LEGAL PROTECTION TO BANK CUSTOMERS AGAINST MALWARE TROJAN IN INDONESIA

Steinly Liwong

Abstract

The purpose of this research is to describe clearly about the legal protection in the existing laws and regulations in Indonesia particularly about legal protection toward bank customers or consumers which domiciled in Indonesia against cybercrime which in this research focused on Malware Trojan attacks. This research also aims to know what are the rights and obligations of financial service business which in this research, financial service business known as banks who provided internet banking services so could be use by their consumers which known as bank customers.

This research is using normative legal research method with qualitative data analysis method. This research is using primary data and secondary data which the data based on the library research and the interview results which only as an additional to support this research. After all data have been collected, these data will be analyzed.

According to this research, it explained that the existing laws and regulations in Indonesia are not really effective to give legal protection especially for the bank customers and banks. Aside from that, banks as the financial service business and customers as the consumers are not doing their obligations which have been ruled in the existing laws and regulations in Indonesia.

Keywords: *Protection, Customers, Malware Trojan, Indonesia*

A. Background

Financial institutions who are banks in common, in their services they prefer the face to face service method and based to paper document for the sake of customers' safety and convenience on their transaction.[1]

In the reformation era, paper document based transactions have been difficult to be implemented which have been switched to the utilization of information technology. This information revolution was called as internet banking. Internet banking facility was designed by the banks as good as possible to give a good service quality to the customers to ensure them that by using internet banking their transactions was done easier, faster, more convenience, more accurate, cheaper and so on.

Aside from the conveniences of using internet banking, definitely there are negative impacts that may happen today or even in the future, such as smuggling, piercing, fraud, carding, cybercrime, cracking, and so on.[2]

Indonesia in 2016 has about 258.316.051 (two hundred fifty eight million three hundred sixteen thousand fifty one) population[3] and for people who are using internet banking itself in 2015, around 13.300.000 (thirteen million three hundred thousand) or about 6 % of the whole population [4] which made Indonesia as the one of the targeted countries by the criminals to do the crime.

Regional Police of Kepulauan Riau stated that the amount of cybercrime generally for cases which inflict a financial loss in banking sector

---

[1] Landasan Teori, "*Pengertian Internet Banking Tujuan dan Manfaat Sistem Keamanan Untuk Nasabah Menurut Para Ahli*" http://www.landasanteori.com/2015/10/pengertian-internet-banking-tujuan-dan.html, accessed on 30th April 2016.

[2] Dudung, 2015, "*20 Dampak Positif dan Negatif Teknologi Informasi di Bidang Ekonomi*" http://www.dosenpendidikan.com/20-dampak-positif-dan-negatif-teknologi-informasi-di-bidang-ekonomi/, accessed on 30th April 2016.

[3] Internet World Statistics, "The World Population and The Top Ten Countries with The Highest Population" http://www.internetworldstats.com/stats8.htm, accessed on 8th December 2016.

[4] USSI, 2016, "*Akankah* Financial Tech *Menggeser Perbankan Konvensional*?" http://ussi-software.com/blog/2016/06/09/akankah-financial-tech-menggeser-perbankan-konvensional/, accessed on 8th December 2016.

total around 103 (one hundred and three) to 120 (one hundred twenty) cases in a year in the period last five years since 2010 until 2015.[5]

In March 2015, a cybercrime happened on BCA Bank where a BCA Bank's customer admitted that his/her bank's account has been smuggled after he/she failed repeatedly from doing transaction on BCA Internet Banking. He/she founded that her funds in his/her account were reduced for Rp. 13.000.000,- (thirteen millions rupiah).[6] This case also happened on Mandiri Bank on 8th April 2015 where a customer of Mandiri Bank was using Mandiri's internet banking has lost for Rp. 40.000.000,- (forty millions rupiah).[7]

President Director of BCA Bank named Jahja Setiaatmadja said that this token synchronization case happened was due to a viruses or malwares that attacked on customer's personal computer.[8] At the moment banks only could mediation to the funds receiver of token synchronization case, but the bank itself does not guarantee that those lost funds are return to the customer.[9]

According to Article 19 in the Indonesian Law Number 8 of 1999 concerning Consumer Protection banks as the service providers of internet banking have to give compensation to the customers which were loss due to

---

[5] Delfind Kiweikhang, "*Tinjauan Yuridis Penanganan Kejahatan Siber* (Cyber Crime) *di Sektor Perbankan Indonesia dan Amerika*," (Undergraduate Final Project Universitas Internasional Batam, Batam, 2015), pg. 46.

