INDONESIA'S CRIMINAL SANCTION TOWARD CRIME OF CREDIT / DEBIT CARD FRAUD

Antonius Maria Laot Kian
Universitas Hasanuddin
Jl.Perintis Kemerdekaan km.10 Makassar
Sulawesi-Selatan, Indonesia
Email: antoniusmarialaotkian@yahoo.com

ABSTRACT

Credit / debit card fraud is a cyber criminal offense increased significantly in Indonesia. The criminal act is stipulated in Law Number 11 year 2008 on Information and Electronic Transactions, having previously used the Penal Code. Although it has been set as a special law, but setting it only accommodated according to its modus operandi, and does not directly touch the core material of the crime, namely computer related fraud, as defined in article 8 of the Convention on Cybercrime. This paper is intended to analyze the Indonesia's crime sanction toward crime of Credit/Debit Card Fraud. The result of this study indicates that there are three kind of crimes are regulated in the Cyber Crime's law in Indonesia, they are illegal access, illegal interception and barrier computer system. To these crimes are threatened with sanctions of absolute sanction with no regard to restitution.

Key words: Credit, Debit, Fraud, Indonesia's Crime Law

Introduction

Malicious behavior emerged long ago and by communities as a reality that is harmful to society (Widodo, 2013). Giriraj Shah as was quoted by Widodo (2013) says that "crime is as old as man", that is that evil age of human civilization, which began when Adam ate the forbidden fruit, which resulted in the issuance of Adam and Eve from paradise. Frank Tannenbaum said that "crime is eternal as its eternal society", the evil immortal eternal as people (Arief Amrullah, 2006).

In principle, actions that are considered evil are always at odds with human moral (immoral) or hurt the feelings of decency in a common life. In terms of the subject, as opposed to evil feelings of decency, and in terms of the object, in this society, such actions detrimental to society, for the crime of touching various aspects of community life. Larry J. Siegel in Widodo (2013) writes: "crime touches all segments of society. Both the poor and desperate, as well as the wealthy and Power full, engage in criminal activity. Crime cuts accross racial, class, and gender lines. It involves acts which shock the collective conscience of the nation, and acts which seems relatively harmless human foibles. Crimes may be comitted among friends and family members, they can also involve absolute strangers".

The existence of human and community development along with technology that followed, led to the emergence of various types of crimes that are new, that grows in various forms and levels in a linear fashion. One crime that is growing in line with the progress of society is crime in cyberspace (cybercrime). Brenner (2001) divides cybercrime within three (3) categories: crimes, in the which the computer is the target of the criminal activity, crimes in the which the computer is a tool used to commit the crime, and crimes in the which the use of the computer is an incidental aspect of the commission of the crime. In line with Brenner, Ian Walden (2007) divides the categories of cybercrime in computer related crime, the content related crime, and computer integrity offenses. In general, there are several types of cybercrime that is cracking, phishing, viruses, hijacking, credit card fraud, online gambling, attacking military and defense. Among the various types of cybercrime, hacking credit cards is the most feared crime and most often occur. In the terminology of criminology, credit card fraud is a cyber crime.

Indonesia is a country with the level of credit card fraud crime is number second behind the Ukraine (Suseno, 2012). Losses due to credit card fraud is often caused by the cause of negative reactions from other countries in online business transactions. Data from the Indonesian National Police stated that an average of 200 cases of cyber crime are dealt with, in general, dominated by a targeted credit card fraud abroad such as USA, Australia, and Canada, with the actors come from major cities like Yogyakarta, Bandung, Jakarta, Semarang, Medan and Riau (http://pritamaardi.wordpress.com, October 21, 2013).

Facts prove that in early February 2008, the Indonesian National Police uncovered a network of credit card fraud and drug dealers in Semarang. Mode used by this mafia is wire tapping, electronic eavesdropping via the telecommunication data such as confidential information such as credit card number, due date and name of the owner, the postscript can be used to make thousands of counterfeit credit cards ready. The result was the discovery of more than 7,000 counterfeit credit cards along with a soft copy of customer data banks in Indonesia. The incident was enough to make banks and credit card issuers scramble immediately take action and replacement of credit cards massively (http://jabar.go.id, April 2, 2008).

