



Consumer Protection Of Internet Banking Users Service In Indonesia In Review Of Law Number 8 Of 1999 Concerning Consumer Protection

Wiwik Sri Widiarty*

*Magister Hukum Universitas Kristen Indonesia, Email: wiwik.widiarty@gmail.com

***Corresponding Author:** Wiwik Sri Widiarty

*Magister Hukum Universitas Kristen Indonesia, Email: wiwik.widiarty@gmail.com

Abstract

Digitalization has brought people access to various digital needs. The banking sector is no exception, where at this time it is very common among the public to carry out various transactions and banking activities digitally. One of the services presented by the banking sector in digitalization is the use of internet banking. Internet banking is a banking product that deserves appreciation because it has a significant impact on people's lives. The presence of internet banking has facilitated various banking activities and public transactions. However, there are concerns about various dangerous activities that have the potential to arise from the use of internet banking. The purpose of this study is to review Law Number 8 of 1999 which regulates consumer protection and its relation to consumer protection in the banking sector by using internet banking. The method used is normative juridical. The results of the research show that basically the government has attempted to protect consumers through the existence of Law Number 8 of 1999. In the banking sector itself this has been strengthened by various regulations issued by Bank Indonesia and the Financial Services Authority. Both of these agencies are agencies that have responsibility for the administration of the banking sector. However, several banking sectors still have loopholes for committing fraud and do not fully comply with the regulations that have been set.

Key word: Consumer Protection: Banking; Internet Banking

Introduction

Today's new era in trade corresponds to the advancement of information technology. Because of technological advancements, world trade is no longer restricted to territorial boundaries; people can still conduct business transactions without even meeting in person. The rapid advancement of information technology has had a wide-ranging impact on human life. In the future, information technology will be used to organize business (e-business) and government (e-government) activities that were previously carried out in the physical world. This method was chosen because it is believed that using information technology across regional borders will increase the efficiency and speed with which businesses and government administration operate.

In Indonesia, the same is true. The pattern that leads to the use of information technology now refers to all economic activity. Whether in terms of goods or services. With the advancement of information technology, Business transactions increasingly imply that transactions between banks and between banks and their customers are conducted electronically, resulting in the development of electronic banking.¹

As a result of advancements in electronic banking, internet banking activities have become a part of daily life. According to data, approximately forty banks in Indonesia provide internet banking services. The scope of services also varies, From sites that only provide bank information to those that can provide simple transaction services, to sites that can fully serve all types of transactions, such as fund transfers, bill payments, subscriptions to specific products, and even stock purchase and sale transactions, there are options for everyone.

¹ Asuan. 2019. Transaction Banking Through Internet Banking. *Solution* 17(3). 317-335

Customers no longer need to return to the bank or even sacrifice time and energy to queue and wait for an extended period of time. Many online networks now offer banking services through Automated Teller Machine (ATM) transactions or mobile banking phones, which are transactions made via cellular or landline telephones, allowing internet banking services to be provided.

The development of internet banking in Indonesia started from Bank Papan Sejahtera as a pioneer at the end of 1997, this year also the banking business was very mushrooming, due to the many conveniences in establishing or forming a bank. Because the risk is not too high and with low capitalization allows entrepreneurs to establish banks. But then in this day and age, the internet banking program has been run very easily. At that time, it also turned out that Bank Papan could provide new breakthroughs by providing services through the internet which at that time was still not as popular as it is now. However, due to insufficient capital, many banks were liquidated, one of which was a Board Bank so that the internet banking program could be said to have failed in its development. But furthermore, at this time, the internet banking program has been run again by several banks in Indonesia. Among them is Bank Lippo which has fulfilled internet banking since April 1998, then recognized by Bank International Indonesia (BII), in May 1998, Bank Permata which has started from Bank Bali in the month of August 2000, as well as BCA in the same month and year as Bank Permata. For example, BCA, which is famous for its extensive ATM network, in addition to having a website about company profiles, also has a menu for making transactions for purchase of goods, payments, transfer of funds, balance information or other transactions.

This demonstrates that Indonesia's banking industry is beginning to demonstrate quite rapid capabilities. However, The issue is that the situation is not being followed, with the renewal of banking law, which is critical to the banking industry's healthy development. As we all know, the laws governing banking are governed by Law Number 10 of 1998 Concerning Banking, which amends Law Number 7 of 1992 Concerning Banking. This Law, however, does not regulate the specific relationship between banks and customers, particularly those who hold rights and obligations in relation to agreements made between the two parties in the use of internet banking services. There is currently no definite guideline for banks to use as a reference regarding the content or clauses that can or cannot be included in a standard contract for the use of the banking internet service.

