# Legal Protection of Customer's Personal Data in Internet Banking Services

**Vivian and Abdul Rasyid [a]**
Business Law Program, Law Department, Faculty of Humanities, Bina Nusantara University, Jakarta, Indonesia 11480
[a)] Corresponding author: arasyid@binus.edu

## Abstract

This study aims to determine the legal protection of customer personal data in internet banking services and what customers can take legal remedies if their data is not protected. Customer data in this service needs to be considered because it involves a person's privacy data and must be provided to the Bank to carry out transactions. The research method used is normative legal research by examining legal principles and systematic law with qualitative data followed by a conceptual approach and legislation. The result of this research is that there are two forms of the legal protection of customer data in internet banking services, namely preventive legal protection with a self-regulation approach from the internal legal rules of bank administrators and a government regulation approach in Law Number 10 of 1998 concerning Banking and Law Number 8 of 1999 concerning Consumer Protection. Second, repressive legal protection is the responsibility of the Bank in the form of handling customer complaints to compensation for losses to customers as regulated in Bank Regulation No. 10/10/PBI/2008 concerning Settlement of Customer Complaints, Bank Indonesia Regulation No. 10/1/PBI/2008 concerning Banking Mediation, and Law Number 19 of 2016 concerning Electronic Information and Transactions has regulated the protection of personal data of customers who use Internet Banking. Efforts that customers can make if personal data in internet banking services are not protected can make customer complaints and mediation. If there is no agreement, the customer can take legal remedies consisting of civil legal remedies, criminal legal remedies, and administrative, legal remedies.

## Keywords
Legal Protection, Personal Data, Internet Banking, Customer, Regulation

## 1. Introduction
Technological developments have had a major impact, especially in the banking sector, with the innovation of electronic banking service products, one of which is Internet banking. Internet banking is different from conventional banking; on internet banking, the invisible process raises many questions about legal arrangements for customers' personal data. (Tacino, 2013)

In banking law number 10 of 1998, the personal data held by the customer becomes secretive the bank must protect that. Just like humans in general, which is not inputted from the perfect word, resulting in the bank not being able to provide maximum protection in safeguarding the personal data of its customers, this will give rise to the misuse of customer personal data by people who do not have authority over the right to the data which is then used for personal, commercial needs or other interests that can harm customers. (Sarapy, 2013) Thus, there are two problems formulated in this research: (1) How is the legal protection of customers' personal data in internet banking services? And (2) What efforts can be made by the customer if the customer's personal data in internet banking services are not protected?

### 1.1 Objectives
The purpose of this research is to find out the form of the legal protection of customer's data in internet banking services, as well as what customers can make efforts if their data is not protected or data leaks due to negligence or by a third party so that it can result in losses. Therefore, this research has several limitations, such as the research being conducted on regulations governing banking and regulations governing Internet Banking Services. Furthermore, the research is conducted on regulations governing legal protection in the form of regulation of customer data.

# 2. Literature Review

## 2.1 Legal Protection

Legal protection is the protection of dignity and worth and the recognition of the rights possessed by legal subjects based on legal provisions to protect against acts that are not following the rule of law. This effort is carried out by limiting specific interests and giving measurable power to others to balance the position of interests in social society. (Hadjon, 1997)

In legal protection, there is a legal relationship that contains the rights and obligations of one party dealing with the rights and obligations of the other party. The legal relationship is reflected in the rights and obligations granted and guaranteed by law. Rights and obligations arise because of events; according to van Apeldoorn, "a legal event is an event that by law creates or eliminates rights. Theoretically, legal protection is one factor that shows the function of the law, which is to protect people who associate in the applicable legal area. This enforcement must be determined and enforced by the government as the maker and implementer of the law to maintain the dignity and worth of a human being. (Soeroso, 2006)

## 2.2 Internet Banking

Internet Banking shall mean one of the Bank services that enable customers to obtain information, communicate and execute banking transactions through the Internet network, not only banks that provide banking services through the Internet; thus, but the establishment of Only Banks Internet shall also not be allowed. Thus, internet banking activity must comply with applicable laws and banking laws. This activity uses the internet network as an intermediary or liaison between the customer and the bank without going to the bank office. Customers can use desktop computers, laptops, tablets, or smartphones connected to the internet network as a liaison between the customer's device and the bank system. (Nelson, 2015)

