www.bircu-journal.com/index.php/birci
Budapest International Research and Critics Institute-Journal (BIRCI-Journal)
Humanities and Social Sciences
ISSN 2615-3076 Online)
ISSN 2615-1715 (Print)
Budapest Institute

Legal Analysis of the Crime of Skimming in Indonesia According to the Electronic Information and Transactions Law (ITE) Number 11 of 2008 concerning Information and Electronic Transactions

Ervina Sari Sipahutar[1], Indra Gunawan Purba[2], Anjani Sipahutar[3]
[1,2,3]*Universitas Al-Azhar Medan, Indonesia*
Vina.sofyan@gmail.com, indrapurba07081978@gmail.com, anjanisipahutar1@gmail.com

Abstract

Crime in cyberspace presents new and serious problems on an international scale and is very complex in efforts to empower the law to deal with them. Economic crimes including Automatic Teller Machine (ATM) cards and theft of money are the second problem that is very worrying for the banking world, especially those committed by Asia. The legal situation in Indonesia, in particular, the laws and regulations made in the last twenty-five years is very easy to swallow. Objectively, this happens because changes in society in the political, economic, social, and cultural fields are going so fast, so that the law is easily left behind. Subjectively, various laws and regulations are made to overcome instant situations, so they pay less attention to insight. In reality, cyber activities (virtual world or the internet), are no longer simple, but quite complicated, because their activities are no longer limited by the territory of a country, which can be easily accessed anytime and from anywhere. Losses can occur, both to the perpetrator of the transaction and to other people who have never made a transaction, for example, the theft of bank customer funds through skimmer mode (procurement of Automated Teller Machines or so-called ATM cards). Advances in information technology that became the beginning of the existence of cybercrime, can legally have an impact on the law, which regulates this matter. Crimes like this can be categorized as acts of theft / fraud contained in the Criminal Code (KUHP) and Law no. 11 of 2008 concerning Information and Electronic Transactions, hereinafter referred to as UU ITE. Anyone in the city or village who already has an Automatic Teller Machine (ATM), especially in a big city, must have at least one plastic card with magnetic tape, which is often called an Automatic Teller Machine (ATM) card.

Keywords
Crime; skimming crime; information and electronic transactions (ITE)

I. Introduction

In the past, theft was carried out using fake keys. Today, computer equipment or automated tools, which are used to commit crimes. In this era of globalization, there are many information and communication technologies that are increasingly leading, almost a lot of technology and tools and electronics that appear and change models from time to time. We know various kinds of technological goods such as cellphones (HP), laptops, the internet and so on. Especially in today's sophisticated life, we are familiar with the Automatic Teller Machine (ATM). One of the weak points of ATMs that are targeted by crime is the mode of PIN theft or manipulating the customer's ATM card.

DOI: *https://doi.org/10.33258/birci.v5i2.4696*

Automatic Teller Machine (ATM) technology, makes it easier for customers of a bank to withdraw / withdraw cash stored in the bank without taking much time in the withdrawal process. However, the increasing velocity of money through Automatic Teller Machines (ATM) without realizing it in everyday life also appears various crimes. One of the weak points of the Automatic Teller Machine (ATM) which is the target of crime is the theft mode of Personal Identification Number (PIN) or manipulating the customer's Automatic Teller Machine (ATM) card. Take, for example, the case of bank burglary in Indonesia through the Automatic Teller Machine

(ATM), namely as in the case of Bank CIMB Niaga. This burglary case became a byword and hot discussion in various mass media at that time. And this is one form of technological crime, which can be called Cybercrime. This kind of thing is very difficult to disclose because it is carried out by criminals who have fairly high technological knowledge, with the technological knowledge possessed by these perpetrators, it is very likely that cybercrime perpetrators can see the customer's Personal Identification Number (PIN).

Retrieval of data needed by criminals, to steal customer funds through ATMs, perpetrators also use spycams or small recording cameras, which are inserted by the perpetrators in the Automatic Teller Machine (ATM) room, this spycam function is to record the pin number, which is pressed by the customer, when using an Automatic Teller Machine (ATM). After that, the perpetrator transferred the data in his possession to a new magnetic stripe card, resulting in the perpetrator having duplicated the Automatic Teller Machine (ATM) card used by the victim. A crime committed by the perpetrators by taking advantage of customers who took money at the Automatic Teller Machine (ATM).