According to article 1 paragraph 10 of Law No. 8 of 1999 on Consumer Protection, " any rules, conditions, and terms that have been prepared and determined unilaterally by business actors as stated in a legally binding document and/or agreement that consumers must follow². Furthermore, as a bank customer, His rights must be safeguarded. In general, the model of agreement used in banking practices is a standard agreement or a standard agreement whose clauses have already been prepared in this manner by the bank. As a result, the customer has only two options: accept or reject the clause in its entirety. This is solely based on the contract freedom principle. If the agreement is solely based on the principle of contract freedom, each party will seek dominance over the other, as is customary.

By Karena, who makes the standard contract only for one party, everything concerning the contract's content prioritizes the interests and security of the party who makes it. This is a financial institution. Of course, the bank will use the maximization concept in determining the standard contract's content; the bank will also avoid any risks that may arise. Limiting liability to the date of its inception is one way to avoid risks with this standard contract, which is known as an exemption clause or Exoneratie clause. If the bank has protected itself against any risks that may arise as a result of the contract's validity, the customer who uses the service will bear all risks. This is obviously unfair because the bank is only interested in profits and not in the risk of loss. This is where the injustice of using inclusion in the standard clause as a battery bat of the principle of contract freedom, which in Indonesia is not limited by the rule of law and is supervised by the government, comes into play. Because the law has lost its function if it is unable to uphold justice for its weak citizens.

² Invite-Invite Number 8 Year 1999 About Protection User. Secretariat Country. Jakarta

Problem Formulation

- 1) How is the regulation of internet banking products service in relation to consumer protection in Indonesia?
- 2) How is the government paying for protection for internet banking consumers in Indonesia?

Theoretical Framework

Every citizen has the right to the legal protection that the government is obligated to provide. Consumer protection is one of the safeguards that must be provided. This is done so that the public is protected by the state when conducting electronic business transactions. The 1945 Constitution, Article 1 paragraph (3), states that Indonesia is a legal state. This statement means that the state guarantees the legal rights of its citizens by providing legal protection, and legal protection will become a right for all state citizens.

Legal protection, according to Satjipto Raharjo's legal protection theory, is to provide protection for human rights (HAM) that have been violated by others, and that protection is given to the community in order for them to enjoy all of the rights granted by law. Not only can the law provide adaptive and flexible protection, but it can also provide predictive and anticipatory protection. Laws are required for those who are socially, economically, and politically weak to obtain social justice. Consumer protection, according to Article 1 number 1 of the Consumer Protection Law, is any effort that ensures legal certainty in order to provide consumers with a sense of security. Legal protection is the protection afforded to legal subjects under the rule of law, whether preventive (prevention) or repressive (coercion), both written and unwritten, in order to enforce the law.³⁴

Research Methods

The research method used is normative judicial, that is, research with an emphasis on literature studies.⁵ Examining laws and regulations that apply or are applied to a specific legal problem, namely the object of study, which is in the form of laws and regulations and materials Book.⁶ The subject of study is Law No. 8 of 1999 on Consumer Protection and Law No. 7 of 1992 on Banking, as well as reading books and journals-scientific journals on the research topics discussed. The data obtained through qualitative analysis is then used to obtain descriptive information about the object under study.

RESULTS OF THE DISCUSSION

Regulation of Internet Banking Service Users in conjunction with Consumer Protection in Indonesia

Currently, non-cash transactions have a fairly high transaction traffic. One of the reasons for the high traffic of non-cash transactions is the high public activity related to electronic transactions. Electronic transactions are closely related to the use of internet banking. The existence of internet banking allows transactions that can be carried out by customers in *real-time* and can be carried out at any time. The existence of mobile phones has further increased the level of internet banking usage because the ease of transactions has become much greater.

Internet banking is a form of internet utilization by the banking world. Banks must be able to fulfill several things in order to provide adequate internet banking and be able to meet customer needs.⁷ Ease of access provided by financial institutions to customers due to the provision of a *real-time* transaction system and *cross-channel view*. In general, the banking service system using internet banking aims to make various banking activities more effective and efficient.

