

Legal Concept of Strict Liability for Banks in the Misuse of Customer Personal Data

Zulfi Diane Zaini^{1*}, Efendi Putra²

¹Lecturer of the Master of Law Study Program, Bandar Lampung University

²Students of the Master of Law Study Program, Bandar Lampung University

DOI: <https://doi.org/10.36348/sijlcj.2026.v09i10.001>

| Received: 20.05.2026 | Accepted: 09.07.2026 | Published: 01.10.2026

*Corresponding author: Zulfi Diane Zaini

Lecturer of the Master of Law Study Program, Bandar Lampung University

Abstract

Leaks and misuse of banking customer personal data in Indonesia are increasingly common along with the acceleration of digital transformation. Although Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has been passed, the burden of proving fault still often presents a challenge for customers as the injured party. This study aims to analyze the urgency of implementing the principle of strict liability as a legal protection instrument for customers in cases of personal data misuse by banking institutions. The research method used is a normative juridical approach with a statutory approach and a conceptual approach. The results show that the application of the principle of fault liability in the highly regulated banking industry is no longer relevant due to information asymmetry and the complexity of information technology systems. Adopting the principle of strict liability holds banks accountable for any failure to protect data without requiring customers to prove fault on their part. The implementation of this principle is expected to encourage banking institutions to maximize cybersecurity standards while providing legal certainty and redress for customers more effectively and efficiently.

Keywords: Strict Liability, Personal Data Protection, Banking, Customers.

Copyright © 2026 The Author(s): This is an open-access article distributed under the terms of the Creative Commons Attribution **4.0 International License (CC BY-NC 4.0)** which permits unrestricted use, distribution, and reproduction in any medium for non-commercial use provided the original author and source are credited.

A. INTRODUCTION

The era of banking digitalization has transformed the financial transaction landscape, making it heavily reliant on the processing of personal data on a massive scale. Banks now function not only as financial intermediaries but also as managers of massive databases containing sensitive customer information, from personal identities to financial profiles. However, this rapid technological innovation has not been accompanied by a fully tamper-proof security system, making data breaches a real threat that continues to haunt the financial industry (Maulia: 2017).

Cases of customer personal data breaches in Indonesia have shown a worrying trend in recent years. This failure to protect data often results in material and immaterial losses for customers, such as account balance drains, social engineering-based fraud, and the use of customer identities for illegal online loans. This phenomenon demonstrates that the risks faced by customers far outweigh their ability to control the security of the data they have submitted to banks (Danny: 2021).

Within the conventional legal framework stipulated in the Civil Code (KUHPPerdata), legal liability for unlawful acts (PMH) is based on Article 1365, which requires proof of fault (fault liability). Customers who feel they have been harmed are required to prove that the data breach occurred due to a specific error or negligence on the part of the bank. This presents a significant obstacle given the information asymmetry and disparity in technical capacity between individual customers and banking institutions with substantial resources.

The complexity of banking cybersecurity systems makes it nearly impossible for customers to pinpoint the source of a data breach. Whether the leak originated from a system vulnerability (bug), a third-party attack (hacker), or insider involvement (insider threat) remains largely unknown to customers. Requiring customers to prove the bank's fault in such a complex IT system constitutes an unfair and disproportionate burden of proof (Makarim: 2020).

The enactment of Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) has indeed provided a breath of fresh air for data subject

protection. However, in the context of civil liability, existing mechanisms are often mired in debates over the extent to which banks have fulfilled their "duty of care." If banks can prove they followed standard operating procedures (SOPs) in accordance with regulations, they are often exempt from legal liability even if customers have suffered real losses.

This is where the relevance of the strict liability doctrine begins to emerge. This principle imposes responsibility on business actors without the need to prove fault. In the highly regulated and high-risk banking industry, banks should assume full responsibility for all risks arising from their business activities, including the risk of data protection system failure resulting in the misuse of customer information (Dewi: 2016).

The application of strict liability is based on the theory of risk distribution, where banks are considered the party best able to bear and transfer risk through insurance premiums or system strengthening. Because banks derive economic benefits from the use of customer data in their digital services, morally and legally, they must also bear the risk of system failure without shifting the burden of proof to customers, who are in a weaker bargaining position.

Comparatively, several international jurisdictions have begun adopting principles similar to strict liability for critical sectors to provide stronger consumer protection. Indonesia needs to consider reorienting its legal liability policy in the banking sector, moving away from a formalistic-procedural approach and toward a substantive-justice approach that protects the interests of customers as the rightful owners of personal data.

