The Criminal Offense Of Credit/Debit Card Fraud And The Implementation Of Its Criminal Sanction From The Perspective Of Indonesian Criminal Law

Antonius Maria Laot Kian

Abstract: Credit/ debit card fraud is a cyber-criminal offense which frequency of occurrences has increased significantly in Indonesia. This type of criminal offense is regulated in the Law No. 11 Year 2008 on Electronic Information and Transactions, and the Criminal Code (KUHP), previously. Although this type of criminal offense has been set as *lex specialis*, this regulation is only accommodated according to its *modus operandi*, and does not directly touch the core material of the criminal offense, i.e. computer-related fraud, as defined in Article 8 of the Convention on Cybercrime.

Index Terms: Credit/Debit Card Fraud, Indonesian Criminal Law

1 INTRODUCTION

Malicious behavior has been for long emerging and the society considers it as a reality that does the society more harm than good (Widodo, 2013: 29)[1]. Giriraj Shah as quoted in Widodo (2013: 31)[1] says that “crime is as old as man”, meaning that crime is as old as human civilization, in which it began when Adam ate the forbidden fruit which resulted in Adam and Eve being expelled from heaven. Frank Tannenbaum states that “crime is eternal as eternal its society”, (Arief Amrullah, 2006: 8)[2]. Basically, actions that are considered as a crime are always contrary to human moral (immoral) or hurt the feelings of decency in a common life. In terms of the subject, crimes are contrary to these feelings of decency, while in terms of the object, in this case is the society, such actions are detrimental to the society for crime touches all segments of the society. Larry J. Siegel in Widodo (2013: 30)[1] writes, ”crime touches all segments of society. Both the poor and desperate, as well as the wealthy and powerfull, 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 development of humans and the society along with the technology that accompanies them has led to the occurrence of a variety of new types of crime, that develops in various forms and levels in a linear fashion. One of the crime that has developed rapidly in line with improvement in the society is crime in cyberspace (cybercrime).

- *Antonius Maria Laot Kian: Graduate Student PhD, Study Program: Science Of Law. Hasanuddin University, Makassar. Indonesia*
- *E-mail: antoniusmarialaotkian@yahoo.com*

Brenner (2001: 12) [3] divides cybercrime into three (3) categories, namely: crimes in which the computer is the target of the criminal activity, crimes in which the computer is a tool used to commit the crime, and crimes in which the use of the computer is an incidental aspect of the commision of the crime. Likewise, Ian Walden (2007: 19)[4] also divedes cybercrime into the categories of computer-related crimes, content-related crimes, and computer integrity offences. Generally, there are several types of cybercrime, namely cracking, phising, viruses, hijacking, credit card fraud, online gambling, and attacking military defense. Of those types of cybercrime, credit card fraud is a type of cybercrime that most people feel affraid of and occurs most Globally, Indonesia is a country with the level of credit card fraud occurrence second only to Ukraine (Sigid Suseno, 2012: 3). Losses imposed due to credit card fraud often trigger negative reactions from other countries to on-line business transactions. Data retrieved from the Indonesian National Police suggest that they deal with an average of 200 cases of cybercrime, which generally are dominated by credit card fraud with countries like U.S.A., Australia, and Canada as the targets, in which the hackers come from major cities like Yogyakarta, Bandung, Jakarta, Semarang, Medan and Riau (http://pritamaardi.wordpress.com, 21 October 2013). Facts prove that in early February 2008, the Indonesian National Police uncovered a international network of credit card fraud and drug dealers in Semarang. The mode used by the mafia is wire tapping, i.e. electronic eavesdropping via the telecommunication data in terms of confidential information such as credit card number, the due date and the name of the owner, which can be used to produce thousands of counterfeit credit cards ready to use. The result was the discovery of more than 7,000 counterfeit credit cards along with customer data in the form of a soft copy from a number of banks based in Indonesia. This makes the banks issuing credit cards scramble and immediately take an action of en masse credit-card replacement (http://jabar.go.id, 2 April 2008). There are a number of credit card fraud cases that once tarnished Indonesia’s good reputation as investigated by Sigid Suseno (2013)[5], namely credit card fraud committed by Suprihatin binti Lusmanto and Stevanus Budi Hasmin in Yogyakarta, as well as credit card fraud conducted Harry P. Samosir and Noftan Ladau in Bandung. Or another credit card fraud case

committed by Rizky Martin aka Steve Rass and Texanto aka Doni Michael. Both perpetrators made a purchase transaction of goods on behalf of Tim Tamsin Invex Corp., a company based n the US via the internet. Both penetrated the credit card system via the internet banking by Rp 350,000,000. These perpetrators have been arrested by the cybercrime unit of Polda Metro Jaya on 10 June 2008 in a warnet (internet cafe) located in Lanteng Agung, South Jakarta (http://pritamaardi.wordpress.com, October 21, 2013) Another surprising thing is that tapping is not only carried out on credit cards, but also on ATM cards and debit cards, and therefore it can be said that such criminal offenses have expanded into debit card fraud. In January 2010, Metro TV (Metro 20 January 2010) reported that there were 15 (fifteen) customers who complained to the police about their BCA account break-in without any transactions. Metro TV (Metro Siang, 21 January 2012) also reported that the total number of customers who experienced this ATM burglary had reached 20 (twenty) people within approximately 10 minutes. The series of this ATM burglary incident or debit card fraud also occurred in Jakarta, especially to the customers of banks such as BCA, BNI, BRI, Bank Permata, Bank Mandiri, and BII. An expert on Electronic Information and Transactions, Ruby Alamsyah explained that generally this burglary was carried out using skimmers and spy cam. Skimmers function to duplicate the existing data in prospective victims' ATM cards using a magnetic reader; while the spy cam is used to know these victims' PIN (Kabar Malam TV One, 22 January 2010). One of ANTV's news program (Topik Malam, 24 January 2010) also mentioned about phone banking (mobile banking) used as a mode to break into customers' money in their ATM. Even later it is revealed that in order to record customers' PIN, carders do not use a spy cam anymore, instead they use a fake pin pad, which design is very similar to the original pin pad. The increasing incidents of credit/ debit card fraud require legal arrangements that are expected to prevent and reduce such a crime. This paper attempts to elaborate legal arrangements regarding credit/ debit card fraud in Indonesia and describe its implementation.

Legal Arrangements against Credit/Debit Card Fraud in Indonesia

According to Ervina Lerry WS, Iman, and Stella KR (http://abba.vlsm.org, 21 January 2010), in an article entitled "The World of Cybercrimes: Carding", credit/debit card fraud "covers a wide range of criminal activities involving credit/debit cards". Then, it is mentioned that, "lost or stolen card fraud occurs when someone other than the cardholder uses such card… a similar crime is intercept fraud, in which the card is intercepted either in transit or from a mailbox while on its way from a financial institution to the legitimate customer". Ari Juliano Gema in his paper entitled "Cybercrime: Sebuah Fenomena di Dunia Maya", classifies credit/debit card fraud into Infringements of Privacy (http://legalitas.org, 2 February 2010). This type of fraud is called so since it is intended to steal very personal and confidential information of someone stored using a computerized system in terms of credit card numbers or ATM PIN number, which if known by others, it can be detrimental to the victim both materially and immaterially. According to Widodo (2013: 106)[1], before the issuance of the Law No. 11 Year 2008 on Electronic Information and Transactions, enforcement of the law against credit/ debit card fraud in Indonesia was carried out pursuant to the Criminal Code (KUHP), namely Articles 263-276 on Forgery, Articles 362-367 on Theft and Articles 378-395 on Fraud. Actually, these articles are an anticipation of conventional crimes, and somewhat difficult to apply to cybercrime. One example of the implementation of the Criminal Code to deal with credit card fraud can be read in the court decision No. 94/ Pid.B/ 2002/ PN. SLMN, dated 24 August 2002, in which the defendant Peter Pangkur (aka Bonny Diobok-Obok), who committed the crime of credit card fraud was sentenced through Article 378 (Fraud). In the plea, it was stated that it was unfair if the defendant was sentenced while there is no legal rules governing such an action committed by the defendant, in this case is cybercrime. However, the panel held that the judges should explore, follow and understand the values that exist in the community; in addition, the judges are not allowed to refuse any cases brought to them just because the law that governs those cases does not exist or is unclear. The judges' consideration above as far as the author is concerned is very appropriate given that despite the absence of the law governing it, a criminal offense can also be categorized as a disgraceful action rejected by the society not only because such an action is regulated in the legislation (mala in prohibita) but also because the action is evil in itself (mala in se). Moreover, Widodo (2013: 114)[1] notes a few things necessary to note in such a judicial process, namely:

a. Judges may have made a fairly spectacular legal breakthrough since they have made an extensive interpretation, i.e. the definition of documentary evidence which includes e-mail, especially in implementing the elements of forgery, although the forgery was committed in cyber space and the victims and the defendant did not know each other and did not meet each other. This paradigm of the judges is very progressive and able to break the long-held assumption that the Criminal Code has been outdated; this is evident from by the ability to apply criminal law in cases related to misuse of information technology.

b. The panel of judges only proved and discussed in detail the elements of a criminal act charged to the defendant, and did not investigate in more detail the elements of criminal responsibility, for examples, how serious is the mistake made, justifications, excuses, and why such an action occurs.

c. In relation to sentencing consideration, the panel of judges had referred to the modern paradigm of sentencing that decided imprisonment as the last option after considering that the other types of punishment were inappropriate.

d. The panel of judges only disclosed things that generally may alleviate and incriminate, without sufficient support of expert witnesses or scientific references in order that the sentence given and the interests of the victims, the defendant and the society as well as justice are in tune.

Although the above argument can be justified, but the need for the existence of lex specialis concerning credit/ debit card fraud becomes a distinct urgency given the complexity of this criminal act cannot simply be equated to other conventional crimes because it requires a comprehensive legal interpretation. In relation to the foregoing, the world of law has actually been long trying to extend its interpretation principles and norms when addressing issues related to intangible material, for an example the case of electricity theft as a crime. The problem is, in today's reality, cyber activities are getting

complicated because, not to mention its virtual nature, these cyber activities are no longer limited by the territory or jurisdiction of a country; although losses may occur either to the implementing information and communication as well as to others who are not involved in it, whether they live in that country or not. Thus, it can be concluded that although the activities in cyber space are virtual, and the evidence is in the form of an electronic instrument, however the impact is very real. This means that the perpetrator(s) should also be considered as someone who has committed a crime. In this perspective, the criminals in the cyber world can be charged legally. Therefore, the Law No. 11 Year 2008 concerning Electronic Information and Transactions is enacted, which mentions that: Activities through the medium of an electronic system, which is also called cyberspace, despite its virtual nature, can be categorized as a real act or a real legal act. Juridically, activities in cyber space cannot be approached by simply using the standards and qualifications of the conventional law because if it is this manner that is used, then there will be too many troubles and things that the law enforcement might not notice. Activities in cyber space are virtual activities with a very real impact even though the evidence is electronic in nature. Thus, the perpetrators should be considered as someone who has committed a real legal act. One thing necessary to note in the aforesaid law is that regulation concerning credit/ debit card fraud is not specifically accommodated but is governed by the modus operandi of the criminal act. In fact, when compared to the Convention on Cybercrime (CoC, Budapest, 2001), which serves as the primary material source of this law, there is a very noticeable difference in term of the regulation related to the credit/ debit card fraud. According to Sigid Suseno (2012: 7-8)[5], in the Articles 2-10 of the CoC, it is mentioned that substantive criminal law includes a criminal offense against confidentiality, integrity, and availability of computer data or computer systems (illegal access, illegal interception, data interference, system interference, misuse of devise), computer-related crimes (computer-related forgery and computer-related fraud), content-related crimes (offenses related to child pornography), and offenses related to infringement of copyright and related rights. Article 8 of the CoC classifies credit/ debit card fraud into computer-related fraud: commited 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, credit/ debit card fraud is regulated according to its modus operandi. In the aforesaid Law No. 11 Year 2008, the criminal act of computer-related fraud that serves as the domain of the criminal act of credit/ debit card fraud is assumed to be preceded by a number of criminal acts (modus operandi), regulated in several articles of the Law No. 11 Year 2008 as follows:

1. Illegal Access

Illegal access is defined in Article 30: (1) Any person who is intentionally and without right or unlawfully accessing a computer and/ or an Electronic System that belongs to others in any way; (2) Any person who is intentionally and without right or unlawfully accessing a computer and/ or an Electronic System in any way with the purpose of obtaining Electronic Information and/ or Electronic Documents; (3) Any person who is intentionally and without right or unlawfully accessing a computer and/ or an Electronic System in any wat with the purpose of violating, penetrating, exceeding, or hacking the security system. Those prohibited actions set forth in Article 30 impose criminal sanctions set forth in Article 46 and the criminal penalty is cumulative in nature, namely: (1) Any person who meets the elements referred to in Article 30 paragraph (1) shall be punished with a maximum of 6 (six) years of imprisonment and/ or a maximum fine of Rp 600,000,000 (six hundred million rupiah); (2) Any person who meets the elements referred to in Article 30 paragraph (2) shall be punished with a maximum of 7 (seven) years of imprisonment and/ or a maximum fine of Rp 700,000,000 (seven hundred million rupiah); (3) Any person who meets the elements referred to in Article 30 paragraph (3) shall be punished with a maximum of 8 (eight) years of imprisonment and/ or a maximum fine of Rp 800,000,000 (eight hundred million rupiah).

2. Illegal Wiretapping

Illegal wiretapping is defined in Article 31: (1) Any person who is intentionally and without right or unlawfully carrying out an interception or wiretapping on Electronic Information and/ or Electronic Documents in a computer and/ or certain Electronic System that belongs to others; (2) Any person who is intentionally and without right or unlawfully carrying out an interception or transmission of Electronic Information and/ or Electronic Documents that is not done publicly from, to, and in a computer and/ or certain Electronic System that belongs to others, either causing any change, removal, and/ or termination of Electronic Information and/ or Electronic Documents being transmitted or not. Those prohibited actions set forth in Article 31 impose criminal sanctions set forth in Article 47: Any person who meets the elements referred to in Article 31 paragraphs (1) or (2) shall be punished with a maximum of 10 (ten) years of imprisonment and/ or a maximum fine of Rp 800,000,000 (eight hundred million rupiah);

3. Disruption to Computer Data

Disruption to computer data is defined in Article 32: (1) Any person intentionally and without right or unlawfully in any manners modifying, adding, , transmitting, damaging, removing, transferring, or hiding Electronic Information and/ or Electronic Documents belonging to others or public property. (2) Disruption to computer data is defined in Article 32: (1) Any person intentionally and without right or unlawfully in any manners transferring Electronic Information and/ or Electronic Documents to an Electronic System that belongs to an unauthorized party. (3) The acts referred to in paragraph (1), which result in the disclosure of confidential Electronic Information and/ or Electronic Documents which makes them accessible to the public but not in the same data integrity. According to Joshua Sitompul (2012: 232)[6], data interference settings and the settings of disruption to electronic information or documents are intended to maintain confidentiality, integrity, and availability of the electronic information or documents. The act of altering means modifying the original electronic information or documents; this term contains the concept of “reduction” that makes the electronic information or documents reduce and the concept of “addition” that makes the electronic information or documents increase (Joshua Sitompul, 2012: 233)[6]. Based on the foregoing, it

can be hypothesized that the number of credit cards multiplied might be an indication for the possibility of the modification of the original electronic documents. Furthermore, the electronic information or documents are transferred from the original electronic system to another unauthorized electronic system. Disruption to these data, in the author's opinion, can be interpreted as "destruction" of the data. Based on this destruction concept, it is suggested that the original data cannot be restored, even the privacy character of the data can be turned into public data that can be accessed by anyone. The CoC reads:... 'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes. 'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable. Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored. The term 'alteration' means the modification of existing data. The input of malicious codes, such as viruses and Trojan horses is, therefore, covered under this paragraph, as is the resulting modification of the data. Those prohibited actions impose criminal sanctions set forth in Article 48, namely: (1) Any person who meets the elements referred to in Article 32 paragraph (1) shall be punished with a maximum of 8 (eight) years of imprisonment and/ or a maximum fine of Rp 2,000,000,000 (two billion rupiah); (2) Any person who meets the elements referred to in Article 32 paragraph (2) shall be punished with a maximum of 9 (nine) years of imprisonment and/ or a maximum fine of Rp 3,000,000,000 (three billion rupiah); (3) Any person who meets the elements referred to in Article 32 paragraph (3) shall be punished with a maximum of 10 (ten) years of imprisonment and/ or a maximum fine of Rp 5,000,000,000 (five billion rupiah).

4. Disruption to Computer Systems

Disruption to computer system is defined in Article 33: (1) Any person intentionally and without right or unlawfully in any manners taking any actions that result in disruption to Electronic Systems and/ or cause the Electronic Systems do not work as they should. Those prohibited actions impose criminal sanctions set forth in Article 49, namely: (1) Any person who meets the elements referred to in Article 33 shall be punished with a maximum of 10 (ten) years of imprisonment and/ or a maximum fine of Rp 10,000,000,000 (ten billion rupiah). The disruption to electronic systems is usually done by spreading viruses (worm-viruses) and attacking computer systems or networks (using the techniques of Denial of Service-DoS Attack and Distributed Denial of Service-DdoS Attack, including spamming) (Widodo, 2013: 62)[1]. In a number of credit/ debit card fraud cases, disruption will generally be created to the computer system via spamming because the electronic data and information of the customers such as PIN and card number can be discovered using these techniques. After careful analysis, to come to the conclusion of the criminal offense in the form of credit/ debit card fraud, investigators must firstly prove the four types of criminal offenses mentioned above, leading to regulatory inefficiency. In fact, in the CoC, credit/ debit card fraud is regulated only in one article (i.e. Article 8 concerning computer-related fraud. This regulatory inefficiency might trigger any legal vacuum. The lex certa principle asserts that legal arrangements must be clear and does not lead to multiple interpretations due to regulatory inefficiency. In addition to indicating regulatory inefficiency, as far as the author is concerned, the defendant who commits a crime of credit/ debit card fraud can be prosecuted using "greatly exaggerated" articles (overload indictment/ prosecution). (Therefore, as stipulated in Article 8 of the CoC, the Law No. 11 Year 2008 must be equipped with an article that directly regulates computer-related fraud as an act that is prohibited., specifically: Any person intentionally and without right, with a view to benefiting themselves or others unlawfully: (a) altering, adding, removing, transmitting, damaging, transferring, or hiding electronic information and/ or electronic documents in any manners, (b) creating disturbance to the electronic system in any manner, which results in the loss or the transfer of goods or property of others. Legal arrangements concerning the criminal offense of of credit/ debit card fraud are urgently required in order that the efficiency of such arrangements in the Indonesian criminal code will be able to support the contante justisia principle, which is quick, simple, and affordable judiciary.

The Implementation of Criminal Sanction against Credit/ Debit Card Fraud in Indonesia

In criminal law, imposing sanctions or punishment becomes the main issue for an act is considered a criminal offense if it imposes a sanction in the form of punishment. That is why criminal sanctions is called ultimum remedium, i.e. as the last option of any criminal sanctions. In relation to this, in Article 51 of the Draft Criminal Code, it is stated that the purpose of punishment is:

- **a.** To prevent a crime by enforcing legal norms and community protection;
- **b.** To have the defendant(s) socialize by fostering the defendant(s) so that the defendant(s) can be someone good and useful;
- **c.** To resolve conflicts caused by the criminal act, restore balance and bring a sense of peace among the community;
- **d.** To release the feeling of guilt that the defendant(s) might feel;
- **e.** Not to make the defendant(s) suffer and it is not allowed to degrade human dignity.

According to G. P. Hoefnagels in Teguh Prasetyo (2010)[7], sanctions in the criminal law is defined as a reaction to all offenders that is determined by the law starting from the detention of a suspect and prosecution of the defendant until sentencing by the judge. It means that sanction imposition in the criminal law is a set of policies in the criminal system. In connection with that, there are several theories about the objectives of punishment or the imposition of criminal sanctions that are generally accepted in criminal law, namely:

a. The Absolute Theory: According to this theory, punishment is the absolute vengeance for the wrong doing that has been done that is oriented towards the crime and the crime occurrence itself (Teguh Prasetyo, 2010)[7]. Therefore, this theory is also called the Theory of Revenge (Erdianto Effendi, 2011)[8]. In relation to this, Hegel asserts radically that character of the revenge is defined as a cessation. Hence, consistent with revenge defined in Hegelian category, revenge defined in this theory should be seen as a harsh emotional

reaction and therefore irrational criminals (Teguh Prasetyo, 2010)[7]. Through this theory, it can be seen that punishment is given because one commits the crime (quia peccatum) and it is not intended to achieve another goal (Frans Maramis, 2013)[9]. In so doing, punishment is a fair retribution for the harm/ loss that the person has caused. This theory is divided into (Frans Maramis, 2013)[9]: The other categorization of this theory is given as follows (Fuad USFA, 2004)[10]:

(1) The theory of objective revenge, which is oriented to the satisfied feeling of revenge of the community;
(2) The theory of subjective revenge, which is oriented to the wrongdoer, in which it is the crime of the wrongdoer that should receive punishment.

Furthermore, Karl O. Christiansen (1974)[11] identifies five (5) basic characteristics of the Revenge Theory, nemely:

(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 resocialize teh offender.

b. The Relative Theory: This theory is built on the view of the intention or purpose of punishment, i.e. community protection and crime prevention (Erdianto Effendi, 2011)[8]. Punishment is given in order that people do not commit a crime (ne peccatur) (Jan Remmelink, 2003)[12]. This theory is divided into (Frans Maramis, 2013[9]):

(1) The Theory of General Prevention, i.e. prevention attempts are intended for the public in general to create psychologische zwang so that people will be afraid of committing a crime. In other words, punishment is given to frighten people using severe penalties. Included in this theory is that punishment is intended to protect people against the evil deeds through the isolation of criminals.
(2) The Theory of Specific Prevention, i.e. prevention attempts are intended for people who commit a crime in order that they do not commit crimes any longer. This theory contains an element of repairing or improving personality of the criminals.

Karl O. Christiansen (1974)[11] provides several main characteristics of the Relative Theory, 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. The Theory of Unification/ Integration: Included in this theory is Grotius' view that anyone who commits a crime, by nature, will be exposed to pain (the absolute aspect), however, to determine the severity of the pain may depend on the social benefit (Frans Maramis, 2013)[9]. In line with the theories of punishment above, Frans Maramis (2013)[9] mentions that sanctions of the criminal law are divided into criminal sanctions (straf) and actions (maatregel). Criminal sanctions are derived from the basic idea of why punishment should be given, while sanction actions are derived from a basic idea of what the purpose of giving punishment is (Sholehuddin, 2003)[13]. Based on the analysis, it is found that the focus of criminal sanctions is on the wrongdoing that the wrongdoer does through the imposition of special suffering (bijzonderleed) in order to raise the deterrent effect (the element of revenge), that also aims to criticize what this perpetrator has done; while the focus of the sanction action is on the efforts to assist the offender in order to change (the curative aspect/ the reparation aspect). In relation to the foregoing, it takes a balance between criminal sanctions and sanction actions, between punishment and treatment, because in the view of Albert Camus as explained by Teguh Prasetyo (2010)[7], the offender though s/he is a human offender, as a human being, s/he remains allowed to learn new values and new adaptation that are educating in nature. This is the core of the double track system of punishment, in which equality in the position of criminal sanctions and sanction actions are very useful to make the most of both types of sanctions in an appropriate and proportional manner, and to avoid the imposition of sanctions that is fragmentaristic (Teguh Prasetyo, 2010)[7]. To realize those criminal sanctions, Article 10 of the Criminal Code specifies the types of those criminal sanctions as follows:

a. Principal Punishment, includes the death penalty, imprisonment, confinement, criminal fines, incarceration;
b. Additional Punishment, includes revocation of certain rights, deprivation of certain goods, announcement of the judges' verdict.

Furthermore, in relation to sanction actions (maatregel), the following are regulated in the Criminal Code:

a. treatment in mental hospitals for offenders who have a mental disorder;
b. conditional sentencing
c. for minors (who have not yet reached the age of 16 years old), judges may choose an alternative action, namely: returning them to their parents/ guardians, returning them to the government to be sent tothe state's educational houses, placement to the state's work place.

With regard to the crime of credit/ debit card fraud that takes place in Indonesia, the sanctions imposed against the defendant are pursuant to the Law No. 11 Year 2008 as lex specialis. However, it does not rule the Criminal Code out as lex generali, depending on the judge's assessment of the facts arising in the trial and the evidence presented. Especially in relation to the Law No. 11 Year 2008, the criminal sanctions put into emphasis are imprisonment and criminal fines, as set forth in Articles 46 to 49 of the Law. In those articles, imprisonment that is imposed lasts for 6 to 10 years on average, while the criminal fine ranges from Rp 600 million to

Rp 10 billion. As far as the author is concerned, the philosophy behind the arrangements of criminal sanctions against the crime of credit/ debit card fraud in Indonesia puts a great emphasis on absolute revenge. This absolute revenge emphasizes the aspects of fair retribution against the perpetrator of credit/ debit card fraud due to the losses incurred. Moreover, the existence of public retaliation against the perpetrator of credit/ debit card fraud is implied. Nevertheless, this absolute revenge mechanism also implies an attempt to protect the society from credit/ debit card fraud as well as to prevent similar crimes in the future. The implementation of criminal sanctions that emphasize the aspects of absolute and relative revenge reflected in imprisonment and fines as set forth in the Law No. 11 Year 2008 indicates that punishment in Indonesia (for the crime of credit/ debit card fraud) does not consider the curative aspects of the criminal. Criminal law was created to restore harmony and balance situations as they were in the early establishment of a community (restituo in integrum). To bring back the peacefull situation to the society, criminal law must consider all the aspects involved in a crime, especially the victim(s), perpetrator(s), and the society as a whole. Therefore, the application of criminal sanctions that builds on absolute and relative revenge as stipulated in the Law No. 11 Year 2008 will not be able to create a restitutio in integrum if it does not take into account the recovery aspects of the perpetrator of the credit/ debit card fraud. In connection with this, the author argues that the regulation of criminal sanctions set forth in the Law No. 11 Year 2008 should also emphasize the sanction actions (maatregel). The sanction actions set forth in the criminal law focus on healing the offender, specifically the offender can change into someone that provides benefits for the society. The author argues that sanction actions can positively emphasize the learning aspect of the scientific aspect of the crime of credit/ debit card fraud. In other words, the perpetrators can be taught to develop their skills that later might help law enforcement officers and the banks to help uncover similar criminal acts in the future.

CONCLUSIONS

The increasing rate of a criminal offense in the form of credit/ debit card fraud demands reforms that start from reformulation of legal products, which in this case is the revision of the Law No. 11 Year 2008 concerning Electronic Information and Transactions. Moreover, the reformulation should include an emphasis on the curative aspect of the penalty against the perpetrators of the credit/ debit card fraud. This is done in order that the enforcement of the criminal law against cybercrime, although specifically regulated, will be able to address issues related to the criminal offense of credit/ debit card fraud holistically.

REFERENCES

[1] Widodo. 2013. Aspek Hukum Pidana Kejahatan Mayantara. Aswaja Pressindo. Yogyakarta.

[2] Amrullah, Arief, 2006. Kejahatan Korporasi, Malang: PT Bayumedia

[3] Susan W. Brenner. 2001. Cybercrime: The Investigation, Prosecution and Defense of A Computer-Related Crime. Carolina Academic Press. Durham, North Carolina.

[4] Ian Walden. 2007.Computer Crimes and Digital Investigations, Oxford University Press, 2007,

[5] Suseno. 2012. Yurisdiksi Tindak Pidana Siber. Refika Aditama. Bandung.

[6] Sitompul, Josua 2012, Cyberspace, cybercrime, cyberlaw, Jakarta: PT Tatanusa,.

[7] Teguh Prasetyo. 2010. Kriminalisasi dalam Hukum Pidana. Nusamedia. Bandung.

[8] Erdianto Effendi. 2011. Hukum Pidana Indonesia Suatu Pengantar. Refika Aditama. Bandung.

[9] Frans Maramis. 2013. Hukum Pidana Umum dan Tertulis di Indonesia. PT. RajaGrafindo Persada. Jakarta

[10] Fuad Usfa. 2004. Pengantar Hukum Pidana. Penerbit Universitas Muhamadiyah Malang. Malang

[11] Karl O. Christiansen. 1974. Some Consideration on Possibility of a Rational Criminal Policy. Resources Material Series No. 7, UNAFEI. Tokyo.

[12] Jan Remmelink. 2003. Hukum Pidana. Gