International Journal of Law, Crime and Justice

E-ISSN: 3047-1362
P-ISSN: 3047-1370

(Research/ Review) Article

Legal Protection For Customer Data Security In Internet Banking Systems

Ayu Margareth R. Sitinjak [1], Martono Anggusti [2], and Roida Nababan[3]

[1] Faculty of Law, HKBP Nommensen University:; e-mail : ayu.sitinjak@student.uhn.ac.id
[2] Faculty of Law, HKBP Nommensen University:;; e-mail : martono.pang@gmail.com
[3] Faculty of Law, HKBP Nommensen University:;: e-mail : roidanababan@uhn.ac.id

Abstract: This study discusses legal protection for customer data security in internet banking systems in Indonesia, especially after the enactment of various related laws and regulations. The purpose of this study is to analyze how legal protection is applied and the legal measures that can be taken by customers if their data is not protected. The research method used is normative legal research with a qualitative approach, through data collection from secondary sources such as laws, legal literature, and official documents. The final findings show that although legal protection has improved with the existence of relevant laws, there are still challenges in its implementation. Customers have the right to file complaints and legal claims in the event of a data breach, which includes complaint procedures with banks and the Financial Services Authority. Compliance with regulations and the principles of legal justice are essential to maintaining public trust in the banking sector.

Keywords: Banking Law, Customer Data Protection, Consumer Rights

1. Introduction

A rapidly developing technology currently being used by banks is Internet Banking. Internet Banking is not a foreign term to Indonesians, due to the large number of national banks that use Internet Banking services. In other words, digital players around the world need what is known as electronic space for their activities.

Internet banking is used by customers to make payments online. Internet banking also facilitates banking activities through computer networks anytime and anywhere quickly, easily, and securely because it is supported by a strong security system. This is useful for ensuring the security and confidentiality of data and transactions carried out by customers. In addition, with internet banking, banks can increase the speed of service and reach in banking activities. In the development of banking technology such as internet banking, banks must pay attention to customer protection aspects, especially security related to customer privacy.

In the context of rapid developments in information technology and the digitization of financial services, financial institutions face new challenges in maintaining the security and confidentiality of customer personal data Data breaches not only cause financial losses to customers but can also damage the reputation of financial institutions, undermine public trust, and affect the stability of the financial system as a whole. Therefore, protecting customers' personal data must be a top priority in the management of data and operations of financial institutions. Effective protection is not only important to prevent losses for customers but also to ensure the integrity and credibility of financial institutions in the public eye and maintain the stability of the financial sector as a whole.

In facing these challenges, various regulations have been implemented to protect personal data. One important legal basis is Law Number 8 of 1999 concerning Consumer Protection. Law No. 8 of 1999, Article 4, states that consumers have the right to comfort, security, and safety in consuming goods and/or services, and Article 19 states that business

Received: August 01, 2025
Revised: August 16, 2025
Accepted: August 30, 2025
Published: September 15, 2025
Curr. Ver.: September 15, 2025

actors are responsible for providing compensation for damage, contamination, and/or consumer losses resulting from consuming goods and/or services produced or traded.

In response to the need for more comprehensive data protection, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) was introduced. Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) considers that the protection of personal data is a human right that is part of personal protection, therefore it is necessary to provide a legal basis to ensure the security of personal data, based on the 1945 Constitution of the Republic of Indonesia; that the protection of personal data is intended to guarantee the rights of citizens to personal protection and to foster public awareness and ensure recognition and respect for the importance of personal data protection. The Law on Personal Data Protection reflects the need to protect personal data in an ever-evolving digital context, providing a stronger and more specific legal basis for personal data protection.

In addition to legislation, Financial Services Authority (OJK) regulations also play an important role in ensuring the protection of personal data in the financial services sector. Financial Services Authority Regulation Number 6/SEOJK.07/2022 also regulates the confidentiality and security of consumers' personal data and/or information, namely that Financial Services Business Operators are prohibited in any way from providing personal data and/or information about their consumers to third parties; in the event that a Financial Services Business Operator obtains the personal data and/or information of an individual and/ or a group of people from another party and the Financial Services Business Operator will use the data and/or information to carry out its activities, the Financial Services Business Operator must have a written statement that the other party has obtained written consent from the person and/or group of people to provide the personal data and/or information to any party, including the Financial Services Business Operator. Bank Indonesia Regulation Number 7/6/PBI/2005 also regulates the transparency of bank product information and the use of customer personal data.