The urgency of implementing strict liability also serves as a deterrent. With the threat of absolute liability, banking institutions will automatically be compelled to allocate greater investment in cybersecurity systems and conduct regular data audits. Banks will no longer feel "safe" simply by meeting minimum regulatory standards, but will strive to achieve the highest security standards due to the significant legal risks looming.

In 2023, an incident occurred in which a major Indonesian bank experienced a system disruption for several days due to a ransomware attack by an international hacker group. The data of millions of customers, including names, phone numbers, account numbers, and transaction details, was leaked and sold on the dark web. Several customers suffered direct losses in the form of balance breaches through the cloning technique of the leaked data. When customers sued the bank, the bank argued that they had implemented security systems in accordance with OJK standards and that the attack was a force majeure or the actions of a third party (hacker) beyond the bank's control.

Without a legal breakthrough regarding this liability principle, customers will remain vulnerable. Public trust in the digital banking system could be eroded if every data breach results in customers being blamed or struggling to seek justice. Based on this explanation, an in-depth study of the legal aspects of strict liability for banks is essential to strengthening a safe, fair, and trustworthy digital economy ecosystem in Indonesia.

B. RESEARCH METHOD

The method in this research uses a type of normative-empirical legal research by examining legal regulations related to facts in the field (Soerjono: 2004). The approach used in this research is using a Case Approach by examining customer data leaks carried out by the Bank. This is very detrimental to customers from a civil law and criminal law perspective. Thus, the multiple case method also needs to be included in the analysis.

C. RESULTS AND DISCUSSION

1. Implementation of the Strict Liability Concept as a Deterrent Effect Function of Banks towards Customers in Indonesia

The application of the concept of absolute responsibility, or what is legally known as strict liability, in the banking sector represents an essential legal breakthrough to address data security challenges in Indonesia's current digital economy. Philosophically, this doctrine positions banks as fully responsible for all losses arising from the breach of customers' personal data, without questioning the existence of any element of fault or negligence. In the context of its preventive function, the application of this principle acts as a deterrent, forcing banking institutions to operate at the highest level of vigilance.

This deterrent effect arises from the financial and reputational pressures banks automatically face when a system failure occurs. When banks realize they no longer have the luxury of defending themselves by following standard operating procedures or by blaming third-party interference, they will view data security not as a cost burden but as a crucial investment. The fear of immediate and certain compensation obligations creates pressure for bank management to strengthen their information technology infrastructure beyond the minimum standards set by regulators such as the Financial Services Authority (Erlina: 2020).

Specifically, this concept also aims to eliminate information asymmetry, which has historically been a barrier to customers seeking justice. In conventional legal disputes, customers often lose before the fight because the burden of proof falls on them, even though they don't have access to server logs or the bank's internal security systems. With strict liability, this burden of proof is shifted or even eliminated from customers, placing banks in a position where they must mitigate risks early. This directly forces banks to implement much

stricter internal oversight against potential insider threats and external cyberattacks.

This implementation will also systematically transform the organizational culture of banking in Indonesia, making it more transparent and accountable. The awareness that the law will always side with customer data protection through the strict liability scheme will encourage banks to continue conducting regular and independent security audits. The resulting deterrent effect is not intended to cripple the banking industry, but rather to create a healthy financial ecosystem where any failure to protect data has real, swift, and equitable legal consequences, ultimately maintaining public trust in the digitalization of national banking.

The deterrent effect of this principle works by changing the risk calculation at the banking management level. Previously, with the principle of fault-based liability, banks often felt legally secure if they met minimum operational procedure standards. However, with absolute liability, banks will realize that even the slightest system failure will immediately result in an obligation to compensate for losses, with no room for evasion.

This legal certainty forces banks to shift from a formalistic compliance approach to a substantive security approach. Banks will no longer simply pursue security certifications to avoid regulatory obligations, but will instead invest in the most advanced encryption and cyber protection technology. This is because banks realize that the cost of paying mass compensation would far outweigh the investment in information system security.

Furthermore, this principle effectively addresses the problem of information asymmetry, which has been so detrimental to customers. In a cyber dispute, it is nearly impossible for customers to prove the location of the leak within the maze of a bank's highly complex technology systems. With strict liability, these technical obstacles to proof are removed, forcing banks, as those with full access to the system, to be more vigilant, as the burden of responsibility shifts entirely to them.