The principle of this type of card is to store data on magnetic tape (an input/output device where information is entered into the CPU), which can then be read back using a device that has a reading device, such as a tape recorder, by means of friction. After the bank customer inserts his ATM card into the ATM machine, then this skimmer will record the data contained in the ATM card magnetic, the way the magnetic tape technology works on the card is basically, when swiped, the contents of the tape data are read, sent, translated and processed at the central side, to check the identity of the cardholder, the validity of the card itself and also the validity of the transaction.

Crimes in the banking sector, as well as the impact of economic crimes in the banking sector on the national economy, resulted in the emergence of victims. Victims of economic crimes in the banking sector, including customers who deposit funds, and the bank concerned. Theft of bank customer funds through ATM card procurement is one of the technological crimes in the banking sector. In fact, it has long been known together and there have been many cases. The incident was repeated together until the theft of 200 BCA Bank customers through ATMs, became known to the public.

Crime in cyberspace presents new and serious problems on an international scale and is very complex in efforts to empower the law to deal with them. Economic crimes including Automatic Teller Machine (ATM) cards and theft of money are the second problem that is very worrying for the banking world, especially those committed by Asia.

Theft of money through Automatic Teller Machine (ATM) cards and the internet, has often been revealed in the mass media in Asia, Asian nations need to work together with full commitment to deal with all forms of crime, old and new, in the worsening banking economy.

II. Research Method

The research method used in answering the above problems uses a normative juridical approach (legal research). Namely research that uses the nature of the research used is descriptive analytic (subject matter), in which the authors describe systematically the judicial review of the law of skimming crime in Indonesia. This research relates to Law NUMBER 10 YEAR 1998 on amendments to Law NUMBER 07 YEAR 1992, concerning Banking, Act No. 03 Year 2004 concerning amendments to Law of the Republic of Indonesia Number 23 Year 1999 concerning Bank Indonesia, Law Number 08 of 1999 concerning Consumer Protection, and ITE Law Number 11 of 2008 concerning Information and Electronic Transactions.

III. Result and Discussion

3.1 Skimming Crime Law Regulations in Indonesia Based on the Law of the Republic of Indonesia Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions

Theft of customer money through the skimming method is still common in Indonesia, for example the case that recently occurred in East Java. Some time ago, a number of customers of PT Bank Rakyat Indonesia Tbk (BRI) and PT Bank Mandiri Tbk became victims, as reported on the detikFinance page. The perpetrators of the skimming mode of customer money burglary are targeting big banks because big banks have ATM networks and a large number of customers in Indonesia.

Skimmingis one of the crimes in cybercrime where this crime is committed through a network of computer systems, both locally and globally, by utilizing technology by illegally copying the information contained on the magnetic stripe of the ATM card to have control over the victim's account. The perpetrators of this cybercrime have a high ability background in their field so that it is difficult to track and eradicate them completely.

Based on Article 32 paragraph (1) of Law no. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE) in the crime of breaking into ATMs with the skimming method there are offenses committed by the perpetrators, namely transmitting, destroying, eliminating, and transferring electronic information or electronic documents belonging to other people or the public due to the use of skimmers. The perpetrator transmits by sending electronic information from the victim's ATM to the ATM made by the victim perpetrators to be accessed and used to take the victim's money through an ATM machine. Article 363 paragraph (5) "theft is committed to enter the place of the crime or can reach the goods for retrieval, by dismantling, breaking or climbing or by using false keys, false orders, or false official clothes". The elements of article 363 paragraph (5) are:

1. Theft
   Theft is regulated in Article 362 of the Criminal Code which states as follows: "Anyone who takes something, wholly or partly belonging to another person, with the intention of being illegally owned, is threatened with theft, with a maximum imprisonment of five years or a maximum fine of six years tens of rupiah".
2. Items to pick up
   That what is meant by taking an item is when an item has moved from its original place with the aim of possessing the item.
3. By dismantling, breaking or climbing or by using false keys, false orders, or false official clothes.

That what is meant by dismantling, breaking or climbing, or using fake keys, false orders or fake clothes is not having rights, permits, or authorities and is contrary to what is justified by applicable law.