## 2.3 Personal Data

Article 1 paragraph (6) Regulation of the Minister of Communication and Information Technology Number 20 of 2016 concerning Personal Data Protection explains that personal data is stored, maintained, and kept proper and confidential. According to article 1 paragraph (1) Bank, Indonesia Regulation Number 7/6/PBI/2005 explains Customer personal data, namely the identity commonly provided by the customer to the bank in the context of conducting financial transactions with the bank, which includes personal consumer data and/or information that must be kept confidential. The relationship between the customer and the bank is based on the principles of trust and confidentiality. One of the things that must be kept confidential by the bank is the customer's personal information or data in internet banking services. Therefore, personal data must be protected because personal data is part of Human Rights (HAM) and has become a mandate conveyed by the constitution of the Republic of Indonesia and the 1945 Constitution and submitted in the Universal Declaration of Human Rights. (Novalian, 2021)

# 3. Methods

In this research, the authors use normative legal research methods to answer the problem formulations listed in the previous chapters. Normative legal research is research conducted by examining library materials or library data. Therefore, normative legal research can also be referred to as library legal research.

# 4. Data Collection

## 4.1 Account Opening Steps

Shinhan Bank is a bank originating in South Korea. The vision of bank Shinhan is "To be the Number 1 Bank that Creates a New Future and is Loved by All." The next mission of bank Shinhan is "Building a Better World Through Financial Strength by leveraging the expertise, knowledge and resources of a financial expert and company. We are reducing the excessive pursuit of performance and reinventing customer spirit and social values." This bank is a part of Shinhan Financial Group. In opening an account at Shinhan Bank, customers are given two choices: opening an account online via mobile banking or opening manually through the nearest branch office by filling out the account opening form provided through Customer Service. (Sonia, 2022)

One of the tangible forms of the government and several agencies in Indonesia related to the commitment to maintain the confidentiality of customer data by drafting legislation related to the protection of customer data in the digitalization era, which is reflected in transactions made on the internet or mobile banking, this regulation aims to protect the interests of consumers if their data is not protected when using internet banking services. Legal protection is divided into 2, namely preventive protection and repressive protection. The following will be

described in a Table 1 related to which article regulations indicate preventive and repressive protection. (Azhari, 2021)

| **Shinhan Bank Account Opening Mechanism** | |
|---|---|
| Via Online | Via Manual |
| (a) Download the SOL application on the App Store or Play Store via smartphone.<br>(b) Select the "Open Now" button on the SOL app.<br>(c) Enter email address, mobile phone number and reference code (if any)<br>(d) Upload photo of e-KTP, NPWP (if any) and signature<br>(e) Enter financial data and employment data.<br>(f) Make video calls with Bank Shinhan Indonesia agents.<br>(g) The account opening process is complete and an SMS notification will be sent after the account has been successfully established.<br>(h) Access the SOL application, select the "Open Now" button and create a User ID<br>(i) Login to the SOL application, select the menu "Debit Card Management -> Issuing Debit Card" for the Debit Card request to be sent to the desired address.<br><br>Requirements for opening an online account:<br>1) Have an e-KTP<br>2) Have an active email address and mobile phone number.<br>3) Do not have a previous account at Bank Shinhan Indonesia<br>4) Only for Individual Customers<br>5) For security reasons, all data entered into the application during registration will be deleted at the end of the day. | (a) customers will be given two types of forms, namely the account opening form and the form for mobile banking registration,<br>(b) fill in several fields contained in the form which ends with the customer's signature.<br>(c) For filling according to the type of customer, if it is an individual, an individual account opening form will be given, but if it is a company, a company-specific form will be given.<br>(d) will be asked for several supporting data like:<br>1) Individual Customers:<br>• Indonesian citizens: KTP and NPWP;<br>• Foreigners: Passport, Kitas, or Temporary KTP<br>2) Company Customers:<br>• Identity of the Director/Management of the Company or the authorized person<br>• Deed of Business Establishment<br>• The latest deed of Articles of Association & Management<br>• SIUP, TDP and SKDP<br>• NPWP<br>(e) All data and forms that have been completed will be carried out in the next stage by Customer Service<br>(f) When finished, the customer will be given an ATM card and a passbook as proof that the savings account has been processed.<br>(g) If the customer then wishes to have a mobile banking account, they will be directed to fill out the full mobile banking opening form according to the form.<br>(h) The terms and conditions contained in the Shinhan Bank account opening form have been stated in sufficient detail on the back of the form. |