The implementation of this concept also has a significant impact on internal oversight of insider threats. Banks will tighten data access mechanisms and conduct more intensive monitoring of employee behavior to prevent data leaks. This is a preventative response by banks, as they understand that employee misconduct cannot be used to absolve the institution from legal responsibility before customers.

This deterrent effect also targets reputational damage, which is vital to the trust-based banking industry. When banks are faced with a strict liability scheme, they tend to be more transparent in their risk

mitigation and incident reporting. Fear of the destruction of public trust due to a series of lawsuits automatically granted by the courts will encourage banks to maintain their highest security performance.

Sociologically, the implementation of strict liability in Indonesia will send a strong message to other players in the digital financial industry. This message emphasizes that personal data protection is not merely a business accessory but a fundamental obligation with serious legal consequences (Zulfi: 2016). This creates a new standard in the market, where data security becomes a healthy competition between banking institutions to win customer sympathy and trust.

From a substantive justice perspective, this principle balances the unequal bargaining position between individual customers and large banking corporations. Customers are no longer positioned as the weak party whose rights are neglected in the event of a cyberattack. The assurance that banks will be held absolutely accountable provides a sense of security for the public to continue using digital banking services without undue worry about the fate of their data.

This principle also encourages the creation of a more mature cyber insurance mechanism in the Indonesian financial industry. Banks will be encouraged to transfer some of their risk through cyber insurance to mitigate potential losses from absolute compensation claims. This indirectly creates a more integrated and professional data security support ecosystem, where insurers will also demand certain security standards from banks.

In the long term, the implementation of strict liability will accelerate the digital maturity of national banking. Every bank will have a full-time cybersecurity command center to detect threats in real time. This transformation is a direct result of the deterrent effect of the law, which leaves no room for negligence or technical incompetence in maintaining the integrity of customer data.

This deterrent effect is also crucial in the face of ransomware attacks or sophisticated hacking from abroad. Even if banks argue they are victims of criminal attacks, from a strict liability perspective, they remain liable to their customers for failing to provide data storage that is impermeable to third-party intervention. This legal logic forces banks to never be satisfied with their current defenses (Radian: 2012).

Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is the primary legal basis in Indonesia, fully enforced, governing the management of personal data, protecting individual rights, and imposing strict sanctions for violators, both individuals and corporations. This law covers general and specific personal data protection, both in physical and electronic

form, with the aim of guaranteeing privacy as a human right. The PDP Law provides a philosophical foundation for the implementation of this responsibility. However, more specific legal or sectoral regulation regarding absolute liability would clarify the direction of consumer protection. Without absolute civil sanctions, banks may still view administrative fines as ordinary business costs that can be compensated.

The PDP Law outlines several rights that must be protected by an institution, in this case, a bank, regarding personal data breaches, as follows:

- a) The right to know: Every individual has the right to know what types of personal data are collected and how that data is used.
- b) The right to access: Data subjects have the right to access personal data stored by the collecting party.
- c) The right to change or rectify, meaning that if the collected personal data is incorrect or inaccurate, individuals have the right to have it corrected.
- d) The right to be forgotten, meaning that data subjects can request the deletion of their personal data if it is no longer necessary for the purpose of its initial collection or if there is a legal basis for doing so.
- e) The right to restrict use, meaning that data subjects can restrict the processing of their personal data in certain situations.

These rights are naturally linked to the strict liability that must be imposed on bank customers who suffer losses. The implementation of this concept also triggers innovation in authentication and privacy protection methods, such as the use of more secure biometrics and blockchain technology. Banks will become pioneers in adopting privacy technologies to minimize their exposure to legal risks. This innovation will ultimately benefit banks not only legally but also improve the overall quality of banking services internationally.

Firm implementation of strict liability will place Indonesia on par with developed countries with very high data protection standards, such as those in the European Union. This will increase the competitiveness of national banks on the global stage, as they are perceived to have strong legal protection standards for global investors and customers. This deterrent effect ultimately transforms into social capital in the form of global trust in the domestic financial system.

The concept of strict liability for banks in cases of misuse of personal data is a concrete manifestation of the state's presence in protecting the human right to privacy. Through this deterrent effect, banks are forced to consistently prioritize customer security over mere profit. Harmonizing legal certainty, technological strength, and institutional responsibility will be the

foundation for a resilient and trusted future for Indonesian digital banking.

2. Legal Aspects of Bank Strict Liability for Misuse of Customer Personal Data in Realizing Compensation

The doctrine of strict liability shifts this paradigm by establishing that banks, as data controllers, are responsible for any losses incurred without needing to prove fault. This is based on the premise that banks benefit economically from processing customer data, and therefore must bear all risks inherent in such activities. Therefore, when personal data misuse occurs, the legal focus is no longer on how the bank operates, but rather on the fact that harm has occurred to the data subject, who should be protected.

