risks and the asymmetry between banks and customers. This research aims to reconstruct a bank liability model that ensures justice, legal certainty, and effective consumer protection through the integration of strict liability and burden-shifting principles.

RESEARCH METHOD

This study employs normative legal research using statutory and conceptual approaches. The statutory approach analyzes relevant laws and regulations governing banking liability and consumer protection, while the conceptual approach examines legal doctrines such as strict liability, vicarious liability, and burden of proof. Legal materials consist of primary sources (laws and regulations), secondary sources (journal articles and books), and tertiary sources (legal dictionaries). Data are analyzed qualitatively using interpretative and prescriptive methods to construct a coherent legal argument and propose a new liability model.

RESULT AND DISCUSSION

Legal Gap and Structural Imbalance

Skimmingis one of the crimes in cybercrime where this crime is committed through a network of computer systems, both locally and globally, by utilizing technology by illegally copying the information contained on the magnetic stripe of the ATM card to have control over the victim's account. The perpetrators of this cybercrime have a high ability background in their field so that it is difficult to track and eradicate them completely (Sipahutar, Purba, and Sipahutar 2022). In Indonesia, skimming cases began to be widely discovered around the 2010s, where perpetrators used the method of installing skimmers and hidden cameras on ATMs to steal card data and customer PIN numbers (Wardani, Raodiah, and Gazali 2025).

The techniques employed in PIN theft have also evolved; whereas such activities were previously conducted via hidden cameras or direct observation (shoulder surfing), perpetrators now utilize counterfeit keypads superimposed over the authentic keypads to capture PIN entries (Syafa and Santoso 2024). Automated teller machines (ATMs) are often prime targets for planting skimmers and other information stealing devices. ATMs are often unattended and may have limited auxiliary security (e.g., cameras, being located behind a secured door, etc.). In order to be effective, thieves must steal both the information on the card and the associated PIN (Shaw 2019).

Skimming constitutes a consequence of misuse by third parties. The term "third parties" refers to hackers and phreakers, namely individuals who unlawfully access or infiltrate computer systems and internet networks (Linggoraharjo, 2020). The methods employed by hackers to steal ATM cardholder data include: intrusion through bank computers and credit card company systems; and Transhing, a technique whereby hackers inspect the discarded waste of companies or retail establishments presumed to process ATM card transactions (Suheimi, 1995).

Bank Indonesia (BI) plays a pivotal role in establishing a robust legal protection framework through its regulation of the national payment system. Specifically, Bank Indonesia Regulation No. 14/2/PBI/2012, in conjunction with Circular Letter No. 17/52/DKSP, mandated the adoption of national chip technology and six-digit PINs to mitigate skimming risks inherent in magnetic stripe cards. However, the protracted transition toward full migration created security vulnerabilities, which criminal syndicates exploited to illicitly acquire financial data from customers still utilizing legacy cards.

The technological complexity of skimming necessitates independent and transparent digital forensic audits. Traditional fraud investigators have a comprehensive knowledge of payment systems and money flows, but often have limited technical knowledge of the underlying systems. Conversely, traditional digital forensics investigators have a comprehensive knowledge of underlying technical systems, but often lack knowledge of financial transaction activity(Nikkel 2020). These investigations transcend financial examination, integrating digital footprint tracing, data recovery, and system log analysis while leveraging Big Data and Artificial Intelligence (AI) to identify anomalous patterns. The integration of analytical technologies into internal audit mechanisms has been proven to enhance fraud detection effectiveness within the banking sector and public corporations (Haris Karyadi et al. 2025). In practice, skimming dispute resolution mechanisms often impose the evidentiary burden on customers, fostering a structural imbalance driven by: asymmetry of information, unequal access to evidence, and dominance of bank-controlled systems.

The legal relationship between a bank and its depositors is essentially constructed upon the pillar of trust (fiduciary relation). However, in practice, this leads to legal asymmetric information, which is a condition where the issuer has much greater information and control than the consumer, while consumers have no legal position to demand or defend the rights to the funds they deposit (Maulana, Murwadji, and Litai 2026). As capital and technology intensive institutions, banks maintain absolute control over payment infrastructures, electronic logs, and security protocols (CCTV). Conversely, customers occupy an inferior position as mere end users of ATM or EDC interfaces. In skimming cases, this structural asymmetry creates a significant juridical impasse regarding the burden of proof (bewijslast) during fund loss disputes. There is very limited information available to distinguish dynamic fraud from genuine customer behavior in such an extremely sparse and imbalanced data environment (Wei et al. 2013).

Civil banking disputes traditionally rely on the principle of *actori incumbit probatio* (the burden of proof lies with the plaintiff); however, this framework is increasingly inadequate for addressing the complexities of modern cybercrime. A skimmer is a manufactured technological device that is placed over the terminal's card reader and does not interfere with the normal checkout or withdrawal process. Skimmers record and pass the financial information to the normal terminal underneath. The compromised data is then transferred to the offender, allowing them to access and drain the victim's bank accounts without the victim's knowledge (Ciaccio and Ismail Onat 2025). Many customers experience difficulty in claiming compensation or obtaining clarity on their responsibilities from the bank. Cases of lost funds through unauthorized transactions often result in a shift in responsibility between the bank and the customer. There are times when in some cases the bank does not want to be held accountable because the error was caused by the customer's negligence in notifying the account number intended for the transfer(Sitorus and Saphira 2024). While customers assume that the bank's security system should have prevented such illegal transactions. As a result, the customer's position becomes weak because they do not actually have access to technical evidence or the ability to prove that there is a system error on the bank's part (Wattimena, Renjaan, and Siswani 2025). Current norms disproportionately emphasize customer negligence, often overlooking the bank's obligation to maintain robust security systems, while the absence of national anti-skimming standards creates a critical regulatory vacuum. This ambiguity leads to protection disparities that contradict the philosophical principle of equality before the law, as consumer safety remains contingent upon varying internal bank policies. Consequently, regulatory harmonization is imperative to guarantee equitable legal protection.