Several cases of credit card fraud ever recorded in Indonesia as stated by Sigid Suseno (2013), is a credit card fraud committed by Suprihatin binti Lusmanto and Stevanus Budi Hasmin in Yogyakarta, as well as credit card fraud conducted by Harry P. Samosir and Noftan Ladau in Bandung. And any other credit card fraud case conducted by Rizky Martin alias Steve Rass, and Texanto alias Doni Michael. Both made purchase of goods on behalf of Tim Tamsin Invex Corp., a company located in the US via the internet. Both break down the credit card via internet banking as much IDR. 350 million. Both have been

arrested by cybercrime City Police officers on June 10, 2008 in a cafe in the area of Lanteng Agung, South Jakarta (http://pritamaardi.wordpress.com, October 21, 2013).

Another surprising case was that the piercing was not only carried out on the credit card, but also to an ATM card or a debit card, so it can be said that a criminal offense has been expanded to debit card fraud. In January 2010, Metro TV (Metro Today, January 20, 2010) reported that there were 15 (fifteen) customers complained to the police about the alleged burglary BCA ATM account with no transaction. Metro TV (Metro afternoon, January 21, 20120) also reported that the number of customers who have already ATM burglary as much of 20 (twenty) people within approximately 10 minutes.

The series of events of ATM burglary or debit card to any place in Jakarta, especially on clients of BCA, BNI, BRI, Permata Bank, Mandiri Bank, and BII. Expert Information and Electronic Transaction (ITE), Ruby Alam explained that generally the burglary was carried out with the help of skimmers and spy cam. Skimmer function doubles the existing data in the victim's ATM with a magnetic reader; while the spy camera is used to get the victim's PIN (TV One News Tonight, January 22, 2010). News of the quiz (Topic Nights January 24, 2010) also calls on mobile banking that is used as a mode to break into customer money at the ATM. Even later revealed that in order to record customer PIN, the spy camera carder not use anymore, but instead uses a fake pad pin, the pin design is very similar to the original pad. The rise of the crime of credit / debit card fraud, requires the law arrangement that is expected to prevent and reduce such crime. This paper attempts to elaborate legal arrangements regarding credit/debit card fraud in Indonesia and how the implementation of its criminal sanctions.

Research Method

This research used secondary data, which are collected through library study and legal document as well. In analyzing data, I used three approaches, namely the conceptual, statute approach and the case approach. The conceptual approach was used to elaborate the concepts on credit card fraud from view of scholars. In addition, the statute approach was used to describe the law regulates the fraud crime both nationally and internationally, while the case approach used to understand how is the theory and law are implemented in that case.

Law of Crime Credit / Debit Card Fraud in Indonesia

According to Ervina Lerry WS, Faith, and Stella KR (http://abba.vlsm.org, January 21, 2010), in the article entitled "The World of Cybercrimes: Carding", credit / debit card fraud "covers a wide range of criminal activities involving credit /debit cards. Further stated that a lost or stolen card fraud occurs when someone other than the cardholder uses the card ... Reviews such a crime is the intercept fraud-similar, in the which the card is intercepted either in transit or from a mailbox while on its way from a financial institution to the legitimate customers ". Ari Juliano Gema in his article entitled "Cybercrime: A Phenomenon in Virtual Worlds", classifying credit / debit card fraud in the crime Infringements of Privacy (http://legalitas.org, February 2, 2010). So called because the crime is directed against the very personal information and secrets from someone who stored computerized form of credit card numbers or ATM PIN number, which if known by others, it can be detrimental to the victim both material and immaterial.

According to Widodo (2013), before the Law Number 11 year 2008 on Information and Electronic Transactions enacted, the rule of law against the crime of credit / debit card fraud in Indonesia is carried out through the Criminal Code, especially in the Article 263-276 of forgery, Article 362-367 of the theft, and Article 378-395 of Fraud. Indeed, these chapters is in anticipation of conventional crimes, and somewhat difficult to apply to cyber crime. One example of the use of the Criminal Code in the completion of the crime of credit card fraud is to be read in the judicial decision Number 94 / Pid.B / 2002 / PN. SLMN, August 24, 2002, in which defendant Peter Pangkur (alias Bonny diobok-obok), who committed the crime of credit card fraud, was sentenced to Article 378 (Fraud). In the plea stated that it is unfair if the accused was sentenced to temporary rules of law governing the actions of the defendant in this case there are no rules cybercrime. However, the panel held that the judge should explore, and understand the values that live in the community; in addition, the judge may not refuse a case brought before it by because the law does not exist or is less clear.