[6]Yoga Sukmana, 2015, "*BCA Minta Nasabah Waspadai "Sinkronisasi Token" Saat Membuka* Internet Banking"
http://bisniskeuangan.kompas.com/read/2015/03/04/144553726/BCA.Minta.Nasabah.Waspadai.Sinkronisasi.Token.Saat.Membuka.Internet.Banking, accessed on 6th May 2016.

[7] HowMoneyIndonesia, "*Uang Hilang Setelah Sinkronisasi Token di Internet Banking Bank Mandiri*" https://howmoneyindonesia.com/2015/04/09/uang-hilang-setelah-sinkronisasi-token-di-internet-banking-bank-mandiri/, accessed on 6th May 2016.

[8] Stefanno Reinard Sulaiman, 2015, "*BCA: 1000 Nasabah Terkena "Sinkronisasi Token" Saat Akses* Internet Banking"
http://bisniskeuangan.kompas.com/read/2015/03/06/061800526/BCA.1.000.Nasabah.Terkena.Sinkronisasi.Token.saat.Akses.Internet.Banking, accessed on 12th May 2016.

[9] Ika Suryani Syarief, 2015, "*Situs BCA Terserang Virus? Nasabah Kehilangan Rp18,9 Juta*" http://www.suarasurabaya.net/print_news/Kelana%20Kota/2015/156303-Situs-BCA-Terserang-Virus?-Nasabah-Kehilangan-Rp18,9-Juta, accessed on 6th May 2016.

the usage of internet banking which provided by the banks. But in the reality there are still more customers did not manage to get their money back safely or the banks could not do much to help those customers either.

According to the background above, there are some issues appealed in this research which are, **first**, what laws that could be imposed to handle Malware Trojan cases in Indonesia? **Second**, how do banks protect their customers against Malware Trojan attacks? And the **third**, what efforts could bank customers do to deal with Malware Trojan attacks?

B. Research Methodology

This research used normative legal research. This research contains of several types of data which are primary data which including in-depth interview and unstructured observation and secondary data which including of primary legal materials, secondary legal materials and tertiary legal materials.

First, primary legal materials gathered from several sources of law, which are Indonesian Civil Code, Indonesian Criminal Code, Indonesian Law Number 8 of 1999 concerning Consumer Protection, Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions, Indonesian Law Number 21 of 2011 concerning Financial Services Authority, Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation, and Regulation of Financial Services Authority Number 1/POJK.07/2013 concerning Consumer Protection Financial Service Sector. ***Second***, secondary legal materials contains mostly of library collections which consists of books, reports, and internet-based sources. ***Third***, tertiary legal materials in this research are mostly from English Oxford dictionary.

The data which have been mentioned above were analyzed with descriptive qualitative data analysis method. The steps to analyze data are

conducted based on data collection, data classification and analyzation, and the conclusion which refer to the data analyzation.

C. Research Findings and Discussions

1. Laws that could be imposed to handle Malware Trojan cases in Indonesia

Malware Trojan has caused the bank's customers or internet banking users have lost of quite a lot of money which was the main intention of the criminal. Therefore in Article 362 Indonesian Criminal Code, the criminal could be punished for a maximum imprisonment of five years or a maximum fine of sixty rupiahs. Malware Trojan has caused lots of people have to believe to do the transaction on the fake website could be punished by a maximum imprisonment of four years according to Article 378 Indonesian Criminal Code.