Regulatory inconsistencies reveal that banking mediation mechanisms fail to fully guarantee transparency and accountability. Limited disclosure of decisions obstructs the establishment of normative precedents for dispute resolution, while inadequate documentation further undermines the evaluation of consumer protection effectiveness. In practice, parties acting in bad faith frequently exploit this system to seek unwarranted benefits. This situation has led to discussion regarding the regulations that permit non-binding mediation (Hartono and Irhamdessetya 2025). This reconstruction is rooted in the constitutional protection of property rights, positioning customer deposits as a core legal interest under the rule of law. Juridically, bank liability represents a professional obligation inherent in the bank-customer relationship. Sociologically, the surge in digital transactions necessitates normative adaptations to remain responsive to technological shifts. Consequently, reforming bank liability regulations is an immediate necessity; any delay risks exacerbating financial exposure for depositors.

Bank Responsibility in Regulatory Framework

In the practice of skimming crimes, customers are placed at a significant disadvantage, as they are often unaware that their personal banking data has been compromised by

unauthorized actors. The *modus operandi* of such activities continues to evolve in tandem with technological advancements. Consequently, as institutions entrusted with the management and storage of customer data, banks are legally obligated to ensure robust information security systems and to safeguard personal data against the risk of leakage resulting from cyber intrusions (Monica et al. 2024). Instances of skimming result in more than just material losses; they fundamentally erode public confidence in the national banking system, which is predicated on the guarantee of fund security. The pervasive losses incurred from cybercrime within the banking sector have prompted regulators to implement more stringent measures.

Implementation of the Banking Prudential Principle in Mitigating the Risk of Skimming Crimes. Pursuant to Article 1, paragraph (2) of Law Number 10 of 1998 concerning Banking, a bank is defined as a business entity that collects funds from the public in the form of deposits and redistributes them through credit and/or other forms to enhance the public standard of living. This definition carries the juridical consequence that the bank serves as a debtor bearing an absolute obligation to guarantee the security of funds entrusted by customers as creditors (Lorensa and Badriyah 2023). The bank functions as an agent of trust, as its role as an intermediary institution depends on public confidence; banking activities are predicated on trust in both the collection and distribution of public funds (Kuntag, Kalalo, and Wahongan 2021). This principle is affirmed in Article 2 of Law Number 7 of 1992 concerning Banking, which states that Indonesian banking is based on economic democracy and applies the prudential principle.

Pursuant to Article 1, paragraph (2) of Law Number 10 of 1998 concerning Banking, a bank is defined as a business entity that collects funds from the public in the form of deposits and redistributes them through credit and/or other forms to enhance the public standard of living. This definition carries the juridical consequence that the bank serves as a debtor bearing an absolute obligation to guarantee the security of funds entrusted by customers as creditors (Lorensa and Badriyah 2023). The bank functions as an agent of trust, as its role as an intermediary institution depends on public confidence; banking activities are predicated on trust in both the collection and distribution of public funds (Kuntag, Kalalo, and Wahongan 2021). This principle is affirmed in Article 2 of Law Number 7 of 1992 concerning Banking, which states that Indonesian banking is based on economic democracy and applies the prudential principle. Article 29, paragraph (3) of Law Number 10 of 1998 concerning Banking stipulates that in providing credit or financing based on Sharia Principles, as well as in conducting other business activities, banks are required to adopt methods that do not disadvantage the bank or the interests of customers who have entrusted their funds.

A bank's responsibility is not limited to the storage of funds; it also encompasses protection against unauthorized third-party access. Consequently, the legal construction of customer protection within the Banking Law places the security burden on the bank as the system operator. This framework is reinforced by Article 40 of the Banking Law, which

emphasizes that bank secrecy is maintained primarily for the interest of the bank itself. Ultimately, the mandate to protect customer confidentiality is rooted in five core principles: personal privacy, contractual property rights, prevailing legislation, evolving banking customs, and the bank's fiduciary duty to maintain public trust. These provisions not only demand transparency but also implicitly hold the bank fully accountable for transaction security.

Customers typically lack the technical capacity to detect ATM *skimming* devices. This technological disparity calls for a progressive legal interpretation: banks commit a tort or breach of contract when they fail to secure customer funds as mandated by law. In this context, legal protection is not merely declarative; it is a tangible manifestation of a bank's fiduciary duty to safeguard public assets. Any security flaw that facilitates *skimming* legally constitutes negligence in risk management. Therefore, *a contrario*, unless a customer is proven negligent (e.g., sharing their PIN), the legal liability rests entirely with the bank as the payment system operator. Ultimately, *skimming* incidents signify a failure in the bank's core fiduciary responsibilities, highlighting critical weaknesses in its operational oversight of ATM infrastructure.