³ Satjipto Raharjo, *Science Law*, Publisher:PT. Image AdityaBakti, Bandung, 2000.p.54.

⁴ Invite – Invite RI Number 8 Year 1999 About Protection User

⁵ Soekanto, Soerjono & Mamuji, Sri. *Research law Normative, One Review Brief*Jakarta: King Grafindo Persada,2003,p.13.

⁶ *Ibid.*

⁷ Santoso, Agus & Pratiwi, Dyah. 2008. Responsibility Organizing System Electronic Banking deep Activities Transaction Electronic Post Law Number 11 Year 2008 about Information and Transaction Electronic. *Journal Legislation Indonesian* 5(4). 74-88.

The ease of transacting with the existence of internet banking in general is indeed a satisfaction for the public.⁸ However, without realizing it, there are dangers that lurk from the ease of access to various banking transactions carried out by the public. In addition, there are also several potential losses that may be experienced by customers from these online banking activities. For example, transaction errors caused by customer negligence in using the online transaction feature will be entirely the responsibility of the customer. This is different from the conventional transaction model where a customer will always be reconfirmed by a bank officer for all transactions made. Similarly, if there is a disruption to the transaction such as a balance that has been deducted from the sender's account but does not enter the recipient's account.

this time, the security of using internet banking is getting bigger and bigger. This can be seen in several events that have occurred recently among the public. The mode of attack on viruses that have the purpose of hacking mobile banking is increasingly varied. This mode can be found through messages or calls received by the public. Some examples of the mode of hacking funds through *mobile banking* hacking that has recently occurred are as follows:

1. Phone Redirection

In this case, the perpetrator of the hack has transferred various communication activities that should have entered the victim's mobile phone number to enter the number provided by the perpetrator. This has an impact on the perpetrator's level of knowledge of various cellular activities carried out by the victim including various calls and messages that enter the victim's cell phone. So, when the perpetrator tries to hack the victim's data and is required to enter the OTP code, the perpetrator can easily enter the verification code to further do took over the victim's account.

2. Phishing

Phishing is a method done by hackers by tricking victims into visiting certain sites or installing applications⁹ that are used to hack. First, the perpetrator will send a message that interests the victim to open it. This message can be in the form of a message to fill in certain data that brings the victim to open the site provided by the perpetrator and fill in the victim's personal data complete. The message can also be a redirect where the hacker sends a message to the victim. Furthermore, the perpetrator will make calls to the victim under various pretexts such as an error in charging the credit number and so on. This continues by asking the victim to mention the code sent to the victim where the code is actually an OTP code. This message can also be a message with an application extension where when the victim opens the message there will be an application that is automatically installed on the victim's cell phone. The application is an application that has been prepared by the perpetrator to hack the *mobile banking* application installed on the victim's cellphone.

Some other security loopholes related to the use of internet banking are the potential for virus attacks that can be used to intercept, modify, delete, and falsify personal data of *mobile banking* users such as PINs or card number. This security loophole lurks in all banking sectors regardless of the status and level of operations of the organizing bank. Internet banking operations basically have several variations of services. Some of the services provided through transactions in internet banking include features to access balance information, features to open accounts independently, features to make transfers either to fellow user banks or between banks, and the *payment gateway* feature or features that are carried out to make various types of payments.¹⁰ Currently,

⁸ Pangginstead of, Blessing Octopus & Baridwan, Zaki. 2013. Interest Individual Towards Use Internet Banking: Approach Modified Theory of Planned Behavior. *Journal Scientific Student Faculty Economy and Business* 1(2). 1-23

⁹ Fauzadel Muhammad Fahri & Apriani Rani. 2022. Protection Law Towards Customer Top E-Wallets Leakage Data and Loss A number of Funds. *Journal Scientific Science QISTIE Law* 15(2). 224-238.

¹⁰ Lailani, Evi Oki & Regina, Tannia. 2021. Use Mobile Banking As Attempt Streamlining Transaction Electronic Customer on PT. Bank Rakyat Indonesia (Persero) Tbk. *Complexity* 10(01). 24-33

quite a lot of banks are even starting to develop the types of transaction services provided by internet banking users.¹¹

Based on the diversity of types of transactions available, there are several risks that may occur to internet banking users. These risks include:

1. Technology risks

This risk is a risk that arises from the sophistication of the technology system. At this time, almost all community activities including activities related to various banking transactions can be carried out with just one hand. This is indeed considered to increase the value of effectiveness and efficiency, but on the other hand, it will also make it easier for hackers to be able to access all information owned by the public. Therefore, the sophistication of the systems and devices used by the community will have an impact on the level of risk that arises from technological developments.

