International Journal of Law
www.lawjournals.org
ISSN: 2455-2194
Received: 21-09-2021, Accepted: 06-10-2021, Published: 22-10-2021
Volume 7, Issue 5, 2021, Page No. 167-172

Consumer legal protection against bank customers from threat of phishing on the use of internet banking

Sri Andrian, Azhari, Teuku Muttaqin Mansur
Master of Law Student, Faculty of Law, Syiah Kuala University, Banda Aceh, Indonesia

Abstract
This study aims to examine regulations regarding legal protection for bank customers using internet banking from the threat of phishing in Indonesia based on the prevailing laws and regulations. This study used a normative legal research method with a statutory approach and data analysis was carried out prescriptively. As internet banking application providers, banks need to pay attention to the privacy or security of their customers' personal data. In the regulations governing the legal protection of customer personal data in the use of internet banking from phishing threats, it is necessary to regulate matters relating to customer data procedures used by irresponsible parties, exceptions to applicable procedures, as well as sanctions in the event of this. Offense. Legal protection from the legal concept of rights and obligations is a concept that explains how the law protects a person's interests, by allocating a power to act in his interests. So far, regulations regarding the protection of internet banking customers from phishing threats have been discovered by interpreting these regulations into an understanding of internet banking, or linking one law to another. This clearly shows the absence of a law that functions to supervise, prosecute and provide protection for internet banking service activities from phishing threats. regulations regarding the protection of internet banking customers from phishing threats have been discovered by interpreting these regulations into an understanding of internet banking, or linking one law to another. This clearly shows the absence of a law that functions to supervise, prosecute and provide protection for internet banking service activities from phishing threats. regulations regarding the protection of internet banking customers from phishing threats have been discovered by interpreting these regulations into an understanding of internet banking, or linking one law to another. This clearly shows the absence of a law that functions to supervise, prosecute and provide protection for internet banking service activities from phishing threats.

Keywords: consumer protection, internet banking, phishing

Introduction

Preliminary

Banks are one of the partners for the community in meeting their financial needs as well as a place to carry out various types of financial transactions. The existence of banks in people's lives is very important because banking institutions are the spirit of a country's financial system, whose functions include agents of development, agents of trust, and agents of services. The development of banking is increasingly rapid and modern along with the times that have entered the digital era. The sophistication of information technology is used by banking institutions in conducting various banking transactions through electronic media. Banking services in the form of internet banking are services intended for bank customers in order to conduct transactions and obtain information [1]. Major advances in internet banking have made it easier for customers to transact in real time and quickly, without any time and place restrictions. So that to carry out banking transactions, customers no longer have to go to the bank or to the nearest ATM, except for making deposits and cash withdrawals.

Developments in the world of information technology must receive sufficient attention to anticipate developments that are taking place in the world of trade, especially in the banking sector. This resulted in the need for an adjustment to the legislation in the banking sector, therefore the birth of an important legal instrument in the form of Law Number 10 of 1998 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection and Law Number 19 of 1998. 2016 concerning Electronic Transaction Information (ITE).

In the practice of Internet Banking, there are various kinds of attacks or threats for the users and internet banking service providers. For example, the crime of phishing, *phishing (internet banking fraud*) is an activity to lure internet users in the hope that the user unconsciously provides information on user data and passwords on a website that has been defaced. Phishing is usually directed at online internet banking users. The target is customers who want to transact internet banking less thorough in writing a website.

The way it works, hackers usually buy a lot of spoof domains from the targeted bank, the target is that the user does not realize that he has typed the website address wrong, but the initial page of the target website is made the same as the original, the result expected by hackers is that the customer fills in the User ID and password. After accessing the customer, they will be given information about the disruption to the target bank's server, even though it is part of the hacker's engineering to make the customer not realize that the user and password have been hacked by intruders.

