JLPH: Journal of Law, Politic and Humanities
E-ISSN: 2962-2816
P-ISSN: 2747-1985
https://dinastires.org/JLPH dinasti.info@gmail.com +62 811 7404 455
DOI: https://doi.org/10.38035/jlph.v5i4

Legal Protection for Bank Customers Who are Victims of Electronic Information Technology Crimes in the Banking Sector in Jayapura City

Eddy Pelupessy[1], Farida Kaplele[2].
[1]Faculty of Law, Cenderawasih University, Jayapura-Papua, Indonesia, eddypelupessy5@gmail.com.
[2]Faculty of Law, Cenderawasih University, Jayapura-Papua, Indonesia, farida.kaplele16@gmail.com.

Corresponding Author: eddypelupessy5@gmail.com[1]

Abstract: Banking crimes are increasing, and perpetrators do it in various ways that can ultimately harm customers. The purpose of this study is to find out and analyze how related laws protect customers who are victims of ITE crimes in the banking sector and how banks are responsible for these customers. This study uses a normative legal method, which means research in the legal field that uses secondary data. This secondary data includes laws and regulations, court decisions, legal theories, and scholarly opinions. The results of this study indicate that adequate legal protection for victims of crime is a national and international problem. Therefore, the importance of protecting victims of violations is recognized. Legal protection for victims of crime is a protection of human rights or a person's legal interests that should receive special attention. This is important because crime and its victims are increasingly complex along with the progress of today's civilization. Therefore, banking institutions and consumer institutions can work together to create agreement clauses that meet the needs of the parties and do not violate the element of propriety. In addition, banks monitor employee behavior periodically to find indications of violations of the law.

Keyword: Legal Protection, Bank Customers, Victims of ITE Crimes in the Banking Sector.

INTRODUCTION

The development of crimes related to this technology is often referred to as a form of cybercrime. The classic form of this crime is such as: Joycomputing (using a computer without permission), hacking (entering a computer network system illegally), The Trojan horse (manipulating computer programs), Data Leakage (data leaks), Data Diddling (computer data manipulation) and Computer Data Destruction. These crimes can be called the 'cost' or high price of a change in global society whose level of development exceeds the existence of law.

Cybercrime, which is popularly called cyber space crime, is a reflection of the condition of society that is always chasing between desires and the pull of global influence that not a few produce and offer changes that are detrimental. For example, making technology a tool to meet the development and basis for developing transaction systems in banking, but we still often fail to reject its destructive impact. Based on the development of the era and the increasingly

sophisticated technology, it is also increasingly spurring cybercrime to evolve into various types of new crimes and modus operandi related to cybercrime. Law functions as a protection of human interests. In order for human interests to be protected, the law must be implemented (Sudino Mertokusumo and A. Pitlo, 1993). So legal protection is protection provided by law or statutes to protect human interests so that human life can proceed normally, peacefully and peacefully.

Legal problems related to the detention of criminals are usually associated with various problems related to several characteristics of cybercrime crimes. First, this crime crosses territorial boundaries or free borders, or even outside the state's territory, which ultimately has a relationship. However, this study focuses on cybercrime violations in national territorial areas. Second, considering that cybercrime is something completely new, can interpretation use criminal law to ensnare such crimes? This is a very important issue for the principle of legality in criminal law. While criminal law usually only accepts original interpretation. In addition to other related issues, such as electronic evidence and continuity. Marc Ancel defines criminal law policy as a science and art that aims to enable legal regulations, especially criminal law policies, to be formulated better

Meanwhile, efforts to formulate better criminal law include policies to change or create special rules (criminal law) related to cybercrime. This means that although it can essentially be analogous to crimes or criminal acts that can be regulated in the Criminal Code, according to experts, criminal law does not accept analogies. In addition, because the characteristics of these crimes are different, it is possible to make them separate criminal acts with their own rules in order to realize a better formulation of criminal law. Criminalization of acts in Chapter VII as acts There are two main laws that regulate information and electronic transactions in Indonesia. The first law is Law No. 11 of 2008 concerning Information and Electronic Transactions. The second law is a law that was issued before the issuance of Law No. 11 of 2008 concerning Information and Electronic Transactions. The law is Law No. 36 of 1999 concerning Telecommunications.