Legal Protection and the Right to Compensation for Customers. Legal protection for customers is inextricably linked to Law Number 8 of 1999 concerning Consumer Protection. Article 1, number (2) defines a consumer as any individual who uses goods and/or services available in society for the benefit of themselves, their families, other individuals, or other living entities, and not for trading purposes. Based on this definition, bank customers qualify as consumers because they utilize goods and services provided by the bank, including Automated Teller Machine (ATM) cards and ATM facilities issued by the bank as a business actor. The protection of customers' personal data stored in the magnetic stripe or chip on an ATM card is the absolute responsibility (strict liability) of the bank as the data controller.

Law Number 8 of 1999 concerning Consumer Protection (UUPK) provides a strong legal foundation for customers to claim compensation for losses arising from the criminal act of skimming. This is regulated in Article 4, letter (h) of the UUPK, which stipulates that one of the rights of consumers is to obtain compensation, indemnification, and/or replacement if the goods and/or services received are not in accordance with the agreement or do not function as they should. When a customer becomes a victim of skimming, their fundamental right to security in utilizing banking services has been violated due to the business actor's inability to guarantee the integrity of its security system. Legal liability is further emphasized in Article 7, letters (f) and (g) of the UUPK, which obligate business actors, including banks, to act in good faith in conducting their business operations and to provide compensation, indemnification, and/or replacement if the goods and/or services received or utilized do not conform to the agreement.

Customers, as consumers, have no control over the bank's information technology security infrastructure. Therefore, the bank's failure to detect or prevent the installation of

skimming devices cannot be attributed to the customer. Negligence in the supervision of ATM infrastructure constitutes a breach of the bank's professional obligation to provide secure services.

The Obligation to Maintain a Reliable and Secure Electronic System. The regulatory framework, as established in Law Number 11 of 2008 concerning Electronic Information and Transactions (2008 ITE Law), as amended by Law Number 19 of 2016 (2016 ITE Law), and most recently by Law Number 1 of 2024 (2024 ITE Law), positions banks not merely as financial institutions, but also as Electronic System Providers (PSE) that bear legal responsibility for the security of customer data. According to Article 1, number (6a) of the 2016 ITE Law, an Electronic System Provider is any person, state administrator, business entity, or community that provides, manages, and/or operates an electronic system, either individually or jointly, for their own benefit and/or the benefit of other parties using the electronic system. Article 15, paragraph (1) of the ITE Law obligates every Electronic System Provider, including banking institutions, to operate electronic systems reliably and securely, and to be responsible for the proper operation of these systems. The phrase "reliably and securely" gives rise to juridical consequences in the form of applying the principle of strict liability to banks. This principle asserts that a party remains liable for losses resulting from its actions without the need to prove the existence of fault or negligence. Within this framework, the existence of a causal relationship between the act and the loss is sufficient to establish legal liability (Suciara et al. 2026). In skimming cases, an *a contrario* reasoning can be drawn that the bank's security system is not operating reliably or that there is a failure in system protection; consequently, the losses resulting from the actions of a third party (the skimming perpetrator) do not necessarily absolve the bank of its responsibility as an Electronic System Provider.

Furthermore, the enactment of Law Number 1 of 2023 concerning the Criminal Code (KUHP) marks a new phase in the codification of Indonesian criminal law, significantly shifting the regulation of cybercrimes, which were previously governed as *lex specialis* under the ITE Law. Prior to the full implementation of the National Criminal Code, skimming acts were prosecuted based on Article 30, paragraphs (1), (2), and (3) in conjunction with Article 46 of the 2008 ITE Law (regarding illegal access), as well as Article 32 in conjunction with Article 48 of the 2008 ITE Law (regarding the unlawful acquisition or transfer of electronic data). However, with the enactment of Law Number 1 of 2023, several penal provisions within the ITE Law have been repealed through the transitional provisions of the National Criminal Code. Specifically, the legal construct for prosecuting the criminal act of skimming has now transitioned to Article 332 and Article 334 of Law Number 1 of 2023.

In the context of skimming, Article 332, paragraph (1) of Law Number 1 of 2023 stipulates that any person who intentionally and without right or unlawfully accesses a Computer and/or Electronic System belonging to another person by any means shall be punished with imprisonment for a maximum of six years or a maximum fine of Category V.

This provision represents both the adoption and refinement of the "illegal access" element previously regulated in Article 30 of the Electronic Information and Transactions Law. In the practice of skimming, the installation of a skimmer device in an ATM card slot to capture a customer's card magnetic stripe data constitutes an act of accessing a computer and/or Electronic System belonging to another person by any means. Furthermore, paragraph (3) stipulates that any person who intentionally and without right or unlawfully accesses a Computer and/or Electronic System by any means by violating, breaching, bypassing, or breaking through a security system shall be punished with imprisonment for a maximum of eight years or a maximum fine of Category VI. The phrase "violating, breaching, bypassing, or breaking through a security system" in this paragraph forms the core of criminal liability. When a skimming perpetrator successfully duplicates customer data without authorization, the element of the criminal act (*actus reus*) has been fulfilled.