Creating a Malware Trojan to fraud people which besides the purpose to steal their money is to get the user ID and password of the internet banking user, the criminal fulfills the element which stated in Article 30 section (2) and (3), and Article 31 section (1) and (2) Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions. Therefore the criminal could be punished as what have stated in Article 46 section (2) and (3), and Article 47 Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions which overall the criminals should be punished not exceeding 10 (years) imprisonment and/or a fine not exceeding Rp. 800.000.000,- (eight hundred million rupiah). As for the couriers could be punish for Article 55 Indonesian Criminal Law.

It is not including the other law that the criminal broke such as Indonesian Law Number 11 of 2008 concerning Electronic

Information and Transactions which if the time of imprisonment summed, the total could reach above 20 (twenty) years which was forbid by Article 12 section (4) Indonesian Criminal Code which stated that: "In no case the term of twenty years may be exceeded."[10]

Moreover, after based on the Bareskrim investigation on one of the token synchronization cases, the criminal was not from Indonesia, but from Ukraine instead, therefore the criminal could not be punished using Indonesian laws and regulations according to Article 2 Indonesian Criminal Law which stated that: "The Indonesian statutory penal provision are applicable to any person who is guilty of a punishable act within Indonesia." This could be known as territoriality principal.

To decide what laws suitable for the criminal if based on the situation and condition are the laws that related to international laws or international agreement laws which will not be explained further because this research is more focused on the legal protection efforts from the banks to their customers or internet banking users, not about the government efforts to handle token synchronization cases and the criminal.

Article 1365 Indonesian Civil Code stated that: "Every unlawful act that causes damage onto another person obliges the wrongdoer to compensate such damage." A bit different with what have been stated in Article 19 section (1) and (2) Indonesian Law Number 8 of 1999 concerning Consumer Protection which stated that businessmen should be responsible to give compensation such as refunding which of one kind or equals to their value towards consumer

[10] Indonesia Criminal Code, Article 12 section (4), http://defensewiki.ibj.org/images/b/b0/Indonesia_Penal_Code.pdf, downloaded on 23rd November 2016.

loss caused by consuming internet banking services which have been produced by the banks.

According to Article 19 section (3) Indonesian Law Number 8 of 1999 concerning Consumer Protection should be within 7 (seven) days after the transaction date. But the fact is the customers have to wait for more than 7 (seven) days for the bank since they already knew that the case would be token synchronization case but still take more than 7 (seven) days to investigate the case by the banks.

To prove if the bank should responsible or not is depend on the bank's responsible to verify or to prove it. In Indonesian Law Number 8 of 1999 concerning Consumer Protection, a law principle applied in this law which is Reversal Burden of Proof or *Omkering van het Bewijslast* which means that the burden of proof was not on the customers who consuming or using the goods and/or services, but to the businessmen instead. Reversal Burden of Proof was stated in Article 28 Indonesian Law Number 8 of 1999 concerning Consumer Protection.

On the legal point of view, the laws in Indonesia supposed to adopt and go along with progressive law theory where means a liberation movement because it tends to be fluid and always agitate in searching from one truth to the next truth, which for example like Indonesian Civil Code, Indonesian Criminal Code and Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions.

Indonesian Civil Code released since 1848[11] and Indonesian Criminal Code released since 1958[12] which means Indonesian Civil

[11] Sudut Hukum, 2015, "*Sejarah KUH Perdata (BW)*", http://www.suduthukum.com/2015/08/sejarah-kuh-perdata-bw.html, accessed on 27th December 2016.

Code and Indonesian Criminal Code have outdated for some reasons.

Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions was released since 2008 and Malware Trojan is a kind of new criminal act that has not been regulated inside it and it does not regulate how is the legal protection towards the user who using electronic to do transactions.

To handle token synchronization cases, there are some limitations that the police officers who as the law enforcers had due to some reasons according to the results of this research, which are:

a. Legal foundation

Legal foundation is the reference for the police officers to handle cybercrime which for now still using Indonesian Criminal Law, even though Indonesian Criminal Law is not effective anymore. The sanctions in Indonesian Criminal Law are not balance with the effect of cybercrime. According to Barda Nawawi Arief, criminal law has limitations to handle crimes, which are:[13]

1) Complexity for reasons of crime which are out of range from criminal law;
2) Criminal law just a small part (subsystem) from a tool of social control;
3) Using criminal law to handle crimes is just a symptomatic therapy and not a causative therapy;

[12] Badan Pembinaan Hukum Nasional (BPHN), "*Sejarah KUHP*", http://hukumpidana.bphn.go.id/sejarah-kuhp/, accessed on 27th December 2016.