Consideration of the above judges decision, in my opinion, that is very appropriate given although there is no law, a criminal act can be categorized as a disgraceful act and rejected by society not only because of the actions stipulated in the legislation (mala in prohibita) but also because of the act on itself is evil (mala in se). Moreover, Widodo (2013), said that there are a few things worth noting about the judicial process are:

a. The judge may make a breakthrough criminal law, because it makes an extensive interpretation, the notion of documentary evidence that it may include e-mail, especially in applying the elements of forgery, although the forgery was committed in cyber space and between the victim and the accused did not know each other and did not meet each other. Paradigm judge is very progressive and able to break the long-held assumption that the Criminal Code is outdated; this is evidenced by the ability to apply criminal law in cases related to misuse of information technology.
b. The judges only proves and discusses in detail about the elements of a crime (criminal act) is charged to the defendant, and not a lot of study in more detail about the elements of criminal liability (criminal responsibility), for example, how large elements mistake, justification, excuse, and why such actions may occur.
c. In consideration for sentencing, the judge had referred to the modern paradigm that makes the kind of punishment of imprisonment as a last option after other types of criminal others are not allowed.
d. The judges just vent about the things that are lighten and burdensome in general, without the support of an expert witness or sufficient scientific references in order of sentences aligned with the interests of the victims, the convicted person and the interests of society and the interests of justice.

Although the above argument can be justified, but the need for the existence of a law regarding credit / debit card fraud becomes a distinct urgency given the complexity of this criminal act can not be equated with other conventional crime because it requires a comprehensive legal interpretation.

Related to the above, the legal world has actually been a long time extending the principles and norms of interpretation when addressing the issue of intangible material, for example in the case of electricity theft as a crime. The problem is, in today's reality, cyber activity is no longer simple because in addition to a virtual character, activities are no longer limited by the territory or jurisdiction of a country; whereas, losses may occur either in implementing information and communication as well as to others who are not involved in it, whether it be inside or outside a country. Based on this we can say that although the activities in cyber space is a virtual activity, and the proof is an electronic instrument, but the impact is very real. This means, the perpetrators should be qualification as people who have to take legal actions in real well. The criminals in the cyber world can be charged legally in this perspective. Therefore, a comprehensive Act Number 11 year 2008 on Information and Electronic Transactions, which is mentioned in the explanation as below:

> "Activities through electronic system, which is also called cyberspace, despite the virtual nature can be categorized as an act or a legal act real. Legally activities in cyber space cannot be approximated by the size and qualifications of the conventional law if only because in this way will be too much trouble and the things that pass from the law. Activities in cyber space are virtual activity that impact is very real even though the evidence is electronic instrument. Thus, the perpetrators should be qualification as people who have committed acts of law are evident".

Thing that should be observed in the law is that the regulation of credit / debit card fraud is not accommodated in particular but is governed by the modus operandi of the criminal act. In fact, when compared to the Convention on Cybercrime (CoC, Budapest, 2001), which became the primary source material of this Act, there is a very noticeable difference on setting the credit / debit card fraud.

According to Sigid Suseno (2012), in an article 2-10 CoC material arranged on criminal law (substantive criminal law) includes a criminal offense against the confidentiality, integrity, and availability of computer data or computer systems (illegal access, illegal interception data interference, system interference, misuse of the devise), crimes related to the computer (computer related forgery and computer related fraud), criminal offenses relating to the content (child pornography offenses related to), and crimes related to the infringement of copyright and related rights (offenses related to infringement of copyright and related rights). The offenses of credit / debit card fraud in the CoC classified in computer related criminal acts of fraud in the article 8 CoC:

> "committed intentionally and without right, the causing of a loss of property to another person by: a. any input, alteration, deletion, or suppression of computer data, b. any interference with the functioning of a computer system, with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person".

In Indonesia, the setting of the crime of credit / debit card fraud is set according to its modus operandi. In Act Number 11 year 2008, the criminal act of computer related fraud is the domain of the crime of credit / debit card fraud, which is assumed to be preceded by some crime (modus operandi), which is regulated in several articles in Law Number 11 year 2008 as follows:

1. Illegal Access

Against unauthorized access, provided for in Article 30: (1) Any person intentionally and without right or unlawfully accessing the computer and / or the Electronic System property of others in any way; (2) Any person intentionally and without right or unlawfully accessing the computer and / or Electronic Systems in any way with the purpose to obtain electronic information and / or electronic documents; (3) Any person intentionally and without right or unlawfully accessing the computer and / or Electronic Systems in any way to violate, break through, exceed, or break through the security system.