## 4.2 Legal Protection Regulations on Customer's Personal Data in Internet Banking Services

One of the tangible forms of the government and several agencies in Indonesia related to the commitment to maintain the confidentiality of customer data by drafting legislation related to the protection of customer data in the digitalization era, which is reflected in transactions made on the internet or mobile banking, this regulation aims to protect the interests of consumers if their data is not protected when using internet banking services. Legal protection is divided into 2, namely preventive protection and repressive protection. The following will be described in a Table 2 related to which article regulations indicate preventive and repressive protection. (Azhari, 2021)

Table 2. Legal Protection Regulations on Customer's Personal Data in Internet Banking Services

| Regulation | Legal Protection | |
|---|---|---|
| | Preventive Protection | Repressive Protection |
| Law Number 10 of 1998 concerning Banking | Article 40 :<br>"Banks are obliged to keep information about Depositors and their deposits confidential, except in the cases as referred | Article 47 :<br>(1) "Anyone who, without bringing a written order or permission from the Management of Bank Indonesia as referred to in Article 41, Article 41A, and Article 42, intentionally |

| | | |
|---|---|---|
| | to in Article 41, Article 41A, Article 42, Article 44, and Article 44A." | forces a bank or an Affiliated Party to provide information as referred to in Article 40, is threatened with imprisonment of at least - a minimum of 2 (two) years and a maximum of 4 (four) years and a fine of at least Rp. 10,000,000.00 (ten billion rupiah) and a maximum of Rp. 200,000,000.00 (two hundred billion rupiah)."<br>(2) "Members of the Board of Commissioners, Board of Directors, bank employees or other affiliated parties who intentionally provide information that must be kept confidential according to Article 40, are threatened with imprisonment of at least 2 (two) years and a fine of at least Rp. 4,000,000,000.00 (four billion rupiah) and a maximum of Rp. 8,000,000,000.00 (eight billion rupiah)."<br><br>Article 47 A :<br>"Members of the Board of Commissioners, Board of Directors, or bank employees who intentionally do not provide information that must be fulfilled as referred to in Article 42A and Article 44A, are threatened with imprisonment for a minimum of 2 (two) years and a maximum of 7 (seven) years and a fine a minimum of IDR 4,000,000,000.00 (four billion rupiah) and a maximum of IDR 15,000,000,000.00 (fifteen billion rupiah)." |
| Law Number 19 of 2016 concerning Information and Electronic Transactions | Article 16 :<br>(1) As long as it is not stipulated otherwise by a separate law, each Electronic System Operator is required to operate an Electronic System that meets the following minimum requirements:<br>b. can protect the availability, integrity, authenticity, confidentiality, and accessibility of Electronic Information in the Electronic System Operation.<br><br>Article 26 paragraph (1) :<br>Unless otherwise stipulated by the Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned. | Article 45 paragraph (1) :<br>Everyone who fulfills the elements as referred to in Article 27 paragraph (1), paragraph (2), paragraph (3), or paragraph (4) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 1,000,000. .000,00 (one billion rupiah). |
| Bank Indonesia Regulation 9/15/PBI/2007 Implementation of Risk Management in the Use of Information Technology by Commercial Banks | Article 11 :<br>In developing and procuring Information Technology, the Bank is required to take control measures to produce systems and data that are maintained in confidentiality and integrity and support the achievement of the Bank's objectives. | Article 30 :<br>Banks that do not implement the provisions as stipulated in this Bank Indonesia Regulation and other related implementing provisions may be subject to administrative sanctions as referred to in Article 52 of Act Number 7 of 1992 concerning Banking as amended by Act Number 10 of 1998, among others in the form of:<br>a. written warning;<br>b. a decrease in the level of health in the form of a decrease in the rating of management |

| | | |
|---|---|---|
| | | factors in the assessment of the level of health;<br>c. freezing of certain business activities;<br>d. the inclusion of members of the management in the list does not pass through the fit and proper test mechanism. |
| Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector | Article 25 :<br>The Financial Services Providers are required to maintain the safety of consumer deposits, funds or assets which are under the responsibility of the Financial Services Providers.<br><br>Article 31 :<br>(1) Financial Services Businesses are prohibited in any way from providing data and/or information regarding their Consumers to third parties | Article 45 paragraph (1):<br>PUJK and/or parties that do not comply with the provisions as referred to in Article 25, 31 may be subject to administrative sanctions in the form of:<br>a. written warning.<br>b. fine.<br>c. prohibition as the main party in accordance with POJK regarding reassessment for the main party of the Financial Services Institution.<br>d. restrictions on products and/or services and/or business activities.<br>e. freezing of products and/or services and/or business activities.<br>f. revocation of product and/or service license; and<br>g. revocation of business license. |
| Government Regulation Number 82 of 2012 concerning Electronic System and Transaction Operations | Article 15 :<br>Electronic System Operators are required to:<br>a. maintain the confidentiality, integrity and availability of the Personal Data it manages;<br>b. guarantee that the acquisition, use, and utilization of Personal Data is based on the approval of the owner of the Personal Data, unless otherwise stipulated by laws and regulations; and<br>c. guarantee that the use or disclosure of data is carried out based on the consent of the owner of the Personal Data and in accordance with the objectives submitted to the owner of the Personal Data at the time of data acquisition. | Article 84 :<br>(1) Violation of Article 7 paragraph (1), Article 8 paragraph (1) and paragraph (3), Article 12 paragraph (1) and paragraph (2), Article 13, Article 14 paragraph (1), Article 15 paragraph ( 1), Article 16 paragraph (1), Article 17 paragraph (1), Article 18 paragraph (1), Article 21, Article 22 paragraph (1), Article 27, Article 29, Article 30 paragraph (1), Article 37 paragraph (1), Article 39 paragraph (1), Article 58 paragraph (1) and paragraph (2), Article 59 paragraph (1), and Article 78 paragraph (1) are subject to administrative sanctions.<br>(2) The administrative sanctions as referred to in paragraph (1) may be in the form of: a. written warning; b. administrative fines; c. temporary suspension; and/or d. removed from the list as referred to in Article 5 paragraph (4), Article 37 paragraph (2), Article 62 paragraph (1), and Article 65 paragraph (4). |
| Financial Services Authority Regulation Number 12/Pojk.03/2018 Concerning the Implementation of Digital Banking Services by Commercial Banks | Article 6:<br>Banks are required to apply the principle of controlling customer data and transaction security from Electronic Banking Services on every electronic system used by the Bank. | Article 21 :<br>(1) Banks providing Electronic Banking Services or Digital Banking Services are required to apply the principles of consumer protection as referred to in the provisions of laws and regulations concerning consumer protection in the financial services sector.<br><br>Article 26 :<br>(1) Banks that do not implement as referred to in Article 2 paragraph (2), Article 4, Article 5 paragraph (1), Article 5 paragraph (2), Article 5 paragraph (3), Article 5 paragraph (8), Article 6 , Article 9 paragraph (1), Article 10 paragraph (2), Article 11 paragraph (1), Article 11 paragraph (4), Article 11 paragraph (5), |

| | | |
|---|---|---|
| | | Article 14, Article 15 paragraph (2), Article 15 paragraph ( 4), Article 15 paragraph (5), Article 16 paragraph (1), Article 17 paragraph (1), Article 19 paragraph (1), Article 19 paragraph (2), Article 19 paragraph (4), Article 19 paragraph (9 ), Article 20 paragraph (3), Article 21 paragraph (1), and/or Article 21 paragraph (2), shall be subject to administrative sanctions in the form of:<br>a. written letter.<br>b. a decrease in the soundness level in the form of a downgrade in the rating of governance factors in the Bank's soundness assessment.<br>c. prohibition to publish products or carry out new activities.<br>d. freezing of certain activities; and/or<br>e. members of the board of directors, board of commissioners, and executive officers on the list do not pass the fit and proper test mechanism |

## 5. Result and Discussion

In opening the account, personal data from customers are very confidential, and the bank, as the holder of the data, is obliged to carry out proper storage concerning bank secrecy. Regarding bank secrecy in the rule of law in Indonesia, it has not been regulated in a particular statutory regulation. Regarding the legal basis for bank secrecy, it is included in the Banking Law, especially in Article 40 paragraph (1), which states that "Banks are obliged to keep information about Depositors and their deposits confidential, except in the cases as referred to in Article 41, Article 41A, Article 42, Article 44, and Article 44A." Based on the contents of the article, it can be concluded that the bank, as a business entity that has a business field of financial services to the Indonesian people, then in carrying out its duties and obligations, banks are required to provide guarantees of protection to their customers regarding personal data or other data that relates to the customer's financial condition in such a bank, including those in Shinhan Bank. (Azhari, 2021)