Legal protection is closely related to the customer's sense of trust and security in the system, therefore an adequate legal protection is needed. However, apart from the added value of internet banking services, from a legal point of view the

presence of internet banking services still has a number of problems. This condition is exacerbated by changes in internet banking services both in terms of technology and business very quickly.

Previous research that focused on legal protection for internet banking users was conducted by Selly Maulina in 2016 which was published in the Kanun Journal of Legal Studies which focused on "Banks' Responsibilities to Customers Who Have Loss in the Use of Electronic Banking".Research by Wafiya in 2012 which has been published in the Kanun Journal of Legal Studies which focuses on "Legal Protection for Customers Who Have Loss in Banking Transactions Through the Internet". Research by I Made Adi Medhyana Putra in 2020 which has been published in the Ketha Wicara Journal which focuses on "Legal Protection of the Rights of Bank Customers as Consumers of Internet Banking Services from the Threat of Cybercrime".

Based on previous research, there are differences in the focus of the research that will be carried out by the author with previous research. Although they have similarities with the theme of customer protection, this research focuses on legal protection that is obtained as a customer's right to use internet banking if they experience a phishing threat. The importance of this research is carried out because of the weak position of customers in general compared to the position of banks, so that discussions about customer protection are always important and actual for further study, especially the legal protection arrangements that are obtained as a customer's right to use internet banking if they experience a phishing threat.

In this study, normative legal research is used, namely legal research that puts the law as a building system of norms. The approach used in this research is the statute approach. The main data sources in normative legal research are primary legal materials consisting of statutory regulations, jurisprudence, and international agreements. Secondary legal materials are legal materials that can provide explanations for primary legal materials, which can be in the form of draft laws, research results, textbooks, scientific journals and internet news. Tertiary legal materials are legal materials that can explain both primary legal materials and secondary legal materials in the form of dictionaries, encyclopedias.

Data collection techniques in normative legal research are carried out by literature studies of legal materials, both primary legal materials, secondary legal materials as well as tertiary legal materials and or non-legal materials. In this case, data processing is carried out by selecting secondary data and legal materials, then classifying according to the classification of legal materials and compiling data from the research results systematically. Data analysis in this study uses the nature of prescriptive analysis to provide arguments for the results of the research that has been done.

Discussion

Consumer Legal Protection Against Bank Customers From the Threat of Digital Phishing (Phishing) for Using Internet Banking

One of the characteristics as well as the purpose of the law is to provide protection (protection) to the community. Law is the latest means in controlling various changes in society so that the existing changes are able to also realize the development of the nation and state in a more positive direction. The law is able to provide solutions to the possibility of using and utilizing science and technology for the maximum benefit and survival of human beings, in the context of internet banking, one of the objectives of the law is to protect consumers. Legal protection is to provide protection for human rights that have been harmed by others and this protection is given to customers so that they can enjoy all the rights granted by law. If the consumer is the community, it means protecting the consumer means also protecting the community.

So far, regulations regarding the protection of internet banking customers from the threat of phishing have been found by interpreting these regulations into an understanding of internet banking or linking one law to another. This clearly shows the absence of a law that functions to monitor, prosecute and provide protection for internet banking service activities from the threat of phishing.

*Phishing*is an act to obtain personal data such as User ID (which is an identification to enter and access the internet), PIN (which is a secret password number between the user and the system), account numbers, credit card numbers against the law by using fake e-mails to someone, company or organization in which the sender certifies that the sender is a legitimate business entity.

The threat of phishing that often occurs in internet banking services is a threat using social engineering techniques with the mode of tricking customers (service users). Customers are attracted by various offers sent via e-mail, short messages, or direct telephone calls from the phishers themselves who disguise themselves as bank entities, then invite customers to provide information about personal banking data.

Banks as business actors providing internet banking applications, need to pay attention to the privacy or security of their customers' personal data. Consumer protection from the legal concept of rights and obligations. The concept that explains how the law protects a person's interests by allocating a power to act in his interests. In consumer protection, the law provides protection in the form of rights for consumers to exercise their power, namely requiring business actors to send products that have been paid for.