Prohibited acts in Article 30 has criminal sanctions provided for in Article 46 that cumulative criminal threats, namely: (1) Any person who meets the elements referred to in Article 30 paragraph (1) shall be punished with imprisonment of six (6) years and / or a fine of not more Rp600.000.000,00; (2) Any person who meets the elements referred to in Article 30 paragraph (2) shall be punished with imprisonment of seven (7) years and / or a fine of Rp700.000.000,00; (3) Any person who meets the elements referred to in Article 30 paragraph (3) shall be punished with imprisonment of eight (8) years and / or a fine of Rp800.000.000,00.

2. Illegal Intercept

About illegal wiretapping, set out in Article 31: (1) Any person intentionally and without right or unlawful interception or eavesdropping on Electronic Information and / or Electronic Documents in a computer and / or certain Electronic Systems belonging to someone else; (2) Any person intentionally and without right or unlawful interception on the transmission of electronic information and / or electronic documents are not public from, to, and within a computer and / or certain Electronic Systems belonging to another person, both of which are not cause any change or cause any change, removal, and / or termination of Electronic Information and / or Electronic Documents being transmitted. Prohibited acts in Article has criminal sanctions provided for in Article 47: Any person who meets the elements referred to in Article 31 paragraph (1) or subsection (2) shall be punished with imprisonment of ten (10) years and / or a fine of many Rp800.000.000,00.

3. Disruption of Computer Data

Regarding the disruption of computer data specified in Article 32: (1) Any person intentionally and without right or unlawful in any way modify, add, subtract, transmitting, damaging, removing, transferring, harboring an Electronic Information and / or Documents electronic belonging to another person or public property. (2) Any person intentionally and without right or unlawful in any way moving or transferring electronic information and / or documents to the Electronic Systems Electronic Other people who are not eligible. (3) Upon the act referred to in paragraph (1) which results in opening of an electronic information and / or confidential electronic documents become accessible to the public in the integrity of the data is not as it should be.

According to Joshua Sitompul (2012), the purpose of the regulation on the data interference or disruption to information or an electronic document is to maintain secrecy (confidentiality), integrity, and availability information or an electronic document. This "change" (alteration) is to modify the original information or electronic documents; here contained the concept of "reduction" that make the information or documents electronically be less than the original and the concept of "additions" that make the information or documents electronically be more than the original (Sitompul, 2012). Related to this may be alleged that the credit card number that is multiplied an indication of the possibility of conversion of native electronic documents. Furthermore, documents or electronic information is transferred from the original electronic systems to electronic systems that are not eligible. Disruption to these data by author, can be interpreted as the "destruction" of the data. In the concept of destruction (destruction) understood that the original data cannot be restored, and even the character of the privacy of the data can be turned into a public data that can be accessed by anyone. In CoC explanation stated that:

> "damaging 'and' deteriorating 'as overlapping acts relate in particular to a negative or alteration of the integrity of information content of the data and Programs. 'Deletion' of the data is the equivalent of the destruction of a corporeal thing. It Destroys and makes them unrecognizable. Suppressing of computer Data means any action that prevents or terminates the availability of the data is to the person WHO has access to the computer or the data carriers on the which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, Reviews such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data".

Prohibited acts have criminal sanctions as provided for in Article 48, namely: (1) Any person who meets the elements as in Article 32 paragraph (1) shall be punished with imprisonment of eight (8) years and / or a maximum fine of Rp 2. 000 000 000; (2) Any person who meets the elements as in Article 32 paragraph (2) shall be punished with imprisonment of nine (9) years and / or a fine of Rp3.000.000.000; (3) Any person who meets the elements as in Article 32 paragraph (3) shall be punished with imprisonment of ten (10) years and / or a fine of Rp5,000,000,000.

4. Disruption of the Computer System

Regarding the disruption of a computer system provided for in Article 33: Any person intentionally and without right or against the law to take any action that result in disruption of Electronic Systems and / or result in the Electronic Systems do not work as they should. Prohibited acts have criminal sanctions in Article 49 that: Any person who meets the elements as in Article 33, shall be punished with imprisonment of ten (10) years and / or a fine of Rp10,000,000,000.