2. Reputational Risk

Internet banking developed by highly reputable banks is certainly considered further than security threats compared to *internet banking* developed by banks that are considered to have a bad reputation. Internet banking providers are parties who are considered guarantors in the provision of *internet banking* services. The level of operational disruption or security disruption that often occurs in an internet banking service provided by a bank will certainly make customers reluctant to use banking services provided. This can be interpreted to mean that banks that have a good reputation among the public have the potential to be able to maintain customer security quite well and can also provide convenience for customers in using various features provided in the internet banking provided.

3. Third Party Risk

As is well known that almost all banks that provide internet banking services always have a third party as the developer. These third parties' function to provide services in the management of *Internet Service Providers* (ISPs) which are also tasked with maintaining and managing the security of user data. On the one hand, this is considered effective and efficient because by using the services of third parties, the bank can obtain a service provider at the most suitable price with a ceiling owned by the bank. However, on the other hand, this also contains considerable risks because the preparation of consumer data which is confidential banking data can be accessed by other parties. Even if there is an agreement in its implementation, this still creates a security loophole.

4. Legal Risks

Legally, regulations related to the implementation of internet banking and the protection of internet banking user data are still very limited and there are no clearly defined regulations. Therefore, if internet banking users face various problems related to the use of internet banking, this can raise potential problems both in criminal law nor civil.

5. Transaction Risk

The high number of transactions made through internet banking can cause several errors that may occur. Risks for the implementation of such transactions can occur in various product and service services accessed through internet banking. Some of the transaction risks that can arise in internet banking use activities include constraints on the transaction process, constraints on calculating transactions, and the complexity of goods and services transacted.

Due to the emergence of these risks, there are several types of user security developed by internet banking providers.¹² The security model developed aims to provide layers of security in

¹¹ Nasmah. 2020. Increased Interest Customer Melallui Service Internet Banking BRI Edge Lero (Analysis Management Sharia). *Thesis*. Faculty Economy and Business Islam Institute State Islamic Religion (IAIN) Parepare

¹² Herdansyah, Decky. 2012. Security Service Internet Banking deep Transaction Banking. *Iqtishaduna* 1(1). 12-33

various banking activities and the security of customer data. These safeguards generally contain elements of identification, authentication, and authorization. The various forms of security developed include:

1. Digital Certificates

These digital certificates can generally take the form of authentication through public key infrastructure and authority certificates. Digital certificates will generally be provided by the developer, which in this case is a third party. A digital certificate is evidence used to demonstrate the legality and validity of the developed banking system.

2. One Time Password

Onetime passwords can be classified into 2 types, namely in the form of tokens and in the form of cards. *One time password* in the form of a token is used to authenticate data which in general the customer will be asked to enter a security code that will change every time the user will using the service. The one-time *password* card is a security code in the form of a card where there is not always a change in every customer's access to internet banking. This security code in the form of a card can be used in several transactions so that it is easier to hack.

3. Device Restrictions

This security is carried out by limiting the number of devices that can access internet banking. This prevents hacking from happening because internet banking accounts cannot be accessed on multiple devices at once. If there is a new device that attempts to log in, the customer will get a notification so that the customer can be aware of any suspicious activity related to the use of internet banking.

4. Register Method

This method develops newer ways of signing in to the account. No longer using the code sent or typed but customer registration can be done using fingerprint or face authentication. This can be used to avoid using remote controls on the device by looking at the *keyboard* usage history.

5. CAPTCHA code

Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is one of the security methods carried out by warding off automatic attacks on *websites*. In this method, the user will be asked to verify by entering a number of information displayed in the form of images or audio which cannot be solved by the robot or automated systems.

6. Positive Identification

It is one of the security techniques that asks customers to enter information that is confidential and only known by customers personally. This authentication is typically used as double authentication or second-level authentication.