In the criminal act of skimming, perpetrators frequently do not merely duplicate card data but also utilize hidden cameras or supplementary devices on the keypad to record customers' PINs. Such actions explicitly fulfill the elements of Article 334, letter (a) of Law Number 1 of 2023, namely, without right or exceeding authority, using or accessing a computer or Electronic System with the intent to obtain financial gain or acquire financial information from the central bank, banking institutions, financial institutions, credit card or payment card issuers, as well as data containing customer reports. Bank customer reports constitute confidential data. Therefore, the unlawful interception and expropriation of transactional data streams must be qualified as a criminal offense against information security, rather than a mere administrative violation.

The Application of the Shifting Burden of Proof Principle in the Resolution of Skimming Crime Disputes. Customer protection under Law Number 3 of 2011 concerning Fund Transfers exhibits a progressive character, particularly regarding the law of evidence. Article 78 of the aforementioned law stipulates that in the event of a delay or error in a fund transfer resulting in financial loss to the Originating Sender or the Beneficiary, the Operator and/or other parties controlling the Fund Transfer System bear the obligation to prove the presence or absence of said delay or error. This provision establishes a mechanism for the reversal of the burden of proof, wherein the bank is obligated to demonstrate that the transaction was authorized by the customer or that the loss resulted from the customer's negligence, rather than vice versa. In skimming cases, the "error" resides in the failure of the bank's security system to detect the card cloning perpetrated by the offender. Consequently, the bank bears strict liability alongside fault liability, coupled with a reversal of the burden of proof, to immediately reimburse customer funds depleted as a result of skimming. In the event of an unauthorized Transfer Order, the Operator is mandated to refund the principal amount, along with any relevant fees, interest, or compensation, to the Originating Sender. This regulatory framework asserts that the restitution of customer rights is not restricted merely to the principal loss, but extends to potential gains, such as interest or service benefits that should have otherwise accrued.

Such a framework provides legal certainty by positioning the risk of information technology security failures as an operational business risk to be absorbed by banking institutions, rather than externalized onto customers. Furthermore, the regulatory instruments issued by the Financial Services Authority (*Otoritas Jasa Keuangan*, or OJK) establish an additional normative foundation for consumer protection against skimming crimes. Notable among these is the Financial Services Authority Regulation Number 6/POJK.07/2022 concerning Consumer and Public Protection in the Financial Services Sector. This regulation reconstructs the liability paradigm of Financial Services Institutions (*Pelaku Usaha Jasa Keuangan*), shifting it from a defensive orientation to a more consumer-protective approach, particularly concerning security system failures. Article 8, paragraph (1) of the aforementioned OJK Regulation stipulates that Financial Services Institutions are liable for consumer losses arising from errors, negligence, and/or actions contrary to statutory provisions within the financial services sector, perpetrated by members of the board of directors, the board of commissioners, employees, and/or third parties acting for and on behalf of the Financial Services Institution.

The legal framework for protecting skimming victims in Indonesia integrates the Banking Law, the Consumer Protection Law, the Electronic Information and Transactions (ITE) Law, and the Funds Transfer Law. This normative framework mandates strict liability for banks, obligating them to secure funds and electronic systems. Consequently, a rebuttable presumption of liability applies; banks are held responsible unless they can prove a customer's willful misconduct or gross negligence (Mahmud 2020). This construction maintains a doctrinal balance between consumer protection and banking stability, aligning with the Indonesian legal principles of good faith and professional responsibility.

Theoretical Foundation of Liability Reconstruction

While these regulations implicitly establish a liability framework that holds banks primarily responsible as system providers, inconsistent implementation often erodes legal certainty. Banks frequently contend that disputed transactions remain legally valid if the correct Personal Identification Number (PIN) was utilized. However, under the principle of prudence governing banking operations, successful PIN verification does not automatically absolve a bank of its liability. The reconstruction of bank liability is predicated on three primary legal doctrines, namely: strict liability theory, shifting burden of proof theory, and risk distribution theory.

In strict liability theory, according to Shelagh Heffernan, the banking sector is among the most stringently regulated sectors due to the immense social costs precipitated by bank failures, which encompass the disruption of its intermediation function and its role in the transmission of the payment system (Sihombing 2010). Consequently, in instances indicative of skimming practices, a bank's fraud detection system ought to serve as the primary line of defense prior to the depletion of customer funds. Should this early detection mechanism prove ineffective, liability cannot be summarily shifted to the customer as the

consumer of banking services. An ideal model of bank liability should integrate the principle of strict liability. According to R.C. Hobert, as cited by Dian Mahardikha, the principle of strict liability is applied because, during the production or distribution of goods and services, consumers are generally situated at a disadvantage when required to prove fault. This doctrine incentivizes producers to exercise a heightened standard of care (Mahardikha 2020). Within the context of electronic transactions, banks operate as business entities that maintain control over security systems, technological infrastructure, and authentication mechanisms. Pursuant to Article 1365 of the Indonesian Civil Code (*Kitab Undang-Undang Hukum Perdata*), any unlawful act that inflicts damage mandates the perpetrator to provide compensation for said damages. However, in cases involving the crime of skimming, substantiating the individual fault of the bank frequently encounters impediments, given that the principal perpetrator is a third party. Consequently, the doctrine of vicarious liability becomes pertinent in assigning liability to entities that derive benefits from high-risk activities. Vicarious liability constitutes a form of accountability whereby an individual or entity, despite the absence of personal fault, is nonetheless held liable for the actions of another party (Mahmud 2020).