[13] Shinta Septiana Dewi, "*Upaya Pemerintah Indonesia dalam Menangani Kasus Cybercrime (Studi Kasus Cyberporn di Indonesia)*". Ilmu Hubungan Internasional. Vol 1 No 2, 2013, pg. 394, downloaded on 17th February 2017.

4) Criminal law sanctions are *remedium* which contained contradictive character and negative side effects; and etc.

b. Uneven cybercrime police unit

In the police organization, there is a unit called as Reserse which their function is to do investigation special crimes especially the investigation which related to the information technology, telecommunication, and electronic transaction. Not only Reserse, there is also Special Economic Crimes Directory (*Dirtipideksus*). But unfortunately, not all parts of Indonesia have this kind of police unit which made some area have difficulties to solve the cybercrime case. As an example, Makassar does not have any police unit which to handle cybercrime.[14]

c. Human resources

Indonesian police officers in facing cybercrime threat, they realized that the resources should be fixed or upgraded considering the number of crimes in the future will increase neither quantity nor quality.

d. Technology system

Technology improvements influence in cybercrime verification[15], which verification is a very important factor which considering that electronic information has not been accommodated in the Indonesian criminal procedural law.[16]

e. Low awareness of the law

[14] Riskawati, "*Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar*)", pg. 102, downloaded on 17th February 2017.
[15] *Ibid.*, downloaded on 17th February 2017.
[16] I Made Agus Windara & AA. Ketut Sukranatha, "Kendala dalam Penanggulangan Cybercrime Sebagai Suatu Tindak Pidana Khusus", pg. 4, downloaded on 17th February 2017.

Indonesian society who lack of understanding cybercrime as crime[17], will lead the awareness to report the case to the police are low.[18]

Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions is the only cyber law that existed in Indonesia which according to the modern viewpoint, the existing laws in Indonesia are not complete, which the laws could not cover all legal events that happened in society.[19]

Hacking clause in Indonesian Law Number 11 of 2008 concerning Electronic Information and Transactions is not suitable for handling token synchronization cases because the process of criminal acts are totally different. Hacking is the gaining of access (wanted or unwanted) to a computer and viewing, copying, or creating data (leaving a trace) without the intention of destroying data or maliciously harming the computer. [20] While token synchronization is to synchronize between the token's PIN and the user ID by using Malware Trojan, not destroying data or even harming the computer.

Due to the legal vacuum, the judge could do legal founding as the best way to handle the case which according to Article 5 section (1) Indonesian Law Number 48 of 2009 concerning Judicial Power stated that the judge and the constitution judge have to dig, follow and to understand the legal values and the sense of justice in the society, which means that the judge should have an ability to do *Rechtvinding*

[17] Riskawati, *op.cit.*, downloaded on 17th February 2017.
[18] Shinta Septiana Dewi, "*Upaya Pemerintah Indonesia dalam Menangani Kasus Cybercrime (Studi Kasus Cyberporn di Indonesia)*". Ilmu Hubungan Internasional. Vol 1 No 2, 2013, pg. 401, downloaded on 17th February 2017.
[19] Kementrian Hukum dan Hak Asasi Manusia Republik Indonesia, "Penemuan Hukum Oleh Hakim (Rechtvinding)", http://ditjenpp.kemenkumham.go.id/umum/849-penemuan-hukum-oleh-hakim-rechtvinding.html, accessed on 13th January 2017.
[20] Urban Dictionary, "Hacking", http://www.urbandictionary.com/define.php?term=hacking, accessed on 19th February 2017.

as what as Paul Schalten has stated.[21] In this condition, the most suitable legal founding method is law construction with law constriction which Malware Trojan or token synchronization case is a special legal relationship which has not been regulated in the laws, so the judge could implement some general regulations to the case with explanation by giving the characteristic of it.