The disruption to electronic systems is usually done via the spread of the virus (worm-viruses) and attacks on computer systems or networks (via engineering-Denial of Service Attack DoS and Distributed Denial of Service Attack-DDoS, including spamming (Widodo, 2013). In many cases credit / debit card fraud in general first conducted disturbances to the system via spamming as computer data and electronic customer information such as PIN and card number can be determined through this technique.

When analyzed carefully, to come to the conclusion that the crime of credit / debit card fraud, investigators must prove the crime of first four mentioned above, leading to the presence of regulatory inefficiency. In fact, in the CoC, the crime of credit / debit card fraud are arranged in a single article (article 8). Inefficiency rules can be triggered any legal vacuum. The principle of lex certa asserted that the rule of law must be clear and not cause multiple interpretations caused by regulatory inefficiencies.

In addition to indicating a regulatory inefficiencies, the author found against the suspects who committed a crime of credit / debit card fraud can be prosecuted in the article "greatly exaggerated" (overload indictment / prosecution). (Therefore, as stipulated in article 8 CoC, Law No. 11 of 2008 must be equipped with a chapter that directly regulates computer related fraud as an act that is prohibited as follows: Any person intentionally and without right, with a view to benefit themselves or others unlawfully: (a) alter, add, subtract, transmitting, damaging, removing, moving, or conceal an electronic information and / or an electronic document in any way, (b) interfere with the electronic system in a way anything, - resulting in the loss or transfer of goods or property of others.

The legislation concerning the crime of credit / debit card is very important to be done so that the efficiency of the new rules in the Indonesian criminal code is capable of supporting contante justisia principle, which is a court that is fast, simple, and inexpensive.

Application Of Criminal Sanctions On Crime Of Credit / Debit Card Fraud In Indonesia

In criminal law, imposing sanctions or punishment is the main thing for an act can be called a criminal offense if it contains a form of penal sanctions. That is why criminal sanctions referred to as ultimum remedium, ie as the final choice of all types of criminal sanctions. On this, in Article 51 of the Draft Penal Code stated that the purpose of punishment are:

a. To prevent the perpetration of a crime by enforcing legal norms of society aegis;
b. Popularizing convicted by holding coaching that makes people good and useful;
c. Resolve conflicts caused by the criminal act, restore balance and bring a sense of peace in the community;
d. Liberating guilt in a criminal;
e. Not intended for and not allowed to retaliation and degrading the human dignity.

According to GP Hoefnagels as cited by Teguh Prasetyo (2010), sanction of the criminal law is a reaction to all offenders who are determined by the law starts from the detention of suspects and prosecution of the defendant to the sentencing by the judge. This means imposing sanctions of the criminal law is a set of policies in the criminal system. In connection with that, there are several theories about the purpose of punishment or criminal sanctions generally accepted in criminal law, namely:

a. Absolute Theory: According to this theory, punishment is an absolute vengeance for the wrongs that have been done, and the action-oriented crime itself (Teguh Prasetyo, 2010). Therefore, this theory is also called the Theory of Judgment (Erdianto Effendi, 2011). Related to this is radically Hegel asserted that character is defined as a cessation of retaliation. Therefore, in line with the category of the Hegelian retaliation, retaliation in theory this should be seen as a

harsh reaction that is both emotional and therefore irrational criminals (Teguh Prasetyo, 2010). Through this theory can be seen that the punishment was given because the person committed the crime and not to achieve other goals (Frans Maramis, 2013). Thus punishment is a just retribution for the harm that has been caused. The theory is distinguished above (Frans Maramis, 2013): Distribution of others regarding this theory is as follows (Fuad USFA, 2004):

(1) The theory of retaliation objective, ie the fulfillment of a feeling of resentment from the community;
(2) The subjective theory of retaliation, which is oriented to the evildoers, where the evil that mistake makers should receive a reply.