Article 32 paragraph (1) "everyone intentionally and without rights or against the law in any way changes, adds to, reduces, commits transmitting, destroying, eliminating, transferring, hiding, electronic information and or Electronic Documents belonging to other people or public property". Law No. 19 of 2016 concerning Amendments to Law No. 11 of 2008 concerning Information and Electronic Transactions (UU ITE). The elements are contained in Article 32 paragraph (1), namely:

a. Person

   Humans as legal subjects are supporters of rights and obligations, meaning that people can have legal rights and obligations. Man as a legal subject begins when he is born and ends when he dies. It can even be before birth (since in the womb) if the interests so desire, for example related to inheritance.

b. Purposely

   Deliberately means willing and knowing what he is doing or doing. The Criminal Code does not explain the meaning or definition of intentional or dolus intent opzet. But Memorie van Toelichting (Explanatory Memory) defines intentionality as wanting and knowing. Intentional must have the three elements of a criminal act, namely the prohibited act, the consequences of which are the main reasons for the prohibition, and that the act violates the law.

   An act that is against the law is an act that violates the subjective rights of others or that is contrary to the legal obligations of the maker himself which has been regulated by law. In other words, against the law is interpreted as against the law.

c. Damage

   Damaging is less than destroying, for example hitting glasses, plates, cups and so on, not to shatter, but only to break a little and crack.

d. Electronic transactions

   Electronic Transaction is a legal act carried out using a computer, computer network, and or other electronic media.

e. Electronic documents

   Electronic Document is any Electronic Information that is created, forwarded, sent, received, or stored in analog, digital, electromagnetic, optical, or similar forms, which can be seen, displayed, and/or heard through a computer or Electronic System, including but not limited to on writing, sound, pictures, maps, designs, photographs or the like, letters, signs, numbers, access codes, symbols or perforations that have meaning or can be understood by people who are able to understand.

Banking crimes and the threat of punishment can be charged under the ITE Law so that the police have a legal basis to take action to investigate and investigate ATM card crimes and other electronic transactions.

The legal basis for the skimming case which is currently rife is inseparable from the regulations regarding banking as stated in Article 1 number (1) of Law no. 7 of 1992 as amended by Law no. 10 of 1998 concerning Banking, Banking is everything related to banks, including institutions, business activities as well as methods and processes in carrying out their business activities.

A banking institution is a financial institution that bridges between parties who have excess funds and those who need funds, or is an institution that acts as a financial intermediary for the community (financial intermediary). Bank Indonesia as the supervisory agency for banking activities in Indonesia issued Bank Indonesia Regulation

No. 9/15/PBI/2007 concerning Determination of Risk Management. In the use of information technology in commercial banks, every bank that uses ATMs can minimize the risks that arise to get the benefits of ATMs. Therefore, commercial banks are required to prepare everything well, starting from the implementation of risk management in ATM activities effectively to planning for ATM operations and conducting periodic evaluations of ATM activities.

The operation of ATM cards is regulated in Bank Indonesia Regulation Number 11/11/PBI/2009 dated April 13, 2009 concerning the Operation of Card-Based Payment Instruments. However, with the recent skimming cases. The government, represented by Bank Indonesia, is currently trying and obliging all banks and card issuers to accelerate the migration of ATM cards from magnetic stripe to chip technology, with the switch to chips expected to reduce skimming cases in the future. This is confirmed in the Circular Letter of Bank Indonesia No. l7/52/DKSP dated December 30, 2015 concerning the Implementation of the National Standard for Chip Technology and the Use of a 6 (Six) Digit Online Personal Identification Number for ATM Cards and/or Debit Cards Issued in Indonesia.

Law No. 8 of 1999 concerning Consumer Protection stipulates legal protection for customer personal data contained in Article 4 Letter H, namely if a customer is proven to have been exposed to a skimming case at an ATM machine of a bank, the bank will compensate for the losses suffered by the customer. In this case, Bank Indonesia admitted that it had summoned the leadership of PT Bank Rakyat Indonesia (BRI) Persero Tbk to ask for an explanation regarding the number of skimming cases. Bank Indonesia said BRI had guaranteed to resolve the alleged skimming case. If it is proven that the mode used is skimming, BRI will replace all the lost customer funds.