In shifting burden of proof theory, the legal framework for the protection of customers as consumers is stipulated in Article 19, paragraph (1) of the Consumer Protection Law (UUPK), which mandates business entities to bear the responsibility of providing restitution for any damage, pollution, and/or loss sustained by consumers as a consequence of utilizing the goods and/or services produced. This provision establishes a vital legal foundation by incorporating the Shifting Burden of Proof doctrine within consumer disputes. Under Article 19(1) of the Consumer Protection Law (UUPK), banks are mandated to indemnify victims of skimming for financial losses, unless the institution can demonstrably prove consumer negligence as stipulated in Article 19(5). Consequently, when skimming stems from systemic security vulnerabilities rather than personal error, the bank's liability remains non-negotiable. By doing so, the UUPK fosters a framework that compels banks to modernize risk management and prioritize restitution, effectively restoring the rights of consumers harmed by the services provided. Banks bear the burden of proof to demonstrate, through digital forensics, that customer negligence such as PIN disclosure occurred, rather than unauthorized 'card cloning' common in skimming operations. If the physical card remains in the customer's possession during geographically anomalous transactions, the legal presumption shifts toward a failure in the bank's security infrastructure. Within civil evidentiary law, the doctrine of *res ipsa loquitur* becomes highly pertinent. Rooted in tort law, this doctrine applies when an incident inflicts harm upon a plaintiff due to the defendant's presumed negligence. The court may draw an inference of negligence on the part of the defendant without requiring the plaintiff to prove it directly(R.Subekti 2015). Its application becomes increasingly appropriate in situations

where the burden of proof would disproportionately burden the plaintiff, particularly when access to the relevant evidence rests entirely within the defendant's control (Angela, Suryamah, and Yuanitasari 2024).

In risk distribution theory, beyond the direct obligation of consumer protection, banks are also required to safeguard the security of their information technology systems through the implementation of effective risk management. This obligation is stipulated in Article 15 paragraph (1) of the Financial Services Authority Regulation Number 11/POJK.03/2022 concerning the Implementation of Information Technology by Commercial Banks (previously regulated under POJK Number 11/POJK.03/2016), which asserts that banks must effectively implement risk management in the administration of their information technology. Paragraph (3) further details that information technology risk management encompasses risk identification, risk measurement, risk monitoring, and risk control. This provision serves as the primary benchmark for assessing the extent to which banks maximize the prevention of skimming. Banks are obligated to implement robust risk management mechanisms, particularly fraud detection systems capable of identifying transaction anomalies. The failure to detect suspicious patterns is deemed an inability of the bank to mitigate operational, legal, and reputational risks resulting from the neglect of its statutory duty to safeguard customer funds. Although prudential in nature, this regulatory framework has direct implications for the reinforcement of customer protection.

The irresponsibility of the banks will certainly harm customers and result in huge losses, therefore the banks may be subject to criminal and civil liability. Criminal liability will result in the detention of the employees who commit banking crime. Inspections and investigations will be conducted by the law enforcement agencies in search of evidence that results in harm to customers. While the liability of civil liability is the responsibility of the banks to replace the losses that occur to customers(Santiago 2018).

Proposed Liability Model

The policy reconstruction proposed in this study positions the bank as the primary risk bearer in electronic transactions, considering that banks possess greater systemic control and risk mitigation capacity compared to customers. Based on the theory of distributive justice, the allocation of losses must consider the bargaining position and information access of the respective parties. Distributive justice focuses on the outcomes of the service recovery process, specifically the efforts undertaken by a company in responding to customer complaints when errors occur, even if this demands significant compensation expenditures. In practice, distributive justice is manifested through the provision of restitution to customers (Tjitrokusmo et al. 2014).

Customers are situated in an asymmetric position as they lack access to the bank's internal security systems. The juridical implication of this reconstruction model necessitates the reformulation of norms within the Banking Law or the establishment of specific

regulations regarding electronic banking fraud. Such regulations must explicitly establish minimum security standards, system audit obligations, and automatic compensation mechanisms within a short timeframe for skimming victims. From a sociological perspective, the certainty of compensation provision will enhance public trust in the digital banking system. Without such guarantees, reputational risks and the potential for large-scale fund withdrawals may increase. The practical implementation of this reconstruction model can be applied through the following steps: initial reporting phase, preliminary compensation, investigation phase, evidentiary mechanism, and final determination.

In initial reporting phase, the first step in mitigating legal risks is reporting. Immediately upon realizing the occurrence of unauthorized account mutations (unauthorized transactions), the customer is obligated to report it through an official call center or the nearest branch office. This report triggers fraud detection, whereupon the bank will immediately block the card or account in real-time to prevent further drainage of funds. This stage represents a form of preventive legal protection. Banks are required to provide a responsive 24-hour complaint channel. In preliminary compensation, within the legal hierarchy of consumer protection, Article 19 paragraph (3) of the Consumer Protection Law (UUPK) stipulates that business actors must provide a response and/or compensation within a period of 7 days following the transaction or report. Banks demonstrating Good Corporate Governance frequently re-credit the lost funds temporarily (preliminary or temporary compensation) while the investigation is underway, particularly if the transaction patterns visibly indicate skimming anomalies (e.g., cash withdrawals abroad while the customer is in Indonesia). This ensures the bank's good faith in serving its consumers.