This legal aspect is crucial in achieving swift and effective compensation for affected customers. Through strict liability, litigation or out-of-court dispute resolution processes are no longer bogged down in technical debates about the bank's cybersecurity standards. This legal certainty ensures that customers' rights to economic recovery for lost balances or misused data can be fulfilled instantly once the loss is factually verified to have originated within the banking system.

The application of this principle also serves as a risk-sharing instrument, with banks considered the entities best equipped to manage risk through insurance mechanisms or emergency fund reserves. By requiring banks to be strictly liable, the law encourages the creation of a more accountable and transparent banking ecosystem. Banks will be more motivated to conduct regular security audits because they recognize that any technical failure will directly impact the institution's financial obligations, leaving no room for defense based on standard procedures (Danrivanto: 2010).

From a social justice perspective, strict liability for banks is a form of compensation for the information asymmetry that exists between financial service providers and service users. Customers submit their personal data based on complete trust in the institution's integrity, so failure to safeguard that data should be considered a breach of public trust. This concept places the protection of human dignity and privacy above procedural corporate interests, which often hide behind bureaucratic and technological complexities.

The impact of implementing strict liability will force banks in Indonesia to raise their cybersecurity standards beyond the minimum limits stipulated in regulations. This is because banks can no longer simply fulfill administrative requirements to avoid sanctions but must truly ensure their systems are impervious to attacks to avoid mass compensation claims. This, in turn, creates a deterrent effect and encourages innovation for banks to create more sophisticated, multi-layered defense systems.

Legally, the basis for applying this principle can actually be found in the development of interpretations of consumer protection laws and personal data protection laws. Although laws and regulations often still use a fault-based basis, in judicial practice, judges can use legal findings to impose absolute liability for the sake of substantive justice. This is important so that the law does not lag behind the pace of technology, which is often misused by third parties through weak banking system loopholes.

Regulations regarding compensation based on strict liability will also simplify the claims mechanism for customers who fall victim to cyber fraud. Customers will no longer need to spend time and money hiring digital forensics experts to prove bank negligence. Simply by proving that an unauthorized transaction or identity information leaked from the bank's database has occurred, the bank's legal obligation to restore the customer's rights is established and must be immediately enforced.

Strict liability encourages banks to be more selective and cautious in collaborating with third parties or technology vendors. Banks will apply very strict selection standards because they understand that any errors made by their appointed vendors will remain the bank's absolute responsibility to customers. Oversight of this data supply chain ecosystem is vital in minimizing data misuse by parties with limited access to banking infrastructure. Legal aspects and updates regarding

Legal strictness regarding strict liability will also enhance the reputation of national banks internationally. Countries with strong data protection and robust enforcement of compensation will be considered safe jurisdictions for investment and global financial transactions. This global trust will ultimately have a positive impact on national economic stability due to the guarantee of data security supported by a legal defense system that strongly supports the rights of data owners.

This principle also puts pressure on regulators to continuously update banking security standards dynamically. The Financial Services Authority can use this strict liability parameter as a benchmark for measuring the health of a bank's risk management (Zainudin: 2018). If a bank frequently experiences compensation claims based on strict liability, this is a strong signal for regulators to intervene or conduct an in-depth audit of the integrity of the bank's information technology.

In the long term, the existence of strict liability will foster a collective awareness among all stakeholders regarding the importance of data sovereignty. Customer personal data will no longer be viewed as a commodity that can be processed without risk, but rather as a legal trust that has direct financial consequences if not safeguarded. This shift in values is fundamental to

building a mature digital society where every individual's rights are respected with tangible, not merely symbolic, redress mechanisms.

The implementation of absolute responsibility will also reduce the burden on courts from protracted small disputes. With certainty that the bank is definitely responsible, many data leakage disputes can be resolved through peace or insurance mechanisms because the bank already knows its legal position which is difficult to win if the case continues. This creates efficiency in the justice system and provides faster legal satisfaction for the wider community affected by cyber incidents.

The calculation of compensation in an absolute liability scheme begins with determining the components of real or material losses suffered by the customer. This component includes the entire amount of funds lost from customer accounts due to unauthorized transactions originating from data leaks. Apart from the lost principal value, the calculation must also include the accumulated interest or potential profits that the customer would have received if the funds had remained under his management. Banks are obliged to return the economic value to its original position or make full restitution as soon as the fact of the data leak is verified without waiting for the internal investigation process regarding who the perpetrator of the hack is to be completed.