Further Karl O. Christiansen (1974) identified five (5) basic characteristics Revenge Theory are:

(1) The purposes of punishment is just retribution;
(2) Just retribution is the ultimate aim, and not in itself a means to any other aim, as for instance social welfare which from this point of view is without any significance whatsoever;
(3) Moral guilt is the only qualification for punishment;
(4) The penalty shall be proportional to the moral guilt of the offender;
(5) Punishment point into the past it is pure reproach, and its purpose is not to improve, correct, educate, or resocialization of the offender.

b. Relative Theory: This theory basing their views on the intent or purpose of punishment is to the protection of society and the prevention of crime (Erdianto Effendi, 2011). Punishment is done so that people do not commit crimes (ne peccatur) (Jan Remmelink, 2003). The theory is divided into (Frans Maramis, 2013):
   (1) The General Theory of Prevention is prevention is addressed to the public at large, to create psychologische zwang so that people are afraid to commit a crime. In other words, the purpose of punishment is given scare by severe penalties. Included in this theory of punishment is intended to protect the public against the evil deeds through the isolation of criminals.
   (2) Theory Special Prevention is prevention is addressed to people who commit crimes that no longer commit crimes. In theory, there are elements of repair or improve personal criminals.

   Karl O. Christiansen (1974) provide some of the main features of a Theory of Relative namely:
   (1) The purpose of punishment is prevention;
   (2) Prevention is not a final aim, but a means to a more suprems aim, e.g. social welfare;
   (3) Only breaches of the law which are imputable to the prepetrator as intent or negligence quality for punishment;
   (4) The penalty shall be determined by its utility as an instrument for the prevention of crime;
   (5) The punishment is prospective, it points ito the future; it may contain as element of reproach, but neither reproach nor retributive elements can be accepted if they do not serve the prevention of crime for the benefit of social welfare.

c. Unification Theory / Integrative: Included in this group is the view that Grotius says that by nature, anyone who commits a crime will be exposed to pain (absolute aspect), but in determining the severity of the pain may be based on social benefit (Frans Maramis, 2013).

In line with the theories of punishment, Frans Maramis (2013) mentions that the distinguished sanction of the criminal law on criminal sanctions (straf) and action (maatregel). Criminal sanctions stem from the basic idea of why organized criminal prosecution, while sanctions, starting from a basic idea as to what the punishment is held (Sholehuddin, 2003). When examined, the focus of criminal sanctions directed at wrongdoing by someone through the imposition of special suffering (bijzonderleed) to appear deterrent effect (an element of retaliation), are also denounced the perpetrator acts; while the focus of sanctions, the more focused on efforts to bring relief to the offender that he changed (curative aspects / repair).

Related to the above, it takes a balance between criminal sanctions and sanction action, between punishment and treatment, as described by Albert Camus Teguh Prasetyo (2010), the offender though Offender applies as human, but as a human being, he remains free to learn new values and new adaptation didactic. This is the core of the double track in the criminal system, in which the position of equality between criminal sanctions and penalties are very useful measures to maximize the use of both sanctions were appropriate and proportionate, and to avoid the imposition of the layered sanctions (Teguh Prasetyo, 2010).

To realize the criminal sanctions, in Article 10 of the Criminal Code are specified types of criminal sanctions as follows:

a. Criminal Principal, the death penalty, imprisonment, imprisonment, criminal fines, penalties cover;
b. Criminal addition, the revocation of certain rights, deprivation of certain goods, the judge's verdict.

Further action related sanctions (maatregel), the Criminal Code is set as follows:

a. Treatment in mental hospitals for offenders who have a mental disorder;
b. conditional Sentencing
c. For minors (not yet 16 years old), the judge may choose an alternative action are: submission to parents / guardians, submission to the government for inclusion in the home country education, placement in a working state.

With regard to the crime of credit / debit card fraud in Indonesia, the sanctions imposed against the defendant based on Law No. 11 of 2008 as *lex*. However it is also possible to use the Criminal Code as well as the *lex generali*, depending on the trial judge's assessment of the facts and evidence presented. Specific to Law No. 11 of 2008, which emphasized the criminal sanctions are sanctions of imprisonment and criminal fines, as defined in Article 46-Section 49 of the Act. In those chapters, imprisonment imposed on average reached 6-10 years, while a fine set of numbers 600 million to 10 billion.

The author argues that the philosophy behind the setting of criminal sanctions against the crime of credit / debit card fraud in Indonesia is very stressed aspects of absolute vengeance. Absolute Vengeance emphasizes aspects of fair retribution against criminals credit / debit card fraud because of the losses incurred. In addition, implied the existence of public retaliation against the perpetrators of the crime of credit / debit card fraud. Nevertheless, in the absolute retaliation mechanism, implied also an attempt to protect the public from criminal acts of credit / debit card fraud, as well as to prevent similar crimes in the future.