The Government's Efforts to Provide Protection to Internet Banking Consumers in Indonesia

Bank Indonesia, the Central Bank of Indonesia, and the Financial Services Authority, which has the authority to protect public funds, have issued regulations concerning consumer protection, in this case a bank customer. Bank Indonesia issued ¹³ Bank Indonesia issued Regulation Number 22/20/PBI/2020 concerning Bank Indonesia Consumer Protection, while the Financial Services Authority issued Regulation Number 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector. In addition, since about 10 years ago, Bank Indonesia has also issued a number of regulations concerning the implementation of internet banking, including the Bank Indonesia Circular Letter Number 6/18/DPNP, which discusses the Application of Risk Management in Bank Service Activities via the Internet, the Bank Indonesia Regulation Number 7/6/PBI/2005, which concerns the Transparency of Bank Product Information and the

¹³Tarigan, Herdian Beautiful Andreana Beru & Paul, Darminto Hartono. 2019. Protection Law Towards Customer Above Organizing Service Banking Digital. *Journal Indonesian Law Development* 1(3). 294-307

Use of Customer Personal Data, and the Bank Indonesia Regulation Number 7/7/PBI/2005, which concerns Complaint Resolution, the Bank Indonesia Regulation Number 9/15/PBI/2007, which concerns the Application of Risk Management in the Use of Information Technology by Commercial Banks, and the Bank Indonesia Circular Letter No. 9/30/DPNP, which concerns the Use of Information Technology by Commercial Banks. Bank Indonesia Regulation Number: 11/12/PBI/2009 concerning Electronic Money, and Circular Letter Bank Indonesia Number: 11/11/DASP dated 13 April 2009 concerning Electronic Money.

In addition, banks that organize internet banking have several obligations that must be fulfilled due to the use of information technology for financial transactions¹⁴. Some of the main rules related to the implementation of internet banking by banks based on PBI Number 9/15/PBI/2007 are:

1. Every bank providing internet banking services has an obligation to implement effective and efficient risk management in maintaining the security of internet banking activities.
2. The implementation of risk management must be based on the Guidelines for the Application of Risk Management in Bank Service Activities Through the Internet (Internet Banking) and must be poured into the policy procedures and guidelines in writing.
3. The application of risk management contains the main elements consisting of:
 - a. Active supervision of the bank's commissioners and directors consisting of effective supervision on various matters related to activities in internet banking and the board of directors must review Internet Banking Security Control Procedures
 - b. Security control that can be demonstrated in several things such as the implementation of identity authentication testing and customer authority of internet banking users, testing the authenticity of transactions, ensuring the existence of categorization and classification of tasks in the developed internet banking system, ensuring adequate procedures to protect customer data and information on every activity and transaction carried out through internet banking, ensuring the availability of a clear flow of transaction mutation tracing, and must be able to take measures to protect the confidentiality of customer information.
 - c. Have legal risk management and reputational risk consisting of the bank's obligation to ensure that the customer has the right information about the bank's profile along with the legal status owned, before the customer decides to use internet banking. The Bank has an obligation to ensure that the confidentiality of customer data and information has been implemented in accordance with consumer protection provisions in accordance with the region or area of domicile. Banks are required to have emergency planning procedures in place and are also required to develop a handling plan in case of unforeseen problems. Finally, if the bank uses the services of a third party as a developer of internet banking services, the bank must turn off that there are provisions and provisions for procedures supervision that can ensure the security of customer data.

Agreements between parties to internet banking users can also be stipulated in the form of electronic documents. The agreement is a form of agreement from the customer. The agreement can be referred to as a standard agreement. Agreements with standard clauses are written in Law Number 8 of 1999 article 1 point 10. The clauses that have been set out in the agreement are referred to as standard terms. The default clauses are as follows:

- (1) Banks that in this case act as business actors are not permitted to make or include standard clauses in any documents and/or agreements if:
 - a. Declare the transfer of responsibility of business actors;
 - b. Declare that business actors have the right to refuse the return of goods that have been purchased by consumers;
 - c. Stating that business actors have the right to refuse the return of money paid for goods or services that have been purchased by consumers.
 - d. Declare the granting of power from consumers to business actors either directly or indirectly to take all unilateral actions related to goods purchased by consumers installments;
 - e. Regulates the proof of the loss of usefulness of goods or services purchased by consumers;

¹⁴Pahlefi. 2015. Settings Bear Answer the Bank deep Electronic Banking According to Regulation Legislation. *Journal Science Law* 6(2). 75-89.