The existing laws in Indonesia were not functioning repressive legal protection theory well which according to the theory the law is aiming to solve the case based with human rights concept, but the reality is the existing laws are not really effective to be implemented the case which the case unsolved efficiently and harmed Indonesian Bank's customers' or internet banking users' right to have legal protection towards Malware Trojan attacks and their money. As for the preventive legal protection theory, Indonesian laws and regulations could prevent cybercrime cases such as hacking, cracking, carding, etc., but could not prevent Malware Trojan or token synchronization cases in the future.

The existing laws in Indonesia also have been outdated which are not as fluid as what progressive law theory supposed to. Along with the time goes on, technology keeps getting more developments and creating some phenomenon or legal events that not regulated in the existing laws. As what as Satjipto Rahardjo's theory about progressive law theory which stated that the law should be for human, not human for the law, he also stated that the law should be fluid and always agitated in searching from one truth to the next truth.

[21] Kementrian Hukum dan Hak Asasi Manusia Republik Indonesia, *op.cit.*, accessed on 13th January 2017.

2. Banks' efforts to protect their customers against Malware Trojan attacks

Token synchronization case could be happen besides from the weaknesses of the bank's system, also could be the internal system problem which controlled and monitored by the bank's server operator which could lead the criminal to do criminal acts which could make a big loss to its customers.

In the BCA Bank's system, Fidelis Harefa as an IT expert believed that the server operator in BCA Bank could be also the one who involved on this token synchronization case too according to his research. The server operator against the rule in Article 28 section (1) Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation which explained that each person who works in the electronic systems operation must secure and protect structure and infrastructures of electronic systems or information transmitted through the electronic system.

According to Article 1 section (4) Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation, bank is the electronic system operator because bank is the one who provide, manage and/or internet banking system. Article 27 Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation stated that electronic system operator is obligated to protect its users and the public from harm caused by its operation of electronic systems.

The statement in Article 27 Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation also supported by Article 25

Regulation of Financial Services Authority Number 1/POJK.07/2013 concerning Consumer Protection Financial Service Sector which stated that financial services business (banks) obligated to make customers' savings, funds, or assets safely which in the responsibility of financial services business.

According to the interview results and personal experience towards token synchronization case, the bank did not explain about the procedure and the risks of using internet banking to the customers which against the rule that regulated in Article 24 section (1) Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation explained that the electronic system operator (banks) shall conduct training about electronic systems to users which at least about the rights, obligations and responsibilities of all parties involved, and the procedures for filing a complaint which stated in the section (3).

In Article 25 letter (c), (d), and (g) Regulation of the Government of the Republic Indonesia Number 82 of 2012 concerning Electronic System and Transaction Operation more explained more about conduct training which stated in Article 24 of this regulation stated that electronic system operator (banks) shall submit information to the electronic system user for at least capability or safety of electronic systems, procedures to use of the device, and guarantee of the privacy and/or protection of personal data. Therefore, according to the rules, the bank has to protect its customers by educating them all information related to internet banking usage and its risks.

Due to the bank did not educate the customers about internet banking usage and its risks, the consumers or internet banking users according to Article 4 letter (d) Indonesian Law Number 8 of 1999 concerning Consumer Protection have the right to being accepted the

consumers' opinion and complaint towards the goods and/or services which the consumers have been using them.

Therefore in Article 38 Regulation of Financial Services Authority Number 1/POJK.07/2013 concerning Consumer Protection Financial Service Sector stated that after financial services businessmen (banks) received complaints, they have to:

a. internal examination of the complaints with competent, truth, and objective;
b. analyze to find out the truth of the complaints; and
c. send apologizes and to offer compensation (redress/remedy) or repair products and/or services, if the consumers' complaints are true.

In order to give compensation to the customers, *Lex specialis derogat legi generalis* principle applied which Article 38 Regulation of Financial Services Authority Number 1/POJK.07/2013 concerning Consumer Protection Financial Service Sector is one of the specific regulations will rule out Article 7 Indonesian Law Number 8 of 1999 concerning Consumer Protection which is more general.