Bank secrecy is essential because, in the service industry, trust is the capital to get good value in the eyes of its consumers. The public will entrust their money to be stored in the bank if the bank also provides guarantees regarding the protection of customer data and other financial data belonging to customers. So it can be said that the principle of bank secrecy is the life or soul of the bank itself, as the theory of legal protection stated by Satjipto Rahardjo, that in an interest owned by the community, it is obligatory to be given legal protection to ensure security and comfort for the community. Likewise, bank secrecy is a tool to protect customers' data so that it does not fall to third parties. (Kusnardi, 1998)

The protection is also related to consumer protection. The Consumer Protection Act, Article 1 paragraph (1) states that: "Consumer protection is all efforts that guarantee legal certainty to provide protection to consumers." Based on the definition of consumer protection, it is also related to the principle of bank secrecy, which in bank secrecy also carries out efforts to provide legal certainty and also protection to customers regarding their data.

Consumer protection related to legal protection regarding bank secrecy in customer personal data through the SOL Indonesia service needs to be considered and known regarding the arrangement, especially for the parties involved, such as the bank and the customer concerned. This is so that the interests of customers regarding their data are protected. The existence of regulation with a self-regulation approach does not become an instrument that can provide complete protection to customers' data. (Miru & Yodo, 2004)

Shinhan Bank, as a bank with many customers, always applies the principles of bank secrecy. This is proven by the management of customer data in SOL Indonesia, including when customers open accounts, related to storing customer data as an effort to maintain bank confidentiality, Bank Shinhan do it in two ways, namely:

1. Storage in Strong Room
   Regarding the physical storage of customer data, the bank provides a particular room only for the customer's data. An anti-fire door protects the room, and the key is only held by one trusted person,

namely the Deputy Branch Manager of Semarang. So when CS or Legal wants to retrieve customer data, they must master the key and, at the same time, collect data. Then, when the customer has paid off and has closed the account, the physical data will be issued in the room and stored in a special warehouse for the customer who is paid off or is no longer a customer, which the same person also holds.

2. System storage
   In addition to physical storage, customer data storage is also carried out by banks in the form of input to the bank system called the Aither system. In this system, data from each customer is input one by one. This is also related to the use of SOL Indonesia, where customer data in SOL Indonesia will automatically be entered into the bank's system. If the customer is no longer a part of Shinhan Bank, the relevant employee, such as the CS department, will delete the data systemically.

Based on this description, Shinhan Bank has maintained bank confidentiality with customers' data. The process of storing customer data as an effort to maintain bank secrecy has turned out to be following what is regulated by the OJK, one of which is stated in Article 21, paragraph (1) and paragraph (3) of the Financial Services Authority Regulation Number 12/POJK.03/2018 which regulates the organizer of electronic financial transactions, which in this case is the Shinhan Bank Party, is obliged to apply the principle of consumer protection, with the mechanism and procedures for its implementation following the laws and regulations. This means that the storage of customer data is an effort on the part of the bank to protect customer data and has been following its application with the legal basis of the POJK. (Andrika, 2022)

Furthermore, this is also a form of application from the Bank of Article 3 of Ministerial Regulation Number 20 of 2016. The article states that storing data is one form of implementing personal data protection under maintaining bank secrecy. In addition, in an effort to implement the principle of bank secrecy related to customer personal data, Shinhan Bank is to conduct an internal audit system and an audit by the OJK. In this case, the auditors will conduct a thorough examination every year regarding the completeness of customer data when opening an account or opening SOL Indonesia and to ensure that the depository can maintain bank secrecy.

Based on some of these descriptions, an opinion can be given that, in general, the bank's efforts to protect bank secrecy concerning customers' data can be made in two types of ways, namely:

(1) Self-regulation
   Regarding maintaining bank secrecy, each bank has its policy to make a special rule to underlie the bank's efforts to protect customer personal data, as has been done by Shinhan Bank, which has its regulations that are adapted to the circumstances of each bank.
(2) Government regulation
   Regarding the efforts to protect customers' data related to bank secrecy, the relevant government can also do so. Regarding this effort, the government provides strict legal rules that regulate bank secrecy. However, unfortunately, several regulations have emerged in Indonesia that do not specifically regulate bank secrecy. Most existing regulations only regulate customer or personal consumer data, which still has something to do with bank secrecy because personal data is part of bank secrecy.