3.2 Implementation of the Law Concerning Sanctions for the Crime of Skimming Crimes in Indonesia

a. Cybercrime Criminal Sanctions in the ITE Law

Legislation policy almost always uses criminal law to frighten or secure various kinds of crimes that may arise from various fields. This kind of phenomenon gives the impression as if it is felt to be imperfect or tasteless if a statutory product does not have a criminal stipulation. Therefore, as one of the central problems in criminal politics.

Criminal law sanctions should take a rational approach, otherwise it will lead to "the crisis of over criminalization" and "the crisis of overarching of criminal law" (crisis of over-criminalization and criminal law). The importance of this rational approach has been put forward by many criminal law experts and criminalologists, including: GP HOEFNAGGELS, KARL O. Cristhiansen, J Andenaes, McGrath WT, and W. Clifford.

The criminal sanctions stipulated in this law are set as sanctions in the form of imprisonment and fines. Two kinds of criminal law are set to a specific maximum only. This needs attention because there are weaknesses if only a special maximum is applied without a special minimum, because in practice it is possible that disparities will occur. Therefore, special minimum sanctions should also be accumulated considering that this cybercrime is not an ordinary crime that causes serious losses.

In addition, with the determination of the two types of punishment without any additional variations in the form of other crimes, for example criminal acts for corporations and also no less important, it is very necessary to regulate criminal compensation for victims through criminal law means. Because as developments in economic law have adopted compensation for victims in criminal matters as in the consumer protection law and the law governing other economic crimes. The position of the victim needs to be considered considering that the losses caused by the crime are not small.

In reality, it is not obvious that the victims of cyber crime are compared to victims of conventional crimes, but apart from the greater number of victims of cyber crimes, the impact is even more dangerous than conventional crimes. This means that this condition cannot be left alone, especially in the practice of law enforcement against these crimes.

All crimes must cause victims, a certain act is said to be evil, because someone is considered to have become a victim, including of course victims of cyber crime which includes individuals, groups of people or entities who have suffered or are victims of illegal activities. The loss can be physical, psychological, or economic. So far in Indonesia it is known that compensation is included in the field of civil law.

3.3 Obstacles in the Implementation of Sanctions against Skimming Crimes in Indonesia

a. Inhibiting Factors in Handling Skimming Crime

1. Obstacles from Law Enforcement

Law enforcement officials in the regions are not ready to anticipate the rise of this crime because there are still many police agencies in the area, both the Resort Police (polres) and the sector police (polsek), not yet equipped with internet networks. With such sophisticated technology, it is possible for crimes to be committed in one area but the consequences can occur in other areas, even abroad. Banking institutions, as well as insurance institutions, pension funds, and pawnshops, are financial institutions that bridge between those who have excess funds and those who need funds, or are institutions that act as financial intermediaries for the public (financial intermediary).

Apart from the inadequate tools used by law enforcement, in proving this skimming crime there are also obstacles because in handling skimming cases in Indonesia, skimming criminals are very observant and very adept at carrying out their actions, skimming criminals use their identities that are difficult to track down by law enforcers, besides using different identities, the perpetrators also have very sophisticated technological tools, exceeding the sophistication of the state apparatus. In law enforcement too.

2. Obstacles of investigators in uncovering the process of investigating criminal acts of theft through credit cards

According to the Criminal Procedure Code Number 8 of 1981, an investigator is a state police official of the Republic of Indonesia or certain civil servant officials who are given special authority by law to carry out investigations. In terms of what investigators do in conducting investigations against perpetrators of theft through credit cards, of course they experience obstacles, both internal and external factors.

a. Internal factors:

1) Human resources:

In carrying out the task of uncovering criminal cases of credit card theft at Polrestabes Surabaya, he experienced various obstacles in his human resources. Actually, the Surabaya Polrestabes police investigators have taken various steps to uncover cases of credit card theft cases. Investigators who are one of the elements of an investigation in the criminal justice system have qualification standards, in the case of the theft of the credit card. Special standards are needed for investigators who are familiar with banking secrets and banking matters and also who are aware of the theft of the credit card lack of skills, ability and tenacity as well as motivation to support the implementation of tasks, especially in the context of the process of investigating the Crime of Theft through Credit Cards. The barriers referred to regarding ability and creativity are still considered inadequate in handling the Crime of Theft through Credit Cards. This is because there is progress in the

times so that everything, both education in the quality of empowering knowledge, is growing and resulting in a more creative and neat level of evil or unlawful acts, which can be exemplified by falsifying names, addresses, ID numbers, to get original credit cards but all biodata is fake.