Furthermore, the calculation mechanism must also accommodate immaterial losses that often accompany misuse of personal data. These losses include loss of privacy, psychological stress, and damage to customers' reputations or credit scores which could hinder their access to financial services in the future. Although the calculation of immaterial losses is subjective, in progressive law, this value can be quantified based on standards of propriety or the cost of restoring one's reputation. The bank in this case bears the financial burden of ensuring that the customer's identity is restored through the central identity authority system as well as providing compensation for the inconvenience caused by the failure of the bank's system.

Another very crucial aspect of this mechanism is the application of consequential costs that arise as a direct impact of data leaks. These costs include expenses incurred by customers for processing reporting, initial legal costs, and costs for replacing compromised documents or identity cards. In the principle of strict liability, all these costs are the absolute responsibility of the bank as part of the business risk. Banks must provide compensation allocations that cover operational costs of directly restoring customer rights. Thus, the calculation of compensation is not only passive regarding lost funds, but actively covers the entire spectrum of impacts experienced by customers in order to realize substantive justice.

D. CONCLUSION

Based on the above discussion, it can be concluded that the implementation of the strict liability concept in the Indonesian banking sector is a crucial legal instrument for balancing the imbalanced bargaining power between customers and financial institutions. By shifting the burden of absolute responsibility to banks for any personal data breach, the law creates a significant deterrent effect, as banks can no longer hide behind complex administrative or technical defenses. This forces banks to shift from mere formal compliance to substantial cybersecurity investments to avoid the financial and reputational risks that inevitably arise from verified system failures. Ultimately, this strict liability serves as a catalyst for the swift and effective delivery of justice in the restoration of customer rights. Furthermore, the application of the legal aspect of strict liability for banks is a highly effective legal solution to guarantee the restoration of customer rights in cases of personal data misuse. By shifting the burden of full responsibility to banks without the need for proof of fault, this concept is able to break down the information asymmetry barrier that has historically hampered customers as the technical and financially disadvantaged parties. This conclusion confirms that strict liability is not merely a punitive instrument, but rather a legal certainty mechanism that ensures swift and comprehensive compensation. Through this scheme, banks are encouraged to fairly shoulder the business risks of their digital activities, ultimately strengthening industry security standards and restoring public confidence in the integrity of the national banking system.

REFERENCES

- Kobrata, Danny, "Personal Data Protection Bill: A Waiting Period," January 2021, Personal Data Protection Bill: A Waiting Period (hukumonline.com)
- Budhijanto, Danrivanto, "Telecommunications, Broadcasting & Information Technology Law: Regulation & Convergence," PT. Refika Aditama, Bandung, 2010, p. 4
- Dewi, S. The Concept of Legal Protection for Privacy and Personal Data Associated with the Use of Cloud Computing in Indonesia." Yustisia Jurnal Hukum, 2016, 5 (1), 22-30.
- Erlina, Melisa Safitri, "Comparative Analysis Between Ordinary Patent Protection and Simple Patent Protection Based on the Patent Law," Legal Regulations Volume 15 Number 1, January 2020, p. 35.
- Makarim, E. "Notaries and Electronic Transactions: A Legal Study on Cyber Notaries or Electronic Notaries in Indonesia." PT RajaGrafindo Persada, 2020, p. 20.
- Jayantina Islami, Maulia "Challenges in Implementing Indonesia's National Cybersecurity Strategy as Perceived from the Global Cybersecurity Index Assessment," Journal of Telematics and Information Society, Vol. 8 No. (2017), p. 137.
- Radian Adi Nugraha, "Juridical Analysis of Personal Data Protection in Cloud Computing Systems in the Light of the Electronic Information and Transactions Law," University of Indonesia, 2012, p. 31.
- Soerjono Soekanto and Sri Mamudji, "Research on Normative Law," 8th ed. (Jakarta: PT RajaGrafindo Persada, 2004), p. 12.
- Zainudin Hasan, "Implications of the Return of State Finances to Judges' Verdicts in Corruption Cases of Funds for the National Independent Rural Community Development Program in Lampung Province," Progressive Justice Volume 9 Number 2, September 2018, p. 138.
- Diane Zaini Zulfi, "Juridical Analysis of Legal Settlements Carried Out by Banks for Debtors in Default," Independent Lecturer Research Report, 2016, Published by Bandar Lampung University.