However, the bank's efforts to keep bank secrets from third parties do not mean that it is rigid, meaning that it cannot be fully disclosed to third parties. There are several exceptions to the permission of a bank secret to being disclosed to a third party. This is as regulated in Article 41, Article 41 A paragraph (1), Article 42 paragraph (1), Article 44 paragraph (1), and Article 44 A paragraph (1). Where in each of these articles, it is stated that bank secrecy regarding customer data may be disclosed to third parties for the following circumstances:

a) Related to the interest of taxation.
   Bank secrecy can be waived to find out the financial condition of a person who is in trouble with taxes and is a bank customer. The importance of disclosing bank secrecy is one form of fulfillment of the public interest because related to tax issues; of course, it also intersects with the interests of the people and the Indonesian state.
b) Related to the interests of the problem of receivables and auctions.
   Regarding this matter, the principle of bank secrecy can be disclosed to third parties about efforts to resolve receivables and auction problems with the bank. Once again, applying the principle of public interest will provide exceptions related to bank secrecy.
c) Related to the judiciary for criminal acts;
   If the customer in question is proven to have committed a criminal act to disclose his actions, a sweep is carried out related to the customer's deposit funds in the bank. This is also related to if the customer is indicated to have committed a criminal act of corruption, embezzlement, and so on, which are often

closely related to money laundering. Therefore, it is necessary to disclose bank secrecy regarding the number of deposits in the bank.

d) For exchanging information between banks.
Regarding this matter, it is normal and natural to occur in the banking world where each bank will exchange information if an emergency problem must be resolved.

e) At the request of the customer concerned
Regarding the customer's application, it must be attached to the application letter made by the customer.

Regarding the disclosure of bank secrets, it is supported by several other regulations, such as Article 31 of the Financial Services Authority Regulation Number 1/POJK.07/2013, which in that article is also allowed to open of bank secrets for reasons required by laws and regulations. (Djoni, 2010)

Shinhan Bank has tried to provide legal protection for bank customers as consumers, which is an essential aspect of the sustainability of the bank's business. This is evidenced by the existence of several preventive legal protections carried out by Shinhan Bank, which are in line with the laws and regulations, namely the Banking Law, Consumer Protection Law, ITE Law, and OJK Regulations. In addition, to protect consumers, repressive protection is also imposed. This is also regulated in POJK Number 1/POJK.07/2013 in Article 29, which states, "Financial Service Business Actors are obliged to be responsible for Consumer losses arising from errors and/or negligence, management, employees of Financial Services Business Actors and/or third parties who work for the interests of the Financial Services Providers."

Regarding the repressive steps taken by the bank concerning a dispute between the bank and the customer relating to the confidentiality of customer data, the settlement process can be carried out as stated in Article 38 of the ITE Law, namely:

a. It is allowed to file a lawsuit against a business actor domiciled as an electronic transaction operator;
b. A lawsuit can also be made on a representative basis if many parties are harmed.

Based on the series of descriptions above, it can be concluded that the consumer in the banking sector has legal protection, both preventive and repressive protection. The provision of legal protection is a fulfillment of the dignity of the fulfillment of human rights owned by the parties, especially consumers. (Zulham, 2013)

In a legal relationship between a bank and a customer, several principles must be considered in building a good relationship between the bank and the customer. These principles are as follows:

(a) Principle of Trust
In banking activities, as the basis for the relationship between a bank and its customers, it is based on a relationship of trust. To build trust with customers, the bank needs to do several ways, such as:
1. Provide true information to customers.
2. Provide services with good quality.
3. Has various facilities that support customer needs.
4. As well as maintaining the confidentiality of the identity or personal data of the customer so that it is not misused by parties outside the bank.

(b) Principle of Confidentiality
Banks, in carrying out their duties, have an obligation to keep secrets regarding everything related to customers, including the customer's identity or the number of deposits in the bank. So regarding the principle of bank secrecy, it is hoped that banks in managing customer data must be cautious so that because of their negligence, parties are harmed.

(c) Precautionary Principle
The principle of prudence is one of the principles or principles that banks must own in carrying out their duties and obligations. Regarding the prudence that the bank must carry out, it is not only limited to credit problems but also customer deposits. Therefore, the bank must be careful in managing customer deposits, including personal data from the customer concerned.