In investigation phase, at this stage, the bank conducts digital forensics. The investigation encompasses the examination of CCTV footage at the ATM, reviewing transaction system logs, and detecting the presence of skimming devices (magnetic stripe readers) or hidden cameras on the respective ATM. This internal audit is highly critical in distinguishing whether the incident is purely a failure of the bank's system and security (pure skimming) or involves customer negligence (e.g., the customer disclosing their PIN and OTP to third parties, or falling victim to phishing). This framework ensures the principles of legal certainty and justice for both parties. In evidentiary mechanism, in modern consumer law doctrine, the principle of Reversed Burden of Proof applies, which is explicitly regulated in Article 28 of the UUPK. This principle states that the burden of proof regarding the presence or absence of fault lies with the Business Actor (the Bank), rather than the customer. Banks are prohibited from hiding behind standard clauses (exculpatory agreements that absolve the bank of liability). Should the bank refuse to provide compensation, it is the bank that must prove, using empirical forensic data, that the customer has committed gross negligence (such as intentionally sharing their PIN). If the bank fails to prove customer negligence, it bears absolute liability.

In final determination, if the investigation and evidentiary mechanism (stages c & d) conclude that the incident is purely skimming resulting from the bank's weak anti-skimming security, the preliminary compensation previously provided will be permanently confirmed as the customer's right (100% restitution). However, if customer negligence is proven (based on compelling evidence from the bank), the bank may retract the preliminary compensation and deny the claim. Should the customer perceive this final determination by the bank as unilateral and detrimental, the customer possesses the legal right to escalate the matter through the Alternative Dispute Resolution Institution for the Financial Services Sector (LAPS SJK) facilitated by the Financial Services Authority (OJK), or to pursue litigation in court. This model guarantees the realization of more expedited protection for customers while simultaneously upholding the principle of justice for the bank.

Implications of the Model

The implementation of this model entails several implications, including: enhancing consumer protection, bolstering public trust in banking institutions, prompting banks to refine their security systems; and providing legal certainty within the dispute resolution process. In enhancing consumer protection, this model deconstructs such inequities by relieving consumers of the complex burden of proof. Protection is operationalized through a 'Preliminary Compensation' mechanism, where banks temporarily credit lost funds during ongoing investigations particularly in cases of skimming anomalies. In bolstering public trust in banking institutions, establishing a responsive, pro-customer compensation model for innocent victims strengthens the assurance of fund security. this guarantee is vital to mitigate escalating reputational risks and prevent potential bank runs (rush). In prompting banks to refine their security systems, the strict liability framework compels banks to increase their investments in security risk mitigation, driving them to establish robust risk management frameworks, deploy proactive *fraud* detection systems for transaction anomalies, and integrate advanced *digital forensic* auditing capabilities. In providing legal certainty within the dispute resolution process, this model eliminates the uncertainty inherent in unilateral internal bank investigations by shifting the burden of proof entirely to the financial institution. Legal certainty is institutionalized through a streamlined procedural flow: immediate account freezing upon reporting, provisional compensation, rigorous forensic investigation, and the final determination of restitution. Should consumers contest the final ruling, the model ensures a formal escalation path via the Alternative Dispute Resolution Sector for Financial Services (LAPS SJK) or judicial litigation.

CONCLUSION

The current bank liability framework in Indonesia remains inadequate in addressing skimming crimes due to structural imbalances in evidentiary mechanisms and risk allocation. This study proposes a reconstructed liability model integrating strict liability and

burden shifting, positioning banks as primary risk bearers. The model requires preliminary compensation followed by verification, ensuring fairness, legal certainty, and effective protection for customers in the digital banking era. [*W*]

BIBLIOGRAPHY

Angela, Irene Maria, Aam Suryamah, and Deviana Yuanitasari. 2024. "Doktrin Res Ipsa Loquitur Pada Perlindungan Konsumen." *Widya Yuridika* 7 (1): 209–16. https://doi.org/10.31328/wy.v7i1.4778.

Begishev, Ildar, Elena Kirillova, Saphiya Mukhametgaliyeva, and E. Laxmi Lydia. 2024. "A Quantitative Evaluation of Digital Crimes and Their Impact on the Banking Industry." In *Proceedings of Eighth International Conference on Information System Design and Intelligent Applications (ISDIA 2024)*, 1:177–186. Cyber Security and Intelligent Systems. https://doi.org/10.1007/978-981-97-4892-1.

Ciaccio, Julia, and Ph.D. Ismail Onat. 2025. "An Analysis of ATM and Point-of-Sale Skimming." *Orion Policy Institute: Orion Forum, Cyber Security & Info Technologies*, 1–12. https://orionpolicy.org/an-analysis-of-atm-and-point-of-sale-skimming/

Hakim, Muhammad Raihan, Moody Rizqi, and Syailendra Putra. 2025. "Analysis of Digital Bank Customer Protection Against Loss of Funds in Accounts Reviewed According to Indonesian Positive Law Banks Play a Vital Role in Driving Indonesia ' s Economy , Serving as the Main Connector for Society in Conducting Various Financi." *Jurnal USM Law Review* 8 (2): 813–24. https://journals.usm.ac.id/index.php/julr/article/download/12073/6322/40223

Haris Karyadi, Hari Purnomo, Nurul Andriani, Siti Fauziah, and Wida Juliyah. 2025. "Optimalisasi Audit Forensik Digital Dalam Mengungkapkan Fraud Melalui Pemanfaatan Teknologi Informasi." *Prosiding Diseminasi Nasional Hasil Penelitian Dan Pengabdian Kepada Masyarakat Tahun 2025* 2 (1): 8. https://doi.org/10.30998/dinamika.v2i1.8338.