The role of technology in the banking world is very absolute, where the progress of a banking system is certainly supported by the role of information technology (Ronny Presetya, 2010). The more developed and complex the facilities implemented by banks to facilitate services, it means that the adoption of technology owned by a bank is increasingly diverse and complex. It is undeniable that in every field including banking, the application of technology aims not only to facilitate the company's internal operations, but also to facilitate services to customers or bank clients. If for now, especially in the banking world, almost all products offered to customers are similar, so that the competition that occurs in the banking world is how to provide products that are easy and fast. However, it seems that behind this development there are various legal problems related to information crimes and electronic transactions in the banking sector which then harm banks, the public and/or customers if not anticipated properly.

Corporations, especially banking institutions, are not only victims of account hacking, but also victims of cybercrime in the banking sector, such as hacking of security systems and hacking of customer accounts or electronic systems in the national banking system. This action is known as carding. Carding modus operandi is that there are various carding programs and how to get credit cards, how to make fake credit card numbers, how to duplicate legitimate credit cards, and how to use fake credit cards. Obtaining data related to an account can be done in various ways. This is usually done without the knowledge of the credit card holder, merchant, or credit card issuing bank at least until the account is used to commit a crime.

So with the emergence of the modus operandi of this carding crime, it becomes a trigger for the emergence of the impacts caused. The impacts of the carding crime include direct and indirect victimization of the community, material and non-material losses to the banking system in particular and the economic system in general, the law in our country must be rejuvenated immediately. So the more the world of communication develops through internet services and

the more dependent business transactions are using banking services via the Internet, the regulation of cybercrime in Indonesia is urgently needed.

Along with the rapid development of information technology has changed the pattern of life, virtual life and reality life. This paradigm change is a result of the presence of cyber space, which is the impact of the global computer network. Especially related to the elements of actions, distributing, transmitting, making accessible. While related to the elements of actions that have the content of "Extortion" and "Threats" are still very less specific in the rules of explanation. Related to the elements that have the content of "Threats" the interpretation is still very broad. For example, if someone accesses a network or computer system belonging to a particular company or bank, it can be said to be an act of threat.

In relation to the matters that have the content of the threat above, there are no explanatory rules in the ITE Law, so the judges make a positive legal interpretation by using the provisions of acts prohibited in the Criminal Code, namely: theft, embezzlement, and fraud. If the judge applies these provisions, it will only be aimed at perpetrators of ITE crimes and the rights of victims, especially the rights of bank customers, have not been fulfilled. So in this problem, the ITE Law still does not provide protection for the rights of bank customers as victims of ITE crimes in the banking sector. Therefore, civil legal efforts need to be made, as an effort to fulfill the rights of bank customers as victims of ITE crimes in the banking sector.

In fact, Article 30 paragraph (1) and Article 46 paragraph (1) of the ITE Law regulate legal sanctions against perpetrators of crimes, but these provisions are rarely used because they are still general. However, when we look at the civil legal efforts made by banks and bank customers who are victims of ITE crimes in the banking sector, their rights have not yet been fulfilled. Due to the fact that ITE criminals break into the banking company system and attempt to access, distribute, manipulate, copy, and break into bank customer data or accounts, banking institutions do not provide guarantees for material losses caused by theft of bank customer accounts if they are not regulated in detail in the draft of the account security guarantee agreement between the bank and the bank customer.

Because the provisions of the Witness and Victim Law are explained in relation to the fulfillment of the rights of victims for losses caused by perpetrators of crimes. So that special provisions are needed in the Banking Law that regulate the rights of bank customers who are victims of ITE crimes in the banking sector. In addition to bank customers who are victims of crimes committed by perpetrators of ITE crimes. Banking companies are also victims of losses caused by perpetrators of ITE crimes in the banking sector. Banks that are victims of ITE crimes are also entitled to rights for the losses experienced. Both regarding the bank's computer system/network that is damaged or hacked by perpetrators of crimes, as well as compensation for customer accounts that have been stolen or hacked by perpetrators of ITE crimes. In addition, banking companies are also obliged to fulfill the rights of bank customers who are victims of crimes by perpetrators of bank account hacking (if there is an agreement that regulates it).

METHOD

This study uses a normative legal approach, namely research in the field of law that uses detailed secondary data that is the main problem in the form of laws and regulations, court decisions, legal theories and opinions of scholars. That is also why qualitative analysis (normative-qualitative) is used because the data is qualitative

RESULTS AND DISCUSSION

Legal Protection for Customers Who Are Victims of ITE Crimes in the Banking Sector.

Until now, the national banking system has not paid proper attention to the issue of banking customer protection. Therefore, the issue of consumer protection and empowerment is a special concern. This shows a strong commitment from Bank Indonesia and the banking sector

to place banking service users in the same position as banks. Customers are always in a weak or disadvantaged position in legal cases or disputes between banks and their customers.

To overcome these problems, banks together with the community will have several agendas aimed at strengthening customer protection. The agenda is to prepare a customer complaint mechanism, establish a banking mediation institution, increase product transparency and implement education on bank products and services to the wider community. Of these programs, the establishment of an ombudsman for banking consumers is something new for us, because currently there is no special institution that handles disputes between banks and bank consumers as in several other countries.

In order to implement protection for bank customers, the following have been carried out:

a. There is a process of reshaping the structure of the Indonesian banking industry. This includes directions regarding institutional aspects, ownership, and operational patterns of a bank or group of banks, in order to achieve the vision and objectives that have been set.
b. Bank Indonesia has determined that the preparation of various banking regulations must always be based on research (research-based) and refer to best practices and international standards. In addition, in the process of regulating banks, Bank Indonesia will always involve banking practitioners.
c. The development of an effective and independent supervision system is attempted to always be directed and in line with the principles of effective bank supervision from the 25 Basel Core Principles. In addition, in order for bank supervision to run effectively, Bank Indonesia will conduct re-engineering in various aspects of supervision, in order to be able to apply a risk-based supervision approach. Other steps are to review the possibility of implementing consolidated supervision, preparing a bank supervisor certification program, and implementing Real Time Supervision.
d. That important issues that will be formulated as optimization steps include good governance, banking management information systems, intermediation functions, handling of problem loans, implementing risk management and the possibility of national banking to implement best practices such as Basel II provisions and anti-money laundering
e. That several supporting infrastructure needs need to be prepared for their existence, including rating agencies, Deposit Insurance Corporation (LPS), credit insurance, and the existence of the Credit Bureau as a center for debtor information and the use of adequate information technology. The existence of these institutions is expected to have a positive impact on the performance of the banking industry.
f. That the need that is considered necessary to be prepared is a mechanism for handling bank customer complaints. Another problem that needs to be considered is efforts to empower consumers who use banking services. In this case, one of the methods taken is in the form of transparency in providing complete information regarding banking products or services, including the possible risks faced by consumers or bank customers.

In addition to the concept of legal protection for customers mentioned above, when customers are customers of banking services, consumer protection for them must be prioritized. Customers are very important in the banking world; the life of the banking world depends on the community or customers themselves. The laws and regulations and provisions of the agreements that regulate the relationship between banks and their customers pay special attention to the issue of customer protection. Both legal agreements and private deeds can form the basis of the legal relationship between banks and their clients. In such a situation, it is very important to maintain protection for consumers without weakening the position of the bank. Therefore, it is important to remember that the agreements made between the bank and the customer are often covered by standard agreements. Other banking services that need to be considered in order to protect customers include credit card issuance, bank guarantees, money transfers, safe deposit box rentals, and other services. Problems that often arise are related to these banking services.