The three principles mentioned above are closely related to the right to privacy, one of the rights the bank must fulfill as a business actor. Article 4 of the Consumer Protection Law also mentions the privacy rights of consumers or customers, which must be protected and accounted for by business actors if these rights are not fulfilled. (Hermansyah, 2007)

If, in the end, there is a violation in which the customer's data is leaked, then the customer will take various legal remedies aimed at the bank as the person responsible for the leakage of the customer's data. Regarding the leakage

of customer personal data to third parties due to statutory orders, this is legal and legal following legal provisions and needs to be done. However, it is different if the bank secret is leaked illegally or as a result of the bank's negligence. So this, of course, will give losses to customers. Because the data is leaked, and if it reaches irresponsible hands, it will undoubtedly provide several losses for the customer whose personal data is spread freely.

Therefore, customers who feel aggrieved can take many legal remedies to demand accountability from the bank. The initial step that the aggrieved customer can take is to make a complaint under the rules stipulated by PBI Regulation No.7/7/PBI/2005 regarding the settlement of customer complaints which can be done in two ways, namely verbally by directly coming to the bank or call the call center, the second in writing sends an email to the bank concerned.

In the case of making a complaint using the methods mentioned above, the customer concerned must attach:

1. Photocopy of identity.
2. Proof of deposit or withdrawal.
3. Proof of savings book or deposit slip.
4. Proof of checking account.
5. Or other data that can support the complaint.

The bank that receives the complaint from the customer who feels aggrieved is obligated to accept the complaint from the customer both verbally and in writing; then, the bank is obliged to explain the chronology, and the problem of the incident parties (customer and bank) can mediate. (Bernadette, 2022)

The process for implementing banking mediation is also regulated in Bank Indonesia Regulation No. 8/5/PBI/2006 jo. Bank Indonesia Regulation No. 10/10/PBI/2008 concerning Banking Mediation. Consumer complaints by financial services authorities according to Financial Services Authority Regulation No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector in Article 40 paragraph (1), paragraph (2), paragraph (3). However, if this problem shows that there is a criminal or civil case, then the resolution process will go through criminal or civil lines; following the written rules, all bank offices can receive customer complaints, which can be done through mediation. (Raditio, 2014)

Mediation is a dispute resolution process in the form of negotiations to solve problems through a neutral and impartial outside party who will work with the disputing parties to help find a solution in resolving the dispute to the satisfaction of both parties. If there is no agreement between the two parties, then legal action can be taken, namely the litigation process in the District Court. Legal remedies that can be taken consist of civil, criminal, and administrative legal remedies.

Thus, the dispute resolution process through the District Court is carried out as in filing an ordinary civil dispute lawsuit by filing a claim for compensation, whether based on an unlawful act based on an element of error. The consequence of the choice of dispute resolution in the District Court is the length of time for settlement of cases, and the decisions handed down often reflect the absence of a unified work or unified legal opinion between the District Court, High Court, and the Supreme Court. (Febby, 2022)

## 6. Conclusion

Based on the research conducted by the author, the following conclusions can be drawn:

1. There are two forms of legal protection for customer data in internet banking services, namely preventive legal protection and repressive legal protection. Preventive legal protection is an effort made by the government to protect consumers or customers in general with a self-regulation approach from the internal law of the Internet Banking service provider itself and the government regulation approach in Article 29 paragraph (4) and Article 40 paragraph (1) and (2) Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking and Article 4 of Law Number 8 of 1999 concerning Consumer Protection. Repressive legal protection is an effort taken if a problem occurs that has the potential to harm customers. The problem occurred because of the leakage of unprotected customer data. So the efforts that customers can make if a data leak causes losses are the responsibility of the digital banking service provider, namely the bank itself. The accountability of the bank can be in the form of handling customer complaints to compensation for losses to customers as regulated in Bank Indonesia Regulation (PBI) Number 7/7/PBI/2005 in conjunction with Bank Indonesia Regulation No. 10/10/PBI/2008 concerning Settlement of Customer Complaints, Bank Indonesia Regulation No.

8/5/PBI/2006 in conjunction with PBI No. 10/1/PBI/2008 concerning Banking Mediation, and Article 21 paragraph (2)A,(2)B, (2)C, (3), (4), (5) and Article 26 paragraph (1) and ( 2) Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions has regulated the protection of personal data of customers who use Internet Banking.

2. Customers can make efforts if personal data in internet banking services are not protected, meaning that it causes harm to customers. They can make customer complaints and mediation first. If there is no agreement between both parties (the customer and the bank), the customer can take legal action, namely the litigation process, in the District Court. Legal remedies that can be taken consist of civil legal remedies, criminal legal remedies, and administrative, legal remedies.