Hartono, Ridwan, and Hani Irhamdessetya. 2025. "Resolving Legal Disputes between Banks and Customers over Credit Default without Collateral through Banking Mediation & Financial Services Authority." *The Virtual International Conference on Economics, Law and Humanities* 4 (1): 326–34. https://callforpaper.unw.ac.id/index.php/ICOELH/article/view/1760

Kartini, Murtiningsih. 2022. "Kejahatan Elektronik Dengan Pemasangan Skimer Pada Sistem Transaksi Mesin Atm." *Yustitia* 8 (2): 211–25. https://doi.org/10.31943/yustitia.v8i2.147.

Kuntag, Rivaldo Fransiskus, Flora Pricilla Kalalo, and Anna S. Wahongan. 2021.

"Pertanggungjawaban Pelaku Usaha Terhadap Konsumen Yang Dirugikan Atas Kerusakan Barang Ditinjau Dari Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen." *Lex Privatum* IX (4): 151–57.

Lestari, Ayu, Muhaimin Muhaimin, and Diman Ade Mulada. 2022. "Tanggung Jawab Pihak Bank Kepada Nasabah Terhadap Kejahatan Skimming (Studi Di Bank Syariah Indonesia Mataram)." *Commerce Law* 2 (1): 105–13. https://doi.org/10.29303/commercelaw.v2i1.1374.

Linggoraharjo, Victoria. 2020. "Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming." *Jurnal Magister Hukum Argumentum* 7 (1): 34–46. https://doi.org/10.24123/argu.v7i1.3013.

Lorensa, Shella Amilia, and Siti Malikhatun Badriyah. 2023. "Perlindungan Hukum Terhadap Nasabah Prima Bank Dalam Resiko Layanan Pick Up Service." *Unes Law Reviw* 6 (2): 7430–38. https://doi.org/10.31933/unesrev.v6i2.

Mahardikha, Dian. 2020. "Penerapan Prinsip Tanggung Jawab Mutlak (Absolut Liability) Berkaitan Dengan Kerugian Konsumen Atas Penggunaan Produk Internet Banking." *Indonesia Private Law Review* 1 (2): 115–26. https://doi.org/10.25041/iplr.v1i2.2057.

Mahmud, Muhammad Isra. 2020. "Peran Vicarious Liability Dalam Pertanggungjawaban Korporasi (Studi Terhadap Kejahatan Korupsi Yang Dilakukan Oleh Kader Partai Politik)." *Jurnal Lex Renaissance* 5 (4): 767–79. https://doi.org/10.20885/JLR.vol5.iss4.art1

Malawai, Hendrik, and Aldi Septian Jamal. 2021. "Perlindungan Hukum Bagi Nasabah Dan Tanggung Jawab Bank Dalam Kasus Skimming." *Projustisia: Isu-Isu Krusial Dalam Hukum Keluarga* 1 (1).

Maulana, Ryan, Tarsisius Murwadji, and Helza Nova Litai. 2026. "Electronic Money : Consumer Protection Versus Legal Asymmetric Information." *Journal of Cultural Analysis and Social Change* 11 (1): 814–25. https://doi.org/10.64753/jcasc.v11i1.3957.

Monica, Eka Syafrina, Herlina Hanum Harahap, Nirwansyah Sukartara, and M Rifqi Romadhona. 2024. "Tanggung Jawab Bank Atas Peretasan Data Nasabah Menurut Sudut Pandang Hukum Perdata." *Journal Of Social Science Research* 4 (6): 7839–48. https://j-innovative.org/index.php/Innovative/article/view/16877.

Nafis Dwi Kartiko, Samuel Putra Soegiono, Carissa Amanda Siswanto, and Astrid Athina Indradewi. 2024. "Perlindungan Konsumen Sektor Keuangan: Peran OJK Dalam Menghadapi Ancaman Phising Dan Skimming." *IURIS STUDIA: Jurnal Kajian Hukum* Volume 5 (2): 347–63. https://doi.org/10.55357/is.v5i2.616

Nikkel, Bruce. 2020. "Fintech Forensics : Criminal Investigation and Digital Evidence in Financial Technologies." *Forensic Science International: Digital Investigation* 33:1–17.

https://doi.org/10.1016/j.fsidi.2020.200908.

Otoritas Jasa Keuangan. 2024. "Pedoman Keamanan Siber Bagi Penyelenggara Inovasi Teknologi Sektor Keuangan." *OJK*. Jakarta. https://ojk.go.id/id/Publikasi/Roadmap-dan-Pedoman/ITSK/Pages/Pedoman-Keamanan-Siber-Bagi-Penyelenggara-Inovasi-Teknologi-Sektor-Keuangan.aspx

R.Subekti. 2015. *Hukum Pembuktian*. 19th ed. Jakarta: Balai Pustaka.

Santiago, Faisal. 2018. "Banking Responsibility to Customers." *European Research Studies Journa* XXI (1): 321–30.

Sari, Rita Puspita. 2025. "Ancaman Digital 2025: 133,4 Juta Serangan Siber Terjadi Di RI." CyberHub. 2025. https://cyberhub.id/berita/ancaman-digital-2025-serangan-siber-ri.