From the focus that needs attention for consumer protection in the banking service sector as above, the main cause is because of weaknesses in several clauses of the agreement between customers and banks, for example, provisions on the obligation for savers to maintain a minimum savings balance, which usually if less than the minimum will be subject to a larger administration fee but will not get interest. Concerning efforts to protect consumers, it does not actually depend on the application of civil law alone as expected through sanctions and compensation mechanisms. Other legal provisions such as criminal law or state administrative law also contain provisions that can protect consumers such as agreement mechanisms and tightened supervision.

Current conditions even consumer protection has received more serious attention with the stipulation of laws and regulations governing it, namely Law No. 8 of 1999 concerning Consumer Protection. However, caution is still needed in determining who is responsible for negligence or errors that have occurred in the management or administration of the bank so that a loss is experienced by the customer. The problem of civil liability for negligence or errors that occur in the bank can be linked to the management of the bank. The bank manager is the party that acts on behalf of the bank's legal entity based on the provisions of the company's articles of association. Thus, the responsibility of the manager for his actions becomes two forms, namely personal responsibility and corporate responsibility.

If the management acts outside the authority stipulated in the company's articles of association when granting the power of attorney, there is personal responsibility. However, if the management's actions are still carried out in accordance with the authority granted by the company's articles of association, then it is the company's responsibility. Thus, the bank is bound by its management's actions towards third parties. Therefore, the bank is responsible for the mistakes of its management based on the company theory, namely that mistakes are the limit of prosperity. In cases where banking institutions suffer losses, especially banks that are liquidated, the victims consist of many consumers who have the same interests and demands.

In order to recover the funds deposited with interest if possible, basically the customer is a concurrent party as the party that receives the first attention to be paid from the proceeds of the sale of the assets of the bank concerned as stipulated in Article 17 paragraph (2) letter a of Government Regulation Number 25 of 1999 concerning Revocation of Business Licenses, Dissolution, and Liquidation of Banks. Although the position of the customer is considered and is positioned as a concurrent party, such protection is still not total, therefore regarding the customer's funds, it is also necessary to guarantee them with deposit insurance in Indonesia.

The intention to implement deposit insurance has been attempted by the government by issuing Government Regulation Number 53 of 1998 concerning State Capital Participation of the Republic of Indonesia for the Establishment of Limited Liability Companies (Persero) in the field of Bank Liability Guarantee. However, if customers do not accept the situation that befell them because the bank where they deposit their funds has had its business license revoked or has been liquidated, then they have the right to sue in court. In the case of a lawsuit for that, they instead file a civil lawsuit as a class action, but it is still possible to sue individually.

In addition, non-governmental consumer protection institutions, the government, or related institutions can also file such lawsuits, in accordance with Article 46 paragraph (1) of Law Number 8 of 1999. If the lawsuit is brought to court, only one representative can bring the matter to court. In this system, all existing customer cases are considered as one unit according to the proportion of each customer section.

In customer protection, criminal provisions contained in the Criminal Code, such as Articles 263, 372, and 374, as well as other articles, can be used. These criminal provisions can also be found in special banking legislation and those related to banking materials. As part of this customer protection effort, inaccurate reports and data provided by a bank to Bank Indonesia can be detrimental to customers. Acts that violate Article 263 of the Criminal Code

in conjunction with Article 49 paragraph (1) letter e of Banking Law Number 7 of 1992 in conjunction with Law Number 10 of 1998 can be subject to sanctions.

Meanwhile, regarding an act of a bank manager who unlawfully uses customer money for personal and group interests, such an act can be charged with embezzlement in accordance with Article 372 or Article 374 of the Criminal Code. As a banking supervisory institution in Indonesia, Bank Indonesia has a very large role in protecting and ensuring that customers do not suffer losses due to wrong bank actions. Bank Indonesia is expected to be more active in carrying out its duties and authority to supervise the implementation of laws and regulations by all banks operating in Indonesia.

Good and effective supervision is a preventive measure that helps prevent or at least reduce customer losses due to illegal actions of banks or other financial institutions. Legal protection for customers can be provided in the Indonesian banking system in two ways, namely:

a) Implicit protection (implicit deposit protection): effective bank supervision and guidance provide protection that prevents bank bankruptcy. This protection is provided through:
   - banking laws and regulations;
   - effective supervision and guidance from Bank Indonesia;
   - efforts to maintain the continuity of bank operations in particular and the banking system as a whole;
   - maintaining bank credibility;
   - acting in accordance with the principle of prudence;
   - providing risk information to customers, and
   - ensuring that the provision of credit does not harm the bank or the interests of customers.
b) Explicit deposit protection, namely protection through the establishment of an institution that guarantees public deposits, so that if a bank fails, the institution will replace the public funds deposited in the failed bank. This protection is obtained through the establishment of an institution that guarantees public deposits, as regulated in Presidential Decree No. 26 of 1998 concerning Guarantees for Commercial Bank Obligations.

In relation to legal protection for depositors, it is divided into two types, namely direct legal protection and indirect legal protection:

1. Direct protection. Direct protection by the banking world for the interests of depositors is a protection given to depositors directly against the possibility of a risk of loss from business activities carried out by the bank. Preferential rights are rights given to a creditor to be prioritized over other creditors. In the Indonesian banking system, depositors are creditors who have preferential rights, meaning that depositors must be prioritized in receiving payments from banks that are experiencing failure or difficulty in fulfilling their obligations. In relation to that, as is known, Law No. 10 of 1998 concerning Banking has regulated articles that aim to provide legal protection for the interests of depositors and their deposits in the bank.
2. Indirect protection. Indirect protection by the banking world for depositors is a legal protection given to depositors against all risks arising from a policy or arising from business activities carried out by the bank. This is an effort and preventive action that is internal by the bank concerned through the following matters. According to Article 2 of Law No. 10 of 1998, it is stated that Indonesian Banking in conducting its business is based on Economic Democracy by using the principle of prudence. From this provision, it shows that the principle of prudence is one of the most important principles that must be applied or implemented by banks in carrying out their business activities. The principle of prudence requires banks to always be careful in carrying out their business activities, in the sense that they must always be consistent in implementing laws and regulations in the banking sector based on professionalism and good ethics.

Bank Responsibilities Towards Customers Who Are Victims of ITE Crimes in the Banking Sector.

ITE crimes in the banking sector can be defined based on the above understanding as crimes committed by the perpetrator using a computer program as a means to carry out the act or committed by the perpetrator against the computer system of a banking company as its target and have been criminalized by criminal law as a criminal act or banking law as a form of banking crime.

Included in the crimes and computer crimes committed by the perpetrator against the computer system as its target are those committed without using a computer as a tool that results in damage to the hardware of another party's computer (for example by using hard objects or by burning it) which of course endangers or damages the computer system contained in the attacked computer hardware.

Legal basis for bank liability to bank customers who are victims of ITE crimes in the banking sector. The legal basis for banking law in Indonesia, concerning sources of law in the formal sense and sources of material law, is the source of law that determines the content of the law itself. Talking about formal sources of law in Indonesia, we will always place the 1945 Constitution as the main source. Furthermore, according to formal sources of law regarding the banking sector, they are as follows:

a. The 1945 Constitution (especially Article 33);
b. Decree of the People's Consultative Assembly, especially regarding the General Guidelines of State Policy;
c. Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE).
d. Basic Laws in the Banking sector and other related supporting sector laws, such as:

1. Basic Regulations, namely Law Number 7 of 1992 concerning Banking and Law Number 10 of 1998 concerning amendments to Law Number 7 of 1992 concerning Banking and Law Number 23 of 1999 concerning Bank Indonesia;
2. Supporting regulations, namely the Criminal Code (KUHP), Civil Code (KUHPerd) and Commercial Code (KUHD) and other laws related to and closely related to banking activities, for example: Laws governing business entities such as: Law Number 5 of 1962 concerning Regional Companies, Law Number 9 of 1969 concerning the Stipulation of Government Regulation in Lieu of Law Number 1 of 1969 concerning Forms of State Enterprises, Law Number 1 of 1995 concerning Limited Liability Companies, Law Number 1 of 1998 concerning Bankruptcy. Law No. 8 of 2010 concerning the Criminal Act of Money Laundering. Ratification laws relating to international agreements in the banking sector and the economic sector such as: Law Number 7 of 1994 concerning Ratification of Agreement Establishing Traderganizaton.

In terms of the legal basis for bank liability related to the use of computer technology in bank operational activities, data related to bank secrecy is no longer limited to written forms on paper; now they are mostly in the form of "electronic pulses stored in various computer storage media." Connecting computers with contemporary telecommunications devices is widely used to transmit this data. Therefore, Article 47 of Law No. 7 of 1992 as amended by Law No. 10 of 1998 concerning Banking applies if there is a leak of bank secrecy through the use of sophisticated technology, such as hacking, cracking, or manipulation of didding data related to electronic documents.

Articles (1) and (2) of Article 47 above indicate that anyone who forces a bank or affiliated party to provide information as referred to in Article 40 shall be subject to criminal sanctions in the form of imprisonment and fines. This sanction shall also be imposed on members of the Board of Commissioners, directors, and employees of the bank or affiliated party who intentionally provide information that must be kept confidential according to Article 40.

In relation to the issue of bank accountability, another potential way is through computer data falsification (data didding) for example by adding a fictitious transaction record in the bank's books, then the perpetrator can be threatened based on the provisions of Article 49 Paragraph (1) letter a of Law No. 7 of 1992 in conjunction with Law No. 10 of 1998. Based on the legal provisions above, it appears that criminal acts in the banking sector tend to be carried out by "insiders". This is understandable because the banking system is closed and difficult to penetrate by unauthorized persons. Moreover, with the use of systems supported by sophisticated technology such as computers which can automatically be operated by those who have special skills and are legally authorized to operate them.

Until now, the national banking system has not paid adequate attention to the issue of bank customer protection. As a result, the Sixth Pillar of the Indonesian Banking Architecture pays special attention to the issue of consumer empowerment and bank customer protection. The purpose of this is to include the issue of bank customer or consumer protection into the Indonesian Banking Architecture.

We often see that customers are always weak or in a disadvantaged position when there are cases of disputes between banks and their customers, so that customers are disadvantaged. To overcome this problem, banks together with the community will have several agendas that aim to strengthen protection for banking customers or consumers. The agenda is to prepare a customer complaint mechanism, establish a banking mediation institution, increase transparency of product information and educate the wider community about bank products and services.

Of the several programs, the establishment of an ombudsman for banking consumers is something new for us because currently it is felt that there is no special institution that handles disputes between banks and bank consumers as in several other countries. In relation to the implementation of the six pillars of the Indonesian Banking architecture, at this time the following things have been done as forms or types of bank accountability:

a) The first pillar, is the main concern and has been formulated. This first pillar is basically a "rub" and reshaping process for the structure of the Indonesian banking industry. It includes directions regarding institutional aspects, ownership and operational patterns of a bank or group of banks, in order to achieve the vision and goals that have been set.
b) The second pillar, Bank Indonesia has determined that the preparation of various banking provisions must always be based on research (research-based) and refer to best practices and international standards. In addition, in the process of regulating banks, Bank Indonesia will always involve banking practitioners.
c) The third pillar, the development of an effective and independent supervision system is attempted to always be directed and in line with the principles of effective bank supervision from the 25 Basel Core Principles. In addition, so that bank supervision can run effectively. Bank Indonesia will conduct re-engineering in various aspects of supervision, in order to be able to apply a multi-risk supervision approach. Another step is to review the possibility of implementing consolidated supervision, preparing a bank supervisor certification program, and implementing Real Time Supervision.
d) The fourth pillar, that important issues that will be formulated for optimization steps include good governance, banking management information systems, intermediation functions, handling of problematic loans, implementing risk management and the ability of national banking to implement best practices such as Basel II provisions and anti-money laundering.
e) The fifth pillar, that the need for supporting infrastructure needs to be prepared for its existence, including rating agencies (Rating Agencies), Deposit Insurance Corporations (LPS), Credit Insurance, and the existence of Credit Bureaus) as debtor information centers and the use of adequate information technology. With the existence of these institutions, it is expected to have a positive impact on the performance of the banking industry.

f) The sixth pillar, that the need that is considered necessary to be prepared is a mechanism for handling bank customer complaints. Another problem that needs to be considered is efforts to empower consumers who use banking services. One way that is taken is in the form of transparency in providing complete information regarding banking products or services, including the potential risks faced by consumers or bank customers.

Forms of bank accountability towards customers who are victims of ITE crimes in the banking sector:

1. Form of Criminal Liability. Based on Law Number 7 of 1992 as amended by Law Number 10 of 1998, several aspects of banking crimes can be found, including those stated below in the form of:
   a. Collecting funds without a banking business license;
   b. Crimes concerning banking secrecy;
   c. Crimes concerning bookkeeping records and bank reports;
   d. Crimes of abuse of authority;
   e. Criminal acts of not implementing steps to comply with bank regulations;
   f. Misuse of credit cards;
   g. Criminal acts by affiliated parties (Article 50);
2. Form of Civil Liability. Bank customers are parties who use bank services, consisting of deposit customers and debtor customers. Depositors are customers who place their funds in the form of deposits based on a bank agreement with the customer concerned, while debtor customers are customers who obtain credit or financing facilities based on sharia principles or those that are equivalent to it based on a bank agreement with the customer concerned. As a customer, of course, they want their funds or accounts that are stored in the bank to be safe and can be received back in time. Therefore, they need protection. Forms of protection for depositors include:
   a) Approval of the appointment of leaders by the appointed institution.
   b) Determination of the cash ratio or reserve requirement.
   c) Capital adequacy or capital adequacy, which functions as an absorber of losses from bank activities on the asset side.
   d) Prevention of bank collapse which is carried out with the supervision of the central bank. This is to prevent bank panic, which can cause monetary instability.
   e) Announcement of bank balance sheets.

One basis that can be used to protect bank customers is security requirements that focus more on banking activities in general. Therefore, more specific and personal protection is needed for customers personally because customers understand banking products and services better. Provisions that provide such protection include provisions on the bank's obligation to provide information about bank products. This obligation is very important to provide clarity to customers about the benefits and risks associated with bank products so that they can protect themselves by refusing service requirements that have the potential to harm them.

Since banking activities are basically more civil, there are many principles of civil procedural law related to the banking business. One of the principles of civil law that is closely related to the banking industry is the principle of contract law. Since legal contracts are part of banking operations, the principle of contract law has become part of the discussion of banking legal principles.

CONCLUSION

Adequate legal protection for victims of crime is not only a national issue, but also an international one. Therefore, this issue needs serious attention. The importance of protecting victims of crime requires serious attention.

Legal protection for victims of crime is a form of protection of human rights or the legal interests of a person who should receive serious attention and it is important to expand the form

of protection, considering that today the forms of crime and their victims are so complex along with the advancement of civilization.