## References

Azhari, A., "*Legal Review of Consumer Law Protection on Personal Data on Digital Platfom*." *Journal Private Law Review*. Vol. 2 No.1, pp. 96-98, 2021.

Febby, N M et al., "*Perlindungan Hukum Bagi Nasabah Bank Yang Dirugikan Dalam Transaksi Layanan E-Banking*." *Jurnal Interpretasi* Hukum. Vol. 3 No.1, pp. 49-50, 2022.

Ghazali, D S. & Usman, R., *Hukum Perbankan*. Cet. 2. Jakarta: Sinar Grafika, 2010.

Hadjon, P. M., *Perlindungan Bagi Rakyat Indonesia "sebuah studi tentang prinsip-prinsipnya, penanganannya oleh pengadilan dalam lingkunganperadilan umum dan pembentukan peradilan administrasi negara"*. Surabaya: Bina Ilmu, 1997.

Ibrahim, H, & Kusnardi, M., *Hukum Tata Negara Indonesia*. Jakarta: Sinar Bakti, 1998.

Bolon, N. T at all. *Bijak Ber-eBanking*. Jakarta: OJK, 2015.

Novaliana, F., "Tanggung Jawab Perbankan Terhadap Pembobolan Rekening Nasabah Melalui Internet Banking." Skripsi ilmu hukum pada Fakultas Syariah Dan Hukum Uin Syarif Hidayatullah Jakarta, 2021.

Raditio, R. *Aspek Hukum Transaksi Elektronik*. Jakarta: Graha Ilmu, 2014.

Republik Indonesia. Undang-Undang Nomor 10 Tahun 1998 perubahan atas Undang-Undang Nomor 7 Tahun 1992 tentang Perbankan

Republik Indonesia. Undang–Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Republik Indonesia. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi dan Transaksi Elektronik.

Republik Indonesia. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Republik Indonesia. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Republik Indonesia. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi Dalam Sistem Elektronik

Republik Indonesia. Peraturan Bank Indonesia Nomor 7/6/PBI/2005 tentang Transparansi Informasi Produk Bank dan Penggunaan Data Nasabah

Republik Indonesia. Peraturan Bank Indonesia Nomor 7/7/PBI/2005 tentang Penyelesaian Pengaduan Nasabah

Republik Indonesia. Peraturan Bank Indonesia Nomor 22/20/PBI/2020 tentang Perlindungan Konsumen Bank Indonesia

Republik Indonesia. Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan

Republik Indonesia. Peraturan Otoritas. Jasa Keuangan Nomor 1/POJK.07/2013 tentang Penyelesaian Pengaduan Nasabah

Republik Indonesia. Peraturan Otoritas Jasa Keuangan Nomor 12/POJK.03/2018 tentang Penyelenggaraan Layanan Perbankan Digital oleh Bank Umum

Sarapi, N., "*Usaha Bank Menjaga Rahasia Bank Dalam Rangka Perlindungan Terhadap Nasabah*." *Lex et Societatis*. Vol. 1 No. 4, pp. 57-65, 2013.

Soeroso, R. *Pengantar Ilmu* Hukum. Jakarta: Sinar Grafika, 2006.

Tacino, M. J., "*Perlindungan Hukum Terhadap Hak Pribadi Seseorang Di Media Sosial Menurut Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik*." Jurnal Ilmiah Ilmu Hukum. Vol. 26 No. 2, pp. 174-184, 2020..

Yodo, S, & Miru, A., *Hukum Perlindungan Konsumen*. Jakarta: Raja Grafindo Persada, 2004.

Zulham, *Hukum Perlindungan Konsumen*. Jakarta: Kencana Prenada Media, 2013.

## Biographies

Vivian is a student majoring in business law at Bina Nusantara University.

Abdul Rasyid is a lecturer and expert on sharia business law. he is a permanent lecturer of the business law department of Bina Nusantara University. Abdul rasyid obtained his bachelor's degree in Islamic law from the sharia faculty of IAIN Imam Bonjol Padang, then continued his master's and doctoral education at Ahmad Ibrahim Kulliayah of Law, International Islamic University Malaysia with expertise in sharia business law. He conducted

various research in the field of sharia business law. He has also published several books on the development of sharia law in Indonesia.