Misuse of privacy data or personal data on the internet is mostly commercial in nature, but it is also possible that personal data may be misused for other harmful purposes. Another issue related to the privacy of internet users is the existence of cookies. These programs can track the activities of internet users, such as which websites they visit, how long they browse on those websites, and various other activity data. Privacy issues are a right for everyone in the sense that no one should be allowed to freely enter another person's privacy.

Then, the misuse of personal data in internet banking is phishing. This is a type of fraud where perpetrators attempt to obtain sensitive information such as passwords, credit card numbers, or personal data by pretending to be a trusted entity through text messages, emails, or fake websites. In the case of internet banking, phishing attacks can occur through text messages that direct customers to access fake websites that mimic the official appearance of internet banking applications. In addition to phishing, social engineering programs also pose a significant threat to the security of customers' personal data. Social engineering involves psychological manipulation of individuals to obtain confidential information or access to systems. In the context of internet banking, social engineering attacks can occur through phone calls or text messages claiming to be from bank officials or other authorities, asking customers to provide personal information or perform certain actions that threaten data security.

According to the customer confidentiality policy of Bank Mandiri Taspen's internet banking service, the internet banking application is guaranteed to use an international standard security system with 2048-bit SSL encryption (Secure Socket Layer 2048-bit Encryption) that will scramble transaction data and protect communications between the customer's computer and the Bank Mandiri Taspen server. To add to the security, an Auto Logoff (session time out) method is used if the customer forgets to log out. After 10 minutes of inactivity, the customer's access will be deactivated.

A case regarding customer data security occurred when the plaintiff, Samsuduri, filed a lawsuit against Bank Mandiri at the Surabaya District Court because his personal data as a customer was leaked to the public. The leaked personal data included his name, full address, customer information file (CIF) number, and his mother's maiden name. It is suspected that the customer data leak occurred after conducting online transactions using a Bank Mandiri account. It was later discovered that the data was disseminated by a customer who had a relative working at Bank Mandiri.

Based on this background, this study aims to analyze "Legal Protection of Customer Data Security in Internet Banking Systems." In this study, the researcher will also analyze how

customer data security is legally protected in internet banking services and what legal measures customers can take if their data in internet banking is not protected.

2. Research Method

In writing this journal, the author used the normative legal research method, which is legal research conducted by examining reference materials or secondary data. The data collection method used in this research is library research. The data collected through this literature study was gathered by collecting data or information from various written sources, such as books, laws and regulations, journals, scientific articles, official documents, and other written sources related to legal protection of customer data security. This method is used to understand theories, concepts, or previous research results relevant to the topic being studied. As well as analyzing data with descriptive qualitative methods, namely analyzing the collected data processed in the form of descriptions and explanations systematically using sentences to obtain systematic and understandable results or explanations. This is followed by drawing conclusions that start from a general understanding that is already known and end with a specific conclusion.

3. Results and Discussion

3.1. Legal protection for customer data security in Internet Banking services

Legal protection for customer data security in Internet Banking services is a crucial aspect of data management in today's digital era. With the enactment of Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998, Law Number 27 of 2022, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022 concerning Personal Data Protection, and Bank Indonesia Regulation Number 7/6/PBI/2005 concerning transparency of bank product information and the use of customer personal data, Indonesia demonstrates its commitment to protecting banking customer data more stringently and in a structured manner. These three regulations aim to provide better protection for personal data and ensure that data management is carried out according to protection principles that comply with national and international standards.

Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998, Law Number 27 of 2022, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022 concerning Personal Data Protection and Bank Indonesia Regulation Number 7/6/PBI/2005 concerning transparency of bank product information and the use of customer personal data regulate the principles of customer data protection, namely clarity, certainty, transparency, and data security. The principle of clarity requires banking institutions to provide clear and easy-to-understand information regarding how customer data will be collected, used, and stored. Certainty in the obligation of banking institutions to obtain customer consent before collecting and processing customer data, and to ensure that the data is only used in accordance with the agreed purposes. The transparency principle ensures that customers receive complete information regarding their rights regarding customer data, while the security principle requires banking institutions to take technical steps to protect data from misuse.

Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998, Law Number 27 of 2022, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022 concerning Personal Data Protection and Bank Indonesia Regulation Number 7/6/PBI/2005 concerning transparency of bank product information and the use of customer personal data also establish clear rights and obligations for parties involved in customer data management. Customers have the right to access, correct, or delete their personal data in accordance with applicable provisions. On the other hand, banking institutions are obliged to provide transparent information to customers regarding how customer data is managed, as well as to maintain the security of that data. This obligation includes implementing strict procedures in the collection, storage, and use of customer data to ensure that it is not misused.

Law Number 8 of 1999 concerning Consumer Protection has the responsibility to protect customer data in accordance with Article 4, namely that consumers have the right to comfort,

security and safety in consuming goods and/or services and Article 19, namely that business actors are responsible for providing compensation for damage, pollution and/or losses to consumers due to consuming goods and/or services produced or traded.

Law Number 27 of 2022 also has the responsibility to protect customer data in accordance with Article 3 letters a, g and h. Letter a, namely what is meant by the "principle of protection" is that every processing of personal data is carried out by providing protection to the personal data subject for their personal data and personal data from being misused. Letter g, namely what is meant by the "principle of accountability" is that all parties related to the processing and supervision of personal data act responsibly so as to guarantee the balance of rights and obligations of the related parties including the personal data subject and letter h, namely what is meant by the "principle of confidentiality" is that personal data is protected from unauthorized parties and/or from unauthorized personal data processing activities.

Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022 is responsible for protecting the interests of customers and the public, as stipulated in Article 11. Financial Services Providers (PUJK) are prohibited from providing personal data and/or information regarding consumers to other parties; requiring consumers to agree to share personal data and/or information as a condition of using products and/or services; using personal data and/or information of consumers who have terminated product and/or service agreements; using personal data and/or information of consumers who have terminated product and/or service agreements; using personal data and/or information of prospective consumers whose product and/or service applications have been rejected by the PUJK; and/or using personal data and/or information of prospective consumers who withdraw their product and/or service applications.

Bank Indonesia Regulation Number 7/6/PBI/2005 also regulates the transparency of bank product information and the use of customer personal data, as stipulated in Article 2. Banks are required to implement transparency of information regarding bank products and the use of customer personal data. In implementing transparency of information regarding Bank Products and the use of Customer Personal Data as referred to in paragraph (1), the Bank is required to establish policies and have written procedures which include: transparency of information regarding Bank Products; transparency of the use of Customer Personal Data; and the policies and procedures as referred to in paragraph (2) must be implemented in all Bank Offices and Article 3, namely the Bank's Board of Directors is responsible for implementing policies and procedures for transparency of information regarding Bank Products and the use of Customer Personal Data as referred to in Article 2.

Sanctions for violations of personal data protection provisions are also regulated in these six regulations. Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998, Law Number 27 of 2022, Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions, Financial Services Authority Regulation (POJK) Number 6/POJK.07/2022 concerning Personal Data Protection, and Bank Indonesia Regulation Number 7/6/PBI/2005 concerning transparency of bank product information and the use of customer personal data stipulate sanctions that can be applied to banking institutions that violate customer data protection provisions. These sanctions include fines, temporary or permanent closure of the institution's operations, and other legal actions. The implementation of sanctions aims to encourage compliance with applicable regulations, protect customers from the risk of misuse of customer data, and ensure that banking institutions implement customer data protection responsibly.

3.2. Legal remedies customers must take if their data is not protected in internet banking

Equations, theorems, and proofs must be cited in the main text. For example, the author could write the sentence: “Eq. (1) is used to calculate blablabla". This is example 1 of an equation:

4. Results and Discussion

Resolving issues that arise when customer data is not protected is a crucial issue in the modern financial world, especially with the increasing amount of personal data being managed in internet banking systems. Customer data leaks not only have the potential to result in financial losses but can also damage the reputation of financial institutions and threaten

individual privacy. Therefore, it is important to understand the legal remedies customers must take if their data is not protected in internet banking.