- f. Providing rights to business actors to reduce the benefits of services or consumer property that are the object of buying and selling services.
- g. Declare the consumer's submission to the tangible regulations as new, additional, continued or continued changes made unilaterally by business actors in the period when consumers utilize the services he purchased;
- h. Stating that the consumer authorizes the business actor to impose dependent rights, liens, or guarantee rights on goods purchased in installments.

(2) Business actors are prohibited from including standard clauses whose location or shape is difficult to see or cannot be read clearly whose disclosure is difficult to understand;

(3) Any standard clause that has been set by the business actor on a document or agreement that meets the provisions as referred to in paragraphs (1) and (2) shall be declared null and void.

Conclusion

The use of internet banking today has a higher traffic due to the higher level of online activity of the public. At this time many people prefer to use internet banking services to carry out various banking transactions because they are considered more efficient and more in accordance with the needs of society at this time. However, in addition to the efficiency and various conveniences offered, there are several potential risks that can occur related to the use of internet banking. These security threats can be in the form of security threats to customer personal data and also security threats to all transaction activities carried out by customers. Therefore, there are several provisions for the use of internet banking that aim to maintain the privacy and security of customer data and transactions such as the use of security codes that must be passed by the customer in every action and activity using internet banking. In addition, the government also has efforts to maintain customer security through several regulations that have been issued by both the executive government, the Bank Indonesia as the central bank or the Financial Services Authority (OJK) which is responsible for customer funds collected in the banking sector.

Bibliography

- Asuan. 2019. Transaksi Perbankan Melalui Internet Banking. *Solusi* 17(3). 317-335
- Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen. Sekretariat Negara. Jakarta
- Undang – Undang Dasar Republik Indonesia Tahun 1945
- Satjipto Raharjo, Ilmu Hukum, Penerbit: PT. Citra AdityaBakti, Bandung, 2000.hlm.54.
- Undang – Undang RI, Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen
- Soekanto, Soerjono & Mamuji, Sri. Penelitian hukum Normatif, Suatu Tinjauan Singkat, Jakarta: Raja Grafindo Persada,2003,hlm.13.
- Santoso, Agus & Pratiwi, Dyah. 2008. Tanggungjawab Penyelenggaraan Sistem Elektronik Perbankan dalam Kegiatan Transaksi Elektronik Pasca Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Jurnal Legislasi Indonesia* 5(4). 74-88.
- Panggalih, Restu Guriting & Baridwan, Zaki. 2013. Minat Individu Terhadap Penggunaan Internet Banking: Pendekatan Modified Theory of Planned Behavior. *Jurnal Ilmiah Mahasiswa Fakultas Ekonomi dan Bisnis* 1(2). 1-23
- Musrifah, Rizqi & Sukananda, Satria. 2018. Analisis Perlindungan Hukum Terhadap Nasabah dalam Transaksi E-Banking di Indonesia. *Jurnal Diversi* 4(1). 98-124
- Fauzadeli, Muhammad Fahri & Apriani, Rani. 2022. Perlindungan Hukum Terhadap Nasabah E-Wallet Atas Kebocoran Data dan Kehilangan Sejumlah Dana. *Jurnal Ilmiah Ilmu Hukum QISTIE* 15(2). 224-238.
- Lailani, Evi Oki & Regina, Tannia. 2021. Penggunaan Mobile Banking Sebagai Upaya Memperlancar Transaksi Elektronik Nasabah pada PT. Bank Rakyat Indonesia (Persero) Tbk. *Kompleksitas* 10(01). 24-33
- Nasmah. 2020. Peningkatan Minat Nasabah Melalui Layanan Internet Banking BRI Ujung Lero (Analisis Manajemen Syariah). Skripsi. Fakultas Ekonomi dan Bisnis Islam Institut Agama Islam Negeri (IAIN) Parepare
- Herdansyah, Decky. 2012. Keamanan Layanan Internet Banking dalam Transaksi Perbankan. *Iqtishaduna* 1(1). 12-33
- Tarigan, Herdian Ayu Andreana Beru & Paulus, Darminto Hartono. 2019. Perlindungan Hukum Terhadap Nasabah Atas Penyelenggaraan Layanan Perbankan Digital. *Jurnal Pembangunan Hukum Indonesia* 1(3). 294-307
- Pahlefi. 2015. Pengaturan Tanggung Jawab Bank dalam Electronic Banking Menurut Peraturan Perundang-Undangan. *Jurnal Ilmu Hukum* 6(2). 75-89.