Shaw, S. 2019. "Skimming : Attacking Your Financial Security," no. December, 1–11.

Sihombing, Jonker. 2010. *Penjaminan Simpanan Nasabah Perbankan*. Bandung: PT. Alumni.

Sipahutar, Ervina Sari, Indra Gunawan Purba, and Anjani Sipahutar. 2022. "Legal Analysis of the Crime of Skimming in Indonesia According to the Electronic Information and Transactions Law (ITE) Number 11 of 2008 Concerning Information and Electronic Transactions." *Budapest International Research and Critics Institute-Journal (BIRCI-Journal)* 5 (2): 9099–9109. https://doi.org/10.33258/birci.v5i2.4696 9099.

Sitorus, Rolib, and Felicia Saphira. 2024. "Bank ' s Responsibility for Customer Money Losses in Inter-Bank Transfer Errors (Study of Decision No . 148 / PID . SUS / 2021 / PN SBY)." *Journal of Legal and Cultural Analytics (JLCA)* 3 (4): 363–72. https://doi.org/10.55927/jlca.v3i4.11904.

Suciara, Angelica, Bryan Idias, Nathasya Jhonray Siregar, Tasya Amira Frananda Siregar, and Tri Widyasto Prabowo. 2026. "Strict Liability vs Fault Based : Perbandingan Indonesia Dengan Jepang Terhadap Kebocoran Data." *Al-Zayn: Jurnal Ilmu Sosial & Hukum* 4 (1): 739–49. https://doi.org/10.61104/alz.v4i1.3146.

Suheimi. 1995. *Kejahatan Komputer*. 1st ed. Jakarta: Andi Offset.

Syafa, Adia Surya Asy, and Imam Budi Santoso. 2024. "Modus Operandi Kejahatan Skimming Terhadap Nasabah Berdasarkan Perspektif Hukum Perbankan." *Jurnal Ilmiah Wahana Pendidikan* 10 (8): 187–94. https://doi.org/10.5281/zenodo.11080130.

Tjitrokusmo, Evelyn, Stefani Susiani, Monika Kristanti, and Agustinus Nugroho. 2014. "Analisa Pengaruh Service Recovery Terhadap Kepuasan Konsumen Di Hotel 'X.'" *Jurnal Hospitality Dan Manajemen Jasa*, 76–90.

Tribratanews. 2021. "Bobol Duit Nasabah Hingga Rp 3 Miliar, 2 Sindikat Skimming Diringkus Polda Bali _ Kumparan." *Tribratanews.Polri.Go.Id.*, February 9, 2021. https://tribratanews.polri.go.id/blog/nasional-3/bobol-duit-nasabah-hingga-rp-3-

milyar-polda-bali-ringkus-2-sindikat-skimming-30495.

Wardani, Dian Eka Kusuma, Raodiah Raodiah, and Indarahayu M. Umar Gazali. 2025. "Comparative Legal Regulation And Enforcement Of Skimming Crimes In Indonesia And The United States Of America." *Kanun: Jurnal Ilmu Hukum* 27 (3): 745–68. https://doi.org/10.24815/kanun.v27i3.49047.

Wattimena, Yohanes Yosua, Henrikus Renjaan, and Carina Budi Siswani. 2025. "Responsibility of Bank Financial Institutions for The Loss of Customer Money Saved In Their Accounts." *Legal Brief* 14 (5): 1001–9. https://doi.org/10.35335/legal.v14i5.1486 .

Wei, Wei, Jinjiu Li, Longbing Cao, Yuming Ou, and Jiahang Chen. 2013. "Effective Detection of Sophisticated Online Banking Fraud on Extremely Imbalanced Data." *World Wide Web* 16:449–475. https://doi.org/10.1007/s11280-012-0178-0.

Wicaksana, Aliph Ramahadi, and Baidhowi Baidhowi. 2025. "Tanggung Jawab Hukum Bank Terhadap Kerugian Nasabah Dalam Kasus Skimming Dan Kejahatan Siber Di Indonesia _ Jurnal Res Justitia_ Jurnal Ilmu Hukum." *Jurnal Res Justitia : Jurnal Ilmu Hukum* 5 (2). https://doi.org/10.46306/rj.v5i2.286.

Yunita, Laely Nova, Elina Elmaghfiroh, Fadhilah Rahmawati, Zedny Amiq Elmina, Azharia Sebrina, Putri Zakiah Rohmah, Bagian Revian Ashar, Nur Jannah Salsabila, Laeli Ambar Dwi Cahyani, and Moch Maola Gansehawa. 2024. "Upaya Pencegahan Praktik Penipuan Online Melalui Sosialisasi Cyberfraud Di Desa Pucangrejo Efforts To Prevent Online Fraud Practices Through Cyberfraud Socialization in Pucangrejo Village." *Jurnal Pengabdian Dan Kesejahteraan Masyarakat* 1 (3). https://doi.org/10.62951/solusibersama.v1i3.437

Yusnita, Ria, Lydia Aprilia Pratiwi, and Helfira Citra. 2025. "Perlindungan Konsumen Terhadap Kerugian Akibat Skimming Dan Kebocoran Data Di Bank." *Jurnal Kajian Hukum Dan Kebijakan Publik* 1 (4): 380–83. https://jurnal.kopusindo.com/index.php/jkhkb.