The initial effort that must be made by the customer to the bank is to submit a complaint in accordance with Bank Indonesia Regulation Number 10/10/PBI/2008 concerning amendments to Bank Indonesia Regulation Number 7/7/PBI/2005 concerning the Settlement of Customer Complaints. In the problem of internet banking services, the customer has filed a complaint to the bank for a loss that occurred without any fault on the part of the customer. The customer complaint mechanism is regulated in Bank Indonesia Regulation Number 10/10/PBI/2008 concerning the settlement of customer complaints provided by Bank Indonesia, namely:

1. **How to submit a complaint to the bank:**
   - **a. Verbally**: by telephone, including through the bank's 24-hour call center, or by visiting the nearest bank branch.
   - **b. In writing**: by submitting an official letter addressed to the bank by hand delivery, fax, email, or the bank's website. Written complaints must be accompanied by photocopies of identification and other supporting documents, such as proof of deposit or withdrawal, proof of transfer, bank statements, and/or other documents related to the transaction or complaint being submitted.
   - **c. Customer Representative**: Submit photocopies of the customer's and the customer's representative's identification, and a power of attorney from the customer to the customer's representative stating that the customer authorizes the complaint to be submitted.
2. **Receipt of Complaints by the Bank**: The Bank accepts every complaint submitted by customers and/or customer representatives, both verbally and in writing. The bank provides an explanation regarding the policies and procedures for resolving complaints when customers and/or customer representatives submit complaints. The bank provides a receipt. If the complaint is submitted in writing, all bank offices can receive customer complaints.

Then customers can make complaints to the Financial Services Authority according to Financial Services Authority Regulation Number 1/POJK.07/2013 Article 40 paragraph (1), paragraph (2), paragraph (3), namely: Article 40 paragraph (1) namely consumers can submit complaints that indicate disputes between financial services business actors and consumers to the Financial Services Authority. Paragraph (2) states that consumers and/or the public can submit complaints that indicate violations of the provisions of laws and regulations in the financial services sector to the Financial Services Authority. Paragraph (3) states that complaints as referred to in paragraph (1) and paragraph (2) are submitted to the Financial Services Authority, in this case the Member of the Board of Commissioners in charge of consumer education and protection. Customers can submit complaints about customer data leaks to the official OJK service link, namely www.konsumen.ojk.go.id

If a customer's complaint is not properly addressed or resolved, the customer can sue the bank in court on the following grounds: an unlawful act (Article 1365 of the Civil Code) if the bank is negligent in maintaining system security and breach of contract (breach of promise) if the bank promises to maintain data confidentiality in the service agreement. Customers can sue the court for both material and immaterial damages. The following are various legal bases that customers can use to claim liability from the bank for customer data leaks:

1. Claims for bank liability for customer data leaks as stipulated in Law Number 10 of 1998, as outlined in Article 47 paragraph 2.
2. Claims for bank liability for customer data leaks as stipulated in Law Number 27 of 2022.
3. Claims for bank liability for customer data leaks as stipulated in Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions.
4. Demands for accountability by banks for customer data leaks as stipulated in Financial Services Authority Regulation (POJK) Number 6/POJK.07/202
5. Demands for accountability by banks for customer data leaks as stipulated in Bank Indonesia Regulation Number 7/6/PBI/2005.

Based on OJK Regulation No. 61/POJK.07/2020, customers can also resolve disputes through an OJK-approved Alternative Dispute Resolution Institution. This route is faster, less costly, and suitable for cases involving less complex losses.

Banks transitioning to digital platforms must ensure they are technologically and resource-wise ready to handle such technology. Customer data, which is highly vulnerable to unauthorized use, must be protected from misuse. In the event of a loss due to a data breach, the bank's liability must be determined through a thorough investigation to determine whether the loss was caused by the fault of the bank, the customer, or a third party.

Unprotected customer data through internet banking applications is caused by social engineering scams, such as phishing, where customers may unknowingly provide their personal information to fraudsters. These scams typically involve links or messages that appear legitimate but are intended to steal sensitive information. If customers provide personal information necessary to commit a crime, they may be liable for the losses. However, customers have the right to seek redress from the bank, and this process can be pursued through the courts or out-of-court.

By adhering to these principles of fairness and complying with applicable regulations, issues of unprotected customer data and misuse of customer data can be resolved in a fair and equitable manner, minimizing the negative impact on both customers and financial institutions. An effective and efficient process for resolving disputes will help maintain public trust in financial institutions and ensure the future protection of customers' personal data.

4. Conclusions

This research shows that legal protection of customer data in internet banking systems in Indonesia has made significant progress following the enactment of various laws and regulations, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998, Law Number 27 of 2022, and Law Number 19 of 2016 concerning Electronic Information and Transactions. These regulations establish important principles such as clarity, certainty, transparency, and data security, while granting customers greater access and control rights.

Banking institutions are required to comply with existing regulations and impose strict sanctions for violations. The role of the Financial Services Authority (OJK) is crucial in oversight and law enforcement to maintain customer trust.