After giving compensation to the customers, the banks should investigate their system weaknesses and try to increase their internet banking system's security as on 9th March 2015, Deputy Commission Supervisor of Financial Services Authority, Irwan Lubis stated that Financial Services Authority has asked and told the banks to increase their internet banking's security. [22] Lack of attention towards the internet system's security could cause the managed sites attacked,

[22] Benedictus Bina Naratama, 2015, "*Ini Modus Pembobolan Rekening Lewat e-Banking*" http://nasional.kontan.co.id/news/ini-modus-pembobolan-rekening-lewat-e-banking, accessed on 6th October 2016.

infiltrated, and injected dangerous virus easily.[23] There are some methods that banks could do to secure the internet based system, which are:[24]

a. Access control;
b. Closing the unused service;
c. Install protection;
d. Firewall;
e. Attacks monitors;
f. System's integrity monitors;
g. Audit;
h. Routine back up;
i. Encryption; and
j. Telnet or safety shell.

But even a computer system has secured by several methods above, but it is also not a guarantee the computer system totally secured from hacker, cracker, etc., therefore to reduce the possibility to be attacked, could be done by follow the safety procedures including accuracy and actuality development of internet system's security always should be followed.

According to the description above, *caveat venditor* is the most suitable law principle which means that sellers have to beware towards the marketed goods and/or services. The sellers have to find out the weaknesses and the possibilities of the bad effects that could be happen in the future after using their products.

Aside from just increase the system security, the banks also could increase their awareness from fraud people who keeps opening

[23] Agus Raharjo, *Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, (Jakarta: PT. RajaGrafindo Persada, 2002), pg. 250.
[24] *Ibid.*, pg. 252-258.

account frequently or by implementing Know Your Customer (KYC) method considering the couriers from token synchronization cases are easily to open the accounts in the banks. KYC policy is an important step developed globally to prevent identity theft, financial fraud, money laundering and terrorist financing and the objective of KYC is to enable banks to know and understand their customers better and help them manage their risks prudently.[25]

KYC could help banks to prevent the couriers to open an account because KYC controls about:[26]

a. Collection and analysis of basic identity information ("Customer Identification Program" or CIP);
b. Name matching against lists of known parties;
c. Determination of the customer's risk in terms of propensity to commit money laundering, terrorist finance, or identity theft;
d. Creation of an expectation of a customer's transactional behavior; and
e. Monitoring of a customer's transactions against their expected behavior and recorded profile as well as that of the customer's peers.

The law that existing in Indonesia such as Indonesian Law Number 8 of 1999 concerning Consumer Protection functioned pretty well with preventive legal protection theory. Preventive legal protection is aiming to prevent conflicts that might happen in the future by using rules or regulations. As what have been explained in Indonesian Law Number 8 of 1999 concerning Consumer Protection,

[25] It's All About Money, "Know Your Customer (KYC) – What Is KYC? What Documents Are Required?, http://www.itsallaboutmoney.com/did-you-know/what-is-kyc-what-documents-are-required-2/, accessed on 20th February 2017.
[26] *Ibid.*, accessed on 20th February 2017.

the seller has to beware of the risks that could appear of selling and distributing the products.

Though the law has functioning preventive legal protection theory, but the fact is the banks did not apply the preventive efforts to the customers by educating them about the terms and conditions including the risks that might the customers experience them before help applying internet banking for the customers.

3. Efforts that bank customers could do to deal with Malware Trojan attacks

According to the chronological cases, all of the customers that involved to token synchronization case did not aware of the Malware Trojan attack which by displaying an additional pop-up. The fact is the customers were believed that the pop-up was originally from the bank and without thinking much the customers just inputted all the data as what have been required on the pop-up.

This is a serious concern for all bank customers to be more careful in consuming or use the facilities or services that provided by the bank. Article 5 letter (a) Indonesian Law Number 8 of 1999 concerning Consumer Protection stated that consumers obligated to read or follow the instructions and procedures of using goods and/or services for safety while this article acknowledge *caveat emptor* principle. *Caveat emptor* means that consumers should be aware from the possibilities of defected goods and/or services before using or consuming them.