2) Facilities and infrastructure

Facilities and infrastructure are problems that always follow in terms of investigations carried out by investigators. Some sophisticated facilities are really very helpful for investigators in uncovering cases of credit card crimes, as well as sophisticated tools are very much needed for the process of investigating theft through credit cards, because in some cases investigators can't handle it because there are no tools that can be used. Sophisticated facilities along with the facilities that are fulfilled in the process of conducting investigations into criminal acts of theft via credit cards, become an inhibiting factor for investigators in uncovering criminal acts of theft via credit cards. Sophisticated tools are a very important factor in uncovering criminal investigations through credit cards.

b. External factors:

1. Lack of public understanding of the dangers of credit card crime the very lack of public understanding of the dangers of credit card crime makes credit card crime continue to grow rapidly as a result of the lack of understanding of the community, making the community itself the victim of credit card crime. The things that the community lacks understanding include:
   a. Ignorance of credit card users in providing photocopies of credit cards to those closest to them, but not understanding that the last 3 numbers are very vulnerable in committing credit card crimes.
   b. The inaccuracy of credit card users in seeing whether the machine
   c. EDC is connected to a skimmer (data tapping device).
   d. Lack of understanding of the community in transacting on the internet and not making sure in advance that the site is valid and safe.
2. The actor factor.

   The factor of actors who are not aware of the law is also an external obstacle experienced by investigators. And perpetrators who increasingly want to get a lot of results from these credit card crimes. By relying on the intelligence and intelligence and intellect of the perpetrators who are above average against other criminals, and are very well versed in rapidly developing technology, which is now a factor that greatly hinders investigators in uncovering investigations into criminal acts of credit card theft. as well as the many loopholes or opportunities that the perpetrators have because many people have now moved away from paying cash and using credit cards. Making it easier for perpetrators to carry out their actions in the credit card crime.

3. Investigators' efforts in dealing with obstacles in uncovering the criminal investigation process

a. Internal effort

1. Human resources

Investigators' efforts in dealing with obstacles in uncovering the investigation process, criminal acts of theft via credit cards, at the Surabaya Police Station are due to weak human resources, namely investigators at the Surabaya Police Station. So it is very necessary to hold, a special training for investigators who are at the Surabaya Polrestabes, specifically to handle cases of theft crimes through the credit card. besides that because of the breadth the Surabaya area as well as today's increasingly rapid and advanced technology, so that there are many gaps for the occurrence and development of crime through the credit card and one of the most effective ways is to hold special training for investigators who handle credit card crime cases at Polrestabes Surabaya.

3. Facilities and infrastructure

Facilities and infrastructure are the main things needed for investigators to investigate or resolve criminal cases of theft through credit cards because it is a means to improve the ability or skill of investigators to conduct examinations or searches of the Crime of Theft through Credit Cards. Likewise with the infrastructure that must be considered properly, for processes that require a building or a security that can guarantee the safety or confidentiality of each investigator to conduct an examination of the Crime of Theft through Credit. As well as an adequate budget is needed as a substitute for the preparation of facilities and infrastructure for wages for performance carried out by investigators.

Transactions at ATMs do not always run smoothly. Problems often occur, whether caused by the banking system or the negligence of the account owner himself. These problematic transactions often make us panic about the safety of the money in the account. In addition, it also causes our business to be delayed because we cannot make transactions at ATMs. Some examples of problems in transactions at the ATM include:

1. Blocked Card

   Personal Identification Number (PIN) is a series of combinations of numbers (6 digits) to be able to transact at ATM machines. If you enter the wrong card PIN number 3 times (three times), the banking system will protect it by blocking the card automatically. This is intended as an effort to prevent misuse of the card by others. If it is purely your negligence as the account owner, then you can report it to the bank office concerned to make a new PIN.

2. Swallowed ATM Card

   Have you ever had this happen? Makes you panic when it's over make a transaction, but you forget to end the menu selection and rush to leave the ATM booth, then in a matter of seconds the ATM machine will automatically swallow the ATM card so that it is not taken or misused by the person who will make the next transaction. Next, you have to make a report to the bank to block and issue a new ATM card.