The application of criminal sanctions that emphasize the absolute and relative retaliation in imprisonment and fines as regulated by Law No. 11 of 2008 indicates that punishment in Indonesia (for the crime of credit / debit card fraud) did not concern the curative aspects of the criminal. Criminal law was created to restore harmony and balance situation as early creation of a community (*restituo in integrum*). To restore a peaceful society, criminal law must consider all the aspects involved in a crime, especially victims, perpetrators, and society as a whole. Thus, the application of criminal sanctions background retaliation absolute and relative as stipulated in Law No. 11 of 2008, will not be able to create a *restitutio in integrum* if the healing aspect of the criminal credit / debit card fraud is not considered.

Related to this, the author argues that the regulation of criminal sanctions in the Act No. 11 of 2008, it should be emphasized also sanctioned action (*maatregel*). The sanctions measures employed in criminal law focused on healing the offender, namely that actors can change from their wicked ways towards personal benefit society. The author argues that sanctions can act positively emphasize the learning aspect of the scientific side of the crime of credit / debit card fraud. In other words, the perpetrators can be educated more positively in order to develop the skills that can be used at any time of law enforcement and the banks to help uncover similar criminal acts in the future.

Conclusion

Increased criminal offense credit / debit card fraud demands of legislation reform starting from product reformulation of the law, in this case the revision of Law No. 11 of 2008 on Information and Electronic Transactions. Moreover, the reformulation should include an emphasis on the curative aspect of punishment against the perpetrators of the credit / debit card fraud. This is done so that the criminal enforcement against cybercrime although specifically regulated, but able to answer the problem of the crime of credit / debit card fraud holistically.

References

Arief Amrullah. (2006). *Kejahatan Korporasi*. Malang: Bayumedia.
Erdianto Effendi. (2011). *Hukum Pidana Indonesia Suatu Pengantar*. Bandung: Refika Aditama.
Frans Maramis. (2013). *Hukum Pidana Umum dan Tertulis di Indonesia*. Jakarta: PT. RajaGrafindo Persada.
Fuad Usfa. (2004). *Pengantar Hukum Pidana*. Malang: Penerbit Universitas Muhamadiyah Malang.
Ian Walden. (2007). *Computer Crime and Digital Investigation*. New York: Oxford University Press.
Jan Remmelink. (2003). *Hukum Pidana*. Jakarta: Gramedia Pustaka Utama.
Josua Sitompul. (2012). *Cyberspace, Cybercrimes, Cyberlaw, Tinjauan Aspek Hukum Pidana*. Jkarta: Tatanusa.
Karl O. Christiansen. (1974). Some Consideration on Possibility of a Rational Criminal Policy. *Resources Material Series* No. 7, UNAFEI. Tokyo.
Sholehuddin. (2003). *Sistem Sanksi dalam Hukum Pidana: Ide Dasar Double Track System & Implementasinya*. Jakarta: PT. RajaGrafindo Persada.
Sigid Suseno. (2012). *Yurisdiksi Tindak Pidana Siber*. Bandung: Refika Aditama.
Susan W. Brenner. (2001). *Cybercrime: The Investigation, Prosecution and Defense of A Computer-Related Crime*. Durham, North Carolina: Carolina Academic Press.
Teguh Prasetyo. (2010). *Kriminalisasi dalam Hukum Pidana*. Bandung: Nusamedia.
Widodo. (2013). *Aspek Hukum Pidana Kejahatan Mayantara*. Yogyakarta: Aswaja Pressindo.
Widodo. (2013). *Hukum Pidana di Bidang Teknologi Informasi, Cybercrime Law: Telaah Teoritik dan Bedah Kasus*. Yogyakarta: Aswaja Pressindo.

Kitab Undang Undang Hukum Pidana (KUHP)
UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Metro Hari Ini, 20 Januari 2010.
Metro Siang, 21 Januari 2010.
Kabar Malam TV One, 22 Januari 2010.
Topik Malam ANTV, 24 Januari 2010.
http://jabar.go.id, 2 April 2008.
http://legalitas.org, 2 Februari 2010.
http://abba.vlsm.org, 21 Januari 2010
http://pritamaardi.wordpress.com, 21 Oktober 2013.