As an effort to implement the provisions of the Banking Law and the ITE Law, it must be supported by the professionalism of law enforcement officers who must be ready and understand the development of electronic crime, the community also plays an active role in overcoming all forms of crime that exist on the basis of self-awareness and being careful about all the conveniences of witnesses who use electronic facilities.

The author's suggestion is that banking institutions, in collaboration with consumer institutions, can jointly formulate agreement clauses that meet the needs of the parties and do not violate the elements of propriety, related to bank operations, banks periodically monitor employee behavior and indications of possible violations of the law. Given the customer's right to submit anything that is detrimental to them to the Customer Complaints and Banking Mediation Institution, the bank needs to provide an explanation regarding the customer's rights and, if necessary, include an agreement to mediate in the credit/financing agreement, as well as the depositor's savings account.

REFERENCE

Ronny Presetya, 2010, Pembobolan ATM, tinjauan hukum perlindungan nasabah korban kejahatan perbankan, PT. Pustaka, Jakarta.

Sudino Mertokusumo dan A. Pitlo, 1993, Bab- bab Tentang Penemuan Hukum, Cet I, PT. Citra Aditya Bakti.

Shinta Dewi, 2009, "Cyberlaw, Perlindungan Privasi Atas Jnform asi Pribadi Dalam £-Commerce Menurut Hukum Internasionaf', Widya Padjadjaran, Bandung.

Soerjono Soekanto, 1986, "Pengantar Penelitian hukum ", UI PRESS, Jakarta.

Soerjono Soekanto dan Sri Mamuji, 2004, "Penelitian Hukum Nonnatif, Suatu Tinjauan Singkat", PT Raja Grafindo Persada, Jakarta.

Sudarto, 1977, "Hukum dan Hukum Pidana", Jakarta.

_____, 1981, "Kapita Selekta Hukum Pidana", Alumni, Bandung.

Sunaryati Hartono, 1991, "Politik Hukum Menuju Satu Sistem Hukum Nasional, Cetakan Pertama ", Alumni, Bandung.

Sutan Remy Sjyahdeni, 2000, "Tindak Pidana Perbankan; Cours Materialpada Pasca Sarjana Rmu Hukum Universitas Indonesia", Jakarta.

_____, 2009, "Kejahatan dan Tindak Pidana Komputer ", Puataka utama Grafiti, Jakarta.

Sutan Zanti Arbi dan Wayan Ardhana, 1984, Rancangan Penelitian Kebijakan Sosial, Pustekkom Dikbud dan CV Rajawali, Jakarta.

Sutarman, 2007, "Cyber Crime, Modus Operandi dan Penanggulangannya", Laksbang Pressindo, Yogyakarta.

Suyud Margono, 2000, "ADR dan Arbitrase, Proses Pelembagaan dan Aspek hu/c:um ", Ghalia Indonesia, Jakarta.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

chromeextension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.mkri.id/public/content/infoumum/regulation/pdf/UUD45%20ASLI.pdf

Undang-Undang Negara Republik Indonesia Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang- Undang Negara Republik Indonesia Nomor 7 Tahun 1992 jo Undang- Undang No. 10 Tahun 1998 tentang Perbankan.

Undang-Undang Negara Republik Indonesia Nomlor 8 Tahun 2010 tentang Tindang Pidana Pencucian Uang.

Undang-Undang Negara Republik Indonesia Nomor 36 Tahun 1999 Tentang Telekomunikasi.

Undang-Undang Negara Republik Indonesia Nomor 13 Tahun 2006 Tentang Perlindungan saksi dan korban.

Undang-Undang Negara Republik Indonesia Nomor 30 Tahun 1999 tentang Arbitrase dan Altematif Penyelesaian Sengketa.

Undang-Undang Negara Republik Indonesia Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen.

Widodo, 2009, "Sistem Pemidanaan Dalam Cyber Crime, Alternatif Ancaman Pidana Kerja Social dan Pidana Pengawasan Bagi Pelaku Cyber Crime", Laksbang Mediatama, Yogyakarta.