3. Swallowed Money

   At the time of withdrawing cash, the money is swallowed back by the ATM machine. Similar to a swallowed card, this is automatic protection by the ATM machine because it takes too long to take money that has been out of the machine. Immediately make a report to the bank for correction of the refund to your account balance.

4. Money Doesn't Come Out or Balance Is Deducted

   Transactions like this sometimes occur because of problems in the banking system. Where when we have chosen a cash withdrawal transaction and the sound of a money counting machine is heard at the ATM machine, but it turns out that the money we are waiting for does not come out. Unfortunately, when we want to repeat the transaction, it turns out that the balance in the account has decreased. No need to panic. As with the incident of swallowing money earlier, you just need to make a report to the bank, and then the bank will return the money to your account after checking the correctness of the transaction. It's just that you have to be patient enough, because it usually takes a maximum of 14 working days from the time the report is received.

5. Transaction Cannot Be Processed

   After selecting the menu on the ATM screen, suddenly the words “Transaction Cannot Be Processed” appear on the ATM screen. You don't need to panic. There may be a connection/network interruption in the bank's IT system. If after trying it again it turns out that it is still the same, you should not have to force yourself to transact first rather than bad things happen.

3.4 Special Division for Skimming Handling

The Head of the National Police Public Relations Division, Inspector General Setyo Wasisto, said investigators could not reveal the ATM burglary syndicate using the skimming method in a short time. This crime is alleged to have been designed in such a way by a network that involves citizens of other countries. "Indeed, this is an organized crime. There are those who take data, print, sell, and take the money. ATM skimming is rampant, Jusuf Kalla Asks Banks to Improve the System Setyo said that the Police need more time to track down other perpetrators. This tracking effort is also being carried out through international cooperation with several countries, one of which is in the exchange of information and data. "We are pursuing the perpetrators of the repressive efforts. Now we have got several suspects and their evidence," said Setyo. The police asked the Immigration Office to tighten monitoring of foreign nationals entering Indonesia. Don't let the skimmer escape border security. Hacking mode with this skimmer is the old way. Setyo said he had uncovered a case of credit card fraud.

IV. Conclusion

1. The legal arrangement regarding the sanction of the crime of skimming in Indonesia is contained in the Republic of Indonesia Law Number 19 of 2016 concerning amendments to Law no. 11 of 2008 concerning Electronic Information and Transactions, the perpetrators of skimming crimes may be subject to the provisions of Article 30 paragraph (1), Article 30 paragraph (2), Article 32 paragraph (2), Article 36 paragraph 27 34 of Law Number 11 of 2008 in the ITE law explains that, any person who intentionally without rights or against the law in any way changes, adds, reduces, transmits, destroys, removes, transfers, hides an electronic information and or Electronic document of another person or public property will be punished for 6 (six) years and a fine of 1,000,000,000.00 (one billion) according to article 45.
2. There are 2 types of sanctions in criminal acts in sekimming in Indonesia, namely imprisonment and fines according to article 10 of the Criminal Code, the perpetrators of crimes are subject to a maximum of 6 (six) years and a maximum fine of 1,000,000,000.00 (one billion) which has been imposed or in articles 45, 45a and 45b in Law no. 11 of 2008 which has been amended in Law no. 19 of 2016 concerning Electronic Transaction Information
3. KThe obstacle in implementing sanctions for skimming crimes in Indonesia still has big obstacles, both state apparatus such as the police who are very difficult to uncover the perpetrators of crimes, because the perpetrators often change their identities, apart from that, the electronic devices used by police investigators are also inadequate, the technology of the perpetrators is more sophisticated than the state apparatus to the law enforcers it is very difficult to trap and arrest the perpetrators of skimming crimes in Indonesia. Apart from law enforcement officers, the sentence given is also very light, which is only 6 (six) years in prison according to Law no. 19 of 2016 article 45.

Suggestion

a. It is better to improve the human resources (HR) of law enforcement officials in the field of information technology, including police officers, prosecutors, judges and even lawyers, especially in dealing with cyber law issues. So that law enforcement in this field can be carried out properly with the support of qualified human resources and experts in their fields.

b. Use a password that is not identical to yourself or those around you. Like your own birthday, mother, or boyfriend. Because it will be very easy to know by others.
c. To IT experts, so that in making data security programs more optimal so that cases of cyber crime can be minimized.
d. Change the password regularly, so that it is difficult for others to know.
e. Do not carelessly conduct internet banking transactions on other people's computers. Because it could be that the computer has embedded a Key Logger that can store your password.
f. Always be careful in every transaction.