Resolving customer data disputes must begin with an assessment of losses, which can be done through a complaint to the bank or the OJK. If the complaint is not addressed, the customer can sue the bank for unlawful acts or breach of contract. The principles of legal justice, transparency, and protection of human rights must be prioritized in every resolution process.

By implementing these regulations and principles, it is hoped that negative impacts on customers can be minimized, and public trust in financial institutions can be maintained.

References

Asril Sitompul. 2001. Internet Law (An Introduction to Legal Issues in Cyberspace). Bandung: PT Citra Aditya BaktI

Bambang, Sunggono. 2013. Legal Research Methods. Jakarta: Raja Grafindo Persada

Bank Indonesia Regulation Number 10/10/PBI/2008 concerning amendments to Bank Indonesia Regulation Number 7/7/PBI/2005 concerning Settlement of Customer Complaints

Bank Indonesia Regulation Number 7/6/PBI/2005

Burhan, Bungin. 2007. Qualitative Research Data Analysis. Jakarta: Raja Grafindo Persada

D. Wardani, 2021, Factors Influencing the Use of Internet Banking. Journal of Administrative and Business Perspectives, 2(1), 27-40

Daulay, A. L., Ramadhan, M. C., & Isnaini, I. (2023). Legal Analysis of the Post-Covid-19 Pandemic Impact on the Auction of Bank Collateral Rights at the KPKNL Medan. Journal of Education

Dwi Gustia Ningsih, R. Hamdani Harahap, & Heri Kusmanto. (2023). Analysis of the Integrity of Voter Data Update Officers in Voter Data Collection for the 2020 Medan Mayor and Deputy Mayor Elections in the Medan Polonia District. Perspektif, 12(1), 251–262

Financial Services Authority Regulation No. 61/POJK.07/2020 concerning Alternative Dispute Resolution Institutions in the Financial Services Sector (LAPS SJK)

Financial Services Authority Regulation Number 6/POJK.07/2022

Fitri, K., Hartono, B., & Isnaini, I. (2022). Implementation of Financial Services Authority Circular Letter Number 6 of 2017 concerning the Determination of General Insurance Premiums at PT. Asuransi Jasa Indonesia Syariah Medan. Journal of Education, Humanities, and Social Sciences (JEHSS), 5(2), 1302–1309

Hotang, N. I., Munte, R., & Simanjuntak, S. (2020). The Influence of Third Parties, Operational Costs, Operational Income, and Credit on Financial Performance in the Banking Sector on the Indonesia Stock Exchange. Journal of Education, Humanities and Social Sciences (JEHSS), 3(2), 538–543

M. R. P., Nasution, Siallagan, R., Ginting, F. A., Oktavia, T. W., & Hariandja, S. B. (2020). Implications of Property Rights on Fiduciary Guarantees in Bank Credit (Case Study of PT. BANK SUMUT). Journal of Education, Humanities, and Social Sciences (JEHSS), 3(1), 125–132

Manihuruk, P. J., Eddy, T., & Fauzi, A. (2020). The Role of Banking in Preventing and Eradicating Money Laundering Crimes Committed by Customers. Journal of Education, Humanities and Social Sciences (JEHSS), 3(2), 325–332

Nurmiati & Mahmud, 2022, Marketing Mix: Customer Decisions in Choosing Simpeda Savings at Bank Sulsel. Laa Maisyir Journal of Islamic Economics, 9(2), 1-18

Rusmawan. 2019. Technical Writing of Final Projects and Programming Theses. Jakarta: Elex Media Komputindo

Setiawan, P., Badaruddin, B., & Amin, M. (2022). Analysis of Village Fund Use Based on Permendesa PDTT Number 16 of 2018 concerning Priorities for Village Fund Use in 2019. Perspektif, 11(2), 718–734

Soerjono Soekanto and Sri Mamudi. 2013. Normative Legal Research: A Brief Review, Jakarta: Raja Grafindo Persada

Windianto, W., Ediwarman, E., & Ramadhan, M. C. (2022). Criminal Liability in Ballpress Smuggling Crimes in the Malacca Strait Waters of North Sumatra. Journal of Education, Humanities and Social Sciences (JEHSS), 4(3), 1459–1465.

Yusran Inaini. 2009. Copyright and Its Challenges in the Cyber Space Era. Bogor: Ghalia Indonesia