In practice, the UUPK is made and enforced with the consideration that the legal provisions that protect consumers in Indonesia are not adequate and a set of laws and regulations is needed to achieve a balance of protecting the interests of consumers and business actors so as to create a healthy economy. Satjipto Raharjo defines legal protection as providing protection for human rights that are harmed by others and this protection is given to the community so that they can enjoy all the rights granted by law.

This right is obtained because the consumer has carried out his obligations in the form of payment for the goods ordered. Ideally, rights are paired with obligations, rights for business actors are obligations for consumers, as well as obligations for business actors will become rights for consumers. The rights owned by consumers are the obligations of business actors which are defined as consumer protection.

Based on Article 1 point (1) UUPK, the purpose of making UUPK is to provide protection guarantees for consumers but based on the interests of business actors so that in the UUPK there are rights and obligations as well as rights and obligations for business actors, especially banks as service

providers of internet banking application services. The term consumer in the legislation in Indonesia, in Article 1 number (2) UUPK. Consumers are every person who uses goods and services available in the community, both for the benefit of themselves, other people's families, and other living creatures and not for trading.

In Article 4 point 1 UUPK mentions the rights of consumers to comfort, security and safety in consuming goods and/or services. So that the bank as an internet banking application service provider must take full responsibility in providing services to customers regarding comfort, security and safety in using internet banking applications.

Article 4 point (4) contains the right to have their opinions and complaints heard on the goods and/or services used. This rule can be used as a reference for customers in providing input or questions regarding the lack of internet banking services provided by banks to avoid losses. So that banks must be more serious in accepting opinions and complaints from customers who feel disadvantaged from the threat of phishing. With that, the bank must improve its security system.

The application of sanctions is very necessary in legal protection so that law violators do not repeat their actions. Judging from Article 60 to Article 63 of the UUPK, these sanctions can be in the form of administrative sanctions and criminal sanctions. One of the civil sanctions is compensation for customers who feel that they have been harmed. The application of sanctions that can be given is a warning letter or a fine as a light sanction that gives the effect of business actors not daring to repeat their actions that can harm customers who use internet banking application services.

Law Number 9 of 1999 concerning Consumer Protection (UUPK) has not fully protected consumers in electronic transactions. This condition is because the UUPK has not regulated further implementation of the notion of consumer protection which includes online consumer protection, the right to information that must be provided to consumers through online media to prevent fraudulent actions, misuse of personal data belonging to others, the responsibilities of business actors which include responsibility for the responsibility of the ISP (Internal Service Provider), the burden of electronic proof, and dispute resolution through information technology facilities.

Article 29 paragraph (4) of Law Number 10 of 1998 concerning Banking states that for the benefit of customers, banks are required to provide information regarding the possibility of risk of loss in connection with customer transactions conducted through banks. This is because banks get sources of funds from the public which are then deposited into the bank based on trust. The application of this rule is very important for banks to provide legal protection to their customers because banks must act more actively in sharing information with customers related to the threat of loss in the use of internet banking.

Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions (hereinafter referred to as UU ITE) is the main legal basis for transactions trade using electronic media. The importance of the ITE Law in providing protection to banking consumers in conducting internet banking media trading activities are:

1. Recognition of transactions, information, documents and electronic signatures within the framework of the law of engagement and the law of evidence, so that the legal certainty of electronic transactions can be guaranteed.
2. Classification of actions that include the qualification of legal violations related to the misuse of information technology accompanied by criminal sanctions.
3. The ITE Law applies to everyone who carries out legal actions, both within the territory of Indonesia and outside the territory of Indonesia. So that the scope of the ITE Law is not only local but also international.

In relation to consumer rights as contained in Article 4 letter (c) of the UUPK that consumers have the right to get correct and clear information about products sold by business actors, then the ITE Law regulates this which is contained in Article 9 of the ITE Law, namely:

Business actors who offer products through electronic systems must provide complete and correct information relating to contract terms, manufacturers, and products offered.

The provisions contained in Article 9 of the ITE Law certainly give consumers the right to obtain correct and complete information regarding goods or products offered by business actors in conducting trading activities through electronic media. Legal protection for consumers in electronic trading transactions is contained in Article 28 paragraph (1) of the ITE Law, namely:

Everyone intentionally and without rights spreads false and misleading news that results in consumer losses in electronic transactions.

Regarding the criminal sanctions applied for violations committed in Article 28 paragraph (1), the provisions are contained in Article 45 (a) paragraph (1) of the ITE Law, namely:

Anyone who intentionally and without rights spreads false and misleading news that results in consumer losses in electronic transactions as referred to in Article 28 paragraph (1) 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).

Legal protection for bank customers in the form of Law Number 19 of 2016 concerning Electronic Transaction Information (ITE), is made in order to easily limit the use of internet media which has not been able to regulate and overcome legal problems, one of which is internet banking from threats. Based on Article 15 paragraph (1) of the ITE Law, it is explained:

"Every electronic system operator must operate the electronic system reliably and safely and be responsible for the proper operation of the electronic system."

In the explanation of Article 15 paragraph (1) it is explained that "reliable" means that the electronic system has capabilities that are in accordance with the needs of its users. Safe means that the electronic system is protected both physically and non-physically. Operating properly means that the electronic system has the capability according to its specifications. In addition, the implementation of the electronic system.

Being responsible means that there are legal subjects who are legally responsible for the operation of the electronic system. The guarantee of legal protection that can be provided by the ITE Law regarding the protection of

customers' personal data, based on Article 26 paragraph (1) that unless stipulated otherwise 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. And Article 26 paragraph (2) that any Person whose rights are violated as referred to in paragraph (1) may file a lawsuit for the losses incurred under this Law.

The regulation of actions that are prohibited and can only be imposed in the form of criminal sanctions are seen from the ITE Law, namely:

1. Article 30 paragraph (1) explains that every person intentionally and without rights or against the law accesses a computer and/or. Electronic Systems belonging to others in any way. Article 46 paragraph (1) explains that any person who fulfills the elements as referred to in Article 30 paragraph (1) shall be sentenced to a maximum imprisonment of 6 (six) years and/or a maximum fine of Rp. 600,000,000.00 (six hundred million rupiah).
2. Article 30 paragraph (2) explains that any Person intentionally and without rights or against the law accesses a Computer and/or Electronic System in any way with the aim of obtaining Electronic Information and/or Electronic Documents. Article 46 paragraph (2) explains that any person who fulfills the elements as referred to in Article 30 paragraph (2) shall be sentenced to a maximum imprisonment of 7 (seven) years and/or a maximum fine of Rp. 700,000,000.00 (seven hundred million rupiah).
3. Article 30 paragraph (3) explains that any Person intentionally and without rights or against the law accesses a Computer and/or Electronic System in any way by violating, breaking through, exceeding, or breaking into the security system. Article 46 paragraph (3) explains that any person who fulfills the elements as referred to in Article 30 paragraph (3) shall be sentenced to a maximum imprisonment of 8 (eight) years and/or a maximum fine of Rp. 800,000,000.00 (eight hundred million rupiah).
4. Article 31 paragraph (1) explains that any Person intentionally and without rights or against the law conducts interception or wiretapping of Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another Person. Paragraph (2) explains that any Person intentionally and without rights or against the law intercepts the transmission of Electronic Information and/or Electronic Documents that are not public from, to, and within a certain Computer and/or Electronic System belonging to another Person, either which does not cause any changes or causes changes, disappearances, and/or termination of Electronic Information and/or Electronic Documents that are being transmitted. Article 47 explains that any person who fulfills the elements as referred to in Article 31 Paragraph (1) and Paragraph (2) shall be sentenced to a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 800,000,000.00 (eight hundred million rupiah).

Currently, there are no specific rules governing the issue of legal protection for banking customers in terms of the use of internet banking. So we need a legal rule regarding customer protection because it becomes important and actual for the creation of legal certainty and protection in the future, especially the legal protection that is obtained as a customer's right in using internet banking.

Legal protection is a narrowing of the meaning of protection, in this case only protection by law. The protection provided by law in the use of internet banking is categorized into 2 parts, namely preventive legal protection and repressive legal protection, also related to the existence of rights and obligations, in this case those owned by humans as legal subjects in their interactions with fellow humans and their environment. As legal subjects, humans have the right and obligation to take legal action.

Consumer protection is a term used to describe the existence of a law that provides protection to consumers from losses on the use of banking goods and/or services in the form of internet banking. UUPK has a broad scope, covering consumer protection for goods and services, starting from the activity stage to obtain goods and services to the consequences of using these goods and/or services.

The scope of consumer protection can be distinguished in two aspects, namely protection against the possibility of goods delivered to consumers not in accordance with what has been agreed. Protection against the application of unfair terms to consumers. The desire to be achieved in consumer protection is to create a sense of security for consumers in using internet banking, it is proven that all consumer protection norms in Law Number 8 of 1999 concerning Consumer Protection (UUPK) have civil and criminal sanctions.

Regulations regarding the principles or principles that apply in consumer protection law are formulated in laws and regulations which state that consumer protection is based on benefits, justice, balance, security, and consumer safety as well as legal participation. In socializing in society, especially regarding businesses that use internet banking, where we live in the midst of people with different temperaments and interests, we certainly will not be able to avoid dealing with problems at all. Problems in business transactions using internet banking are caused by the irresponsible use of personal data by certain parties.

In short, all the efforts intended for consumer protection are not only preventive measures, but also repressive measures in all areas of protection provided to banking consumers. To be able to enforce consumer protection law, it is necessary to apply principles that serve as the basis for legal determination.

Preventive legal protection is protection provided by the government with the aim of preventing violations before they occur. This is contained in the Laws and Regulations with the aim of preventing a violation and providing signs or limitations in carrying out an obligation. Repressive legal protection is repressive legal protection which is the final protection in the form of sanctions such as fines, imprisonment, and additional penalties given if a dispute has occurred or a violation has been committed.

The law functions as the protection of human interests, so that human interests are protected, the law must be implemented professionally. The implementation of the law can take place normally, peacefully and in an orderly manner. Laws that have been violated must be enforced through law enforcement. Law enforcement requires legal certainty, legal certainty is justifiable protection against arbitrary actions.

Customers expect legal certainty in the use of internet banking when problems occur in the use of internet banking, because with legal certainty the community will be orderly, safe and peaceful. The community expects benefits in implementing law enforcement. The law is for humans, so the implementation of the law must provide benefits, usefulness for the community, do not let the law be implemented causing unrest in society.

Customers who get good and right treatment will create a situation that is understated and peaceful. The law can protect the rights and obligations of each individual in actual fact, with strong legal protection the general goals of law will be realized, order, security, peace, prosperity, peace, truth, and justice.

These rules become limitations for society in burdening or taking action against individuals. The existence of such a rule and the implementation of these rules creates legal certainty. Thus, legal certainty contains two meanings, namely first, the existence of general rules that make individuals know what actions may or may not be done and two, in the form of legal security for individuals from government arbitrariness because with the existence of general rules individuals can know what the State may charge or do against individuals. Legal certainty is not only in the form of articles in the law, but also the consistency in the judge's decision between the decisions of one judge and the decisions of other judges for similar cases that have been decided.

In the use of internet banking using online networks in banking activities, customers are parties who must get legal protection. Banking services through internet banking have in principle raised a number of legal issues regarding the protection of customers' personal data that can be accessed by others, namely the threat of phishing in the use of internet banking.

The customer's personal data that is accessed is an identity that is commonly provided by the customer to the bank in the context of conducting financial transactions with the bank. In the event that the bank will provide and disseminate customer personal data to other parties for commercial purposes, unless stipulated by other laws and regulations.

Legal protection of customers' personal data, in practice the banking sector needs to be done through protection of the confidentiality and security of customer information, where all transactions related to customers are kept confidential from other parties, as well as provisions regarding the provision of customer information from banks to other parties where the bank needs to request approval from the customer so that without the customer's consent, the bank should not be able to provide customer data to other parties.

In the regulations governing the legal protection of customer personal data in the use of internet banking from the threat of phishing, it is necessary to regulate matters relating to procedures in customer data used by irresponsible parties, exceptions to applicable procedures, as well as sanctions in the case of violation occurs. Legal protection of customers' personal data in the use of internet banking can be done using self-regulation and government regulation approaches. Preventive legal protection in the use of internet banking from the threat of phishing with a self-regulation approach basically refers to internal legal arrangements in terms of the process of providing internet banking services itself.

The current legal arrangement is felt to be very unsupportive of the implementation of banking activities using the online network. UUPK, UU ITE and Banking Law do not specifically accommodate the implementation of internet banking. Interpreting crimes in the banking sector using the existing law does not reflect the role of legal protection, namely providing protection for human rights that have been harmed by others and this protection is given to the public so that they can enjoy all the rights granted by law.

The form of protection is the existence of certain requirements in the use of technology that will be used to transact using internet banking services at banks. This is done based on an awareness that all technologies must have their respective weaknesses and not all banks can master internet banking technology. There needs to be a mechanism that protects an act of wiretapping in internet banking. This is because the communication that occurs between the client-server goes through an encrypted path, but this system does not protect against malicious user entry, nor does it protect whether a code downloaded from a site can be trusted.

From the government regulation approach, it can be found in the Banking Law, namely Article 29 paragraph (5) and Article 40 paragraph (1) and paragraph (2). Article 28 paragraph (5) states that for the benefit of customers, banks provide information regarding risks arising for customer transactions conducted through banks. Furthermore, Article 40 paragraph (1) and paragraph (2) states:

1. Banks are required to keep confidential information regarding depositors and their deposits, except in the case as referred to in Article 41, Article 41A, Article 42, Article 43, Article 44 and Article 44A.
2. The provisions as referred to in paragraph (1) also apply to affiliated parties

According to the author, the application of the principle of confidentiality as regulated in the implementation of internet banking is not optimal, because the legal protection given to customer personal data as stated in the provisions of the Act is only limited to data stored and collected by the bank. Like various legal efforts that must be given by law enforcement officers to provide a sense of security, both mentally and physically from disturbances and various threats from any party.

In the implementation of internet banking, existing customer data is not only stored and collected, but includes data transferred by the customer from the electronic media where the customer makes transactions. Based on these. The Banking Law has not been able to provide full protection to customers' personal data in the implementation of internet banking, so that the threat of phishing and so on is still possible to cause customer data to be used by irresponsible parties, and legal protection for consumers is expected not to be implemented properly.

Conclusion

Arrangement consumer legal protection for bank customers from the threat of digital phishing for the use of internet banking refers to Article 28, Article 29 and Article 40 of Law Number 10 of 1998 concerning Banking. Article 4, Article 19 of Law Number 8 of 1999 concerning Consumer Protection and Article 28, Article 15, Article 26 paragraph (2) of Law Number 19 of 2016 concerning Information and Electronic Transactions. To the Government together with the banking sector to form laws and regulations related to

the implementation of internet banking in order to maintain the rights and obligations of banks and customers.

References

1. Janus Sidabalok. Consumer Protection Law in Indonesia Cet. Third, PT. Citra Aditya Bakti, Bandung, 2014.
2. Kasmir. Banking Fundamentals Revised Edition, PT Raja Grafindo Persada, Depok, 2014.
3. Mukti Fajar, Yulianto Achmad. Dualism of Normative and Empirical Legal Research, Student Library, Yogyakarta, 2010.
4. Maryanto Supriyono. Smart Book on Banking, ANDI, Yogyakarta, 2011.
5. Sentosa Sembiring. Banking Law Revised Edition, CV. Mandar Maju, Bandung, 2021.
6. Trisadini P. Usanti and Abd. Shomad. Banking Law, KENCANA, Depok, 2017.
7. Journals and Other Scientific Works
8. Dwi Ayu Astini, Legal Protection of Internet Banking User Bank Customers from Cybercrime Threats.*https://ejournal.unsrat.ac.id/index.php/lexprivatum/article/view/7035.* Lex Privatum, Vol 3 No 1, Accessed,2021:3:1.
9. Kornelius Benuf, Siti Maheasy, Ery Agus Priyono, Legal Protection of Financial Technology Consumer Data Security in Indonesia, *https://ejournal.uksw.edu/releksi Hukum/article/view/2413*. Journal of Legal Reflection. Accessed, 2021:3:2.
10. Lukmanul Hakim, Accountability of Banking Institutions Against Customer Data Theft, *https://journal.maranatha.edu/index.php/dialogia/article/view/918*,Dialogia Iuridica Journal of Business and Investment Law, Vol 10 No 1, Accessed April 23, 2021
11. Ikhsan Radiansyah, Candiwan, Yudi Priyadi, Phishing Threat Analysis in Online Services, https://ejournal.umm.ac.id/index.php/jibe/article/view/jekobisnis.v7i1.3083, Journal of Innovation in Business and Economics (JIBE), Vol 1 No 1, Accessed April 27, 2021
12. I Made Adi Medhyana Putra, Legal Protection of the Rights of Bank Customers as Consumers of Internet Banking Services from Cybercrime Threats, *https://ojs.unud.ac.id/index.php/kerthawicara/article/view/58241*, Journal of Kertha Wicara, Vol 9 No 4, Accessed April 26, 2021
13. Nugraha, Ferry Satya, And Rinitami Njatrijani Budiharto, Legal Protection of Bank Customers in Internet Banking Breaking Through Malware Methods, *https://ejournal3.undip.ac.id/index.php/dlr/article/view/12348/11994*, Diponegoro Law Journal 5, Vol 5 No. 3, Accessed April 28, 2021
14. Mansyur, Ali, And Irsan Rahman, Law Enforcement of Consumer Protection as an Effort to Improve National Production Quality, *http://jurnal.unissula.ac.id/index.php/PH/article/view/1411*, Journal of Legal Reform, Vol 2 No 1, Accessed April 28, 2021
15. Selly Maulina, Dahlan, Mujibussalim, The Bank's Responsibility Towards Customers Who Suffer Loss in the Use of Electronic Banking, http://www.jurnal.unsyiah.ac.id/kanun/article/viewFile/5929/4883. Kanun Journal of Legal Studies, Vol 18 No 3, Accessed April 30, 2021
16. Wafiya, Legal Protection for Customers Who Suffer Losses in Banking Transactions Through the Internet, http://jurnal.unsyiah.ac.id/kanun/article/view/6198/5094. Kanun: Journal of Legal Studies, Vol 14 No 1, Accessed April 30, 2021
17. Regulation
18. Law Number 10 of 1998 concerning Banking (State Gazette of the Republic of Indonesia of 1998 Number 182)
19. Law Number 8 of 1999 concerning Consumer Protection (State Gazette of the Republic of Indonesia of 1999 Number 42)
20. Law Number 19 of 2016 concerning Electronic Transaction Information (State Gazette of the Republic of Indonesia of 2016 Number 251)