References

Abdul Wahid dan M. Labib. (2005). Kejahatan Mayantara (Cybercrime), (Bandung:

Abdul Wahid dan Mohammad Labib. (2005). Kejahatan Mayantara, Refika Aditama, Bandung,

Adami Chazawi. (2001). Pelajaran Hukum Pidana Bagian I, Jakarta: Raja GrafindoPersada, Yahya Harahap, Pembahasan Permasalahan dan Penerapan KUHAP Penyidikan dan Penuntutan Edisi Kedua, Sinar Graiika, Jakarta.

Ade Arie Sam Indradi. (2006). CardingModus Operandi, Penyidikan dan Penindakan, (Jakarta: Grafika Indah)

Barda Nawawi Arief. (2006). Tindak Pidana Mayantara Perkembangan Kajian Cyber Crime di Indonesia, Rajawali Pers, Jakarta.

Budi Suhariyanto. (2013). Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya, Rajawali Pers, Jakarta, hlm. 17.

Budi Suhariyanto. (2013). Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya, Jakarta: Rajawali Press
dan Penuntutan Edisi Kedua, Sinar Grafika, akana.

Dikdik M. Arief Mansur, Cyber Law Aspek Hukmn Teknologi Informasi, Reflka Aditama Bandung

Harahap Yahya. (2010). Pembahasan Permasalahan dan Penerapan KUHAP Penyidikan

Muhamad Djumhana. (2008). Asas-asas hukum perbankan Indonesia, PT citra Aditya bakti, Bandung.

Muhammad Djumhana. (2008). Asas-Asas Hukum Perbankan Indonesia, Bandung: PT Citra Aditya Bakti.

PAF Lamintang. (1984). Kitab Undang-Undang Hukum Acara Pidana dengan Pembahasan Secara Yuridis menurut Yurisprudensi dan Ilmu Pengetahuan Hukum Pidana, CV.Sinar Baru, Bandung. Refleksi Ketidakberdayaan Hukum dan Penegakan HAM, Cet I, Jakatta: Edsa Mahkota.

Pasal 143 ayat (2) huruf b Undang-Undang Nomor 8 Tahun 1981 tentang Kitab Undang-Undang Hukum Acara Pidana

Peraturan Bank Indonesia Nomor 11/ 1 1/PBI/2009 tanggal 13 April 2009 tentang Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu Surat Edaran Bank Indonesia No. 17/52/DKSP tanggal 30 Desember 2015 tentang Implementasi Standar Nasional Teknologi Chip dan Penggunaan Personal Identification Number Online 6 (Enam) Digit untuk Kartu ATM dan/atau Kartu Debet yang Diterbitkan di Indonesia

Prasetyo, Roni. (2004). Tinjauan Hukum Perlindungan Nasabah Korban Kejahatan Perbankan, (Jakarta, Prestasi Pustaka).

Rahaljo Satjipto. (1980). Hukum dan Masyarakat, Cetakan Terakhir, Angkasa.Bandung.

Refika Aditama).
Rehulina, Hatialum. (2012). Analisis Yuridis Kejahatan Cyber Crime Dalam Pembobolan Mesin Atm Bank, (Surabaya).
Republik Indonesia, Pasal 32 ayat 1 Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik merupakan perubahan dari Undang - Undang Republik Indonesia Nomor 11 Tahun 2008
Sudarto. (1986). Hukum dan Hukum Pidana, Alumni, Bandung, hlm. 113.
Sunardi, Danny Tanuwijaya. (2005). Abdul Wahid, Republik "Kaum Tikus";
Undang-Undang Republik Indonesia Nomor 10 Tahun 1998 Perubahan atas Undang-Undang Nomor 7 Tahun 1992, Tentang Perbankan.
Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik merupakan perubahan dari Undang-Undang Republik Indonesia Nomor 11 Tahun 2008.
Undang-Undang Republik Indonesia Nomor 3 Tahun 2004 tentang Perubahan atas Undang – Undang - Undang Republik Indonesia Nomor 23 Tahun 1999 Tentang Bank Indonesia.
Undang-Undang Republik Indonesia Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.