There is one method that could the customers use to more aware of notification by e-mail from the bank in the future which informing certain transactions even the customers did not do them, such as information of destination account registration, information of

delay transaction registration, and information of succeeded transactions.

There are other methods that could be done to minimalize malware attack in browser, which are:[27]

a. Use a personal computer and trusted connection to access internet banking;
b. Complete the personal computer with an updated antivirus;
c. Avoid download file from untrusted websites;
d. Aware from the unusual information requests, such as request to input a token code to the pop-up; and
e. Contact the official call center immediately if there is any suspicious notification from the bank.

Indonesian Law Number 8 of 1999 concerning Consumer Protection functioned pretty well with preventive legal protection theory which forced the consumer has to beware of the risks that could appear from consuming or using the products or services. As for the repressive, Indonesian Law Number 8 of 1999 concerning Consumer Protection have mentioned that bank customers could take this case to the Settlement of Consumer Disputes Organization, in Indonesian known as BPSK.

Indonesian Law Number 8 of 1999 concerning Consumer Protection has been outdated and not functioning progressive law theory because the law does not follow the developments which have been implemented in Indonesia. For an example, there is no regulation related to electronic transaction which regulate about the rights and the obligations of the consumers if they do the transactions via electronics.

[27] Otoritas Jasa Keuangan (OJK), 2015, "*Buku Bijak Ber-eBanking*", http://www.ojk.go.id/Files/box/buku%20bijak%20ber-ebanking.pdf#search=malware, downloaded on 19th January 2017

D. Conclusion

After the elaboration and in-depth discussion previously, there are some conclusions that could be concluded on this research with the title of "Legal Protection to Bank Customers against Malware Trojan in Indonesia" follows:

1. Mainly the token synchronization case were not the customers and the banks fault, but because there is cybercrime motive which done by a foreigner and use some couriers from Indonesia. Indonesia have some existing laws that could be imposed to against Malware Trojan or synchronization cases, but all of the laws have been outdated and not effective enough to solve the cases as what the legal protection theory and progressive law theory told so;
2. The bank did not apply some existing laws and regulations to protect their customers and did not apply *caveat venditor* law principle. Therefore, the bank should give compensation to the customers according to existing laws in Indonesia; and
3. Bank's customers did not do the *caveat emptor* principle or did not aware of the unusual transactions on internet banking which caused the token synchronization case happened.

Bibliography

Books and Journals

Dewi, Shinta Septiana, "*Upaya Pemerintah Indonesia dalam Menangani Kasus Cybercrime (Studi Kasus Cyberporn di Indonesia)*", *Ilmu Hubungan Internasional*, Vol. 1, No. 2.

Raharjo, Agus. 2002, *Cybercrime Pemahaman Dan Upaya Pencegahan Kejahatan Berteknologi*, Jakarta: PT. RajaGrafindo Persada.

Riskawati. "*Penanganan Kasus Cyber Crime di Kota Makassar (Studi pada Kantor Kepolisian Resort Kota Besar Makassar*)".

Windara, I Made Agus & AA. Ketut Sukranatha. "*Kendala dalam Penanggulangan Cybercrime Sebagai Suatu Tindak Pidana Khusus*".

Undergraduate Final Project

Kiweikhang, Delfind, 2015, *Tinjauan Yuridis Penanganan Kejahatan Siber (Cybercrime) di Sektor Perbankan Indonesia dan Amerika*, Undergraduate Final Project, Law Faculty Universitas Internasional Batam, Batam.

Laws and Regulations

Indonesian Civil Code.

Indonesian Criminal Code.

Indonesian Law Number 8 of 1999 concerning Consumer Protection.

Indonesian Law Number 11 of 2008 concerning Electronic Information and Transaction Law.

Regulation of the Government of the Republic Indonesia concerning Electronic System and Transaction Operation. Number 82 of 2012.

Financial Services Authority, Regulation of Financial Services Authority concerning Consumer Protection Financial Service Sector. Number 1/POJK.07/2013.

Internet Websites

Badan Pembinaan Hukum Nasional (BPHN). "*Sejarah KUHP*", http://hukumpidana.bphn.go.id/sejarah-kuhp/. Retrieved on 27th December 2016.

Dudung. "*20 Dampak Positif dan Negatif Teknologi Informasi di Bidang Ekonomi*" http://www.dosenpendidikan.com/20-dampak-positif-dan-negatif-teknologi-informasi-di-bidang-ekonomi/. Retrieved on 30th April 2016.

HowMoneyIndonesia, "*Uang Hilang Setelah Sinkronisasi Token di Internet Banking Bank Mandiri*" https://howmoneyindonesia.com/2015/04/09/uang-hilang-setelah-sinkronisasi-token-di-internet-banking-bank-mandiri/. Retrieved on 6th May 2016.

Internet World Statistics. "The World Population and The Top Ten Countries with The Highest Population" http://www.internetworldstats.com/stats8.htm. Retrieved on 8th December 2016.

It's All About Money, "Know Your Customer (KYC) – What Is KYC? What Documents Are Required?, http://www.itsallaboutmoney.com/did-you-know/what-is-kyc-what-documents-are-required-2/. Retrieved on 20th February 2017.

Kementrian Hukum dan Hak Asasi Manusia Republik Indonesia. "*Penemuan Hukum Oleh Hakim* (*Rechtvinding*)", http://ditjenpp.kemenkumham.go.id/umum/849-penemuan-hukum-oleh-hakim-rechtvinding.html. Retrieved on 13th January 2017.

Landasan Teori. "*Pengertian Internet Banking Tujuan dan Manfaat Sistem Keamanan Untuk Nasabah Menurut Para Ahli*" http://www.landasanteori.com/2015/10/pengertian-internet-banking-tujuan-dan.html. Retrieved on 30th April 2016.

Naratama, Benedictus Bina. "*Ini Modus Pembobolan Rekening Lewat e-Banking*" http://nasional.kontan.co.id/news/ini-modus-pembobolan-rekening-lewat-e-banking. Retrieved on 6th October 2016.

Otoritas Jasa Keuangan (OJK). "*Buku Bijak Ber-eBanking*", http://www.ojk.go.id/Files/box/buku%20bijak%20ber-ebanking.pdf#search=malware. Downloaded on 19th January 2017.

Sudut Hukum. "*Sejarah KUH Perdata (BW)*", http://www.suduthukum.com/2015/08/sejarah-kuh-perdata-bw.html. Retrieved on 27th December 2016.

Sukmana, Yoga. "*BCA Minta Nasabah Waspadai "Sinkronisasi Token" Saat Membuka* Internet Banking" http://bisniskeuangan.kompas.com/read/2015/03/04/144553726/BCA.Minta.Nasabah.Waspadai.Sinkronisasi.Token.Saat.Membuka.Internet.Banking. Retrieved on 6th May 2016.

Sulaiman, Stefanno Reinard. "*BCA: 1000 Nasabah Terkena "Sinkronisasi Token" Saat Akses* Internet Banking" http://bisniskeuangan.kompas.com/read/2015/03/06/061800526/BCA.1.000.Nasabah.Terkena.Sinkronisasi.Token.saat.Akses.Internet.Banking. Retrieved on 12th May 2016.

Syarief, Ika Suryani. "*Situs BCA Terserang Virus? Nasabah Kehilangan Rp18,9 Juta*" http://www.suarasurabaya.net/print_news/Kelana%20Kota/2015/156303-Situs-BCA-Terserang-Virus?-Nasabah-Kehilangan-Rp18,9-Juta. Retrieved on 6th May 2016.

Urban Dictionary. "Hacking", http://www.urbandictionary.com/define.php?term=hacking. Retrieved on 19th February 2017.

USSI. "*Akankah* Financial Tech *Menggeser Perbankan Konvensional*?" http://ussi-software.com/blog/2016/06/09/akankah-financial-tech-menggeser-perbankan-konvensional/. Retrieved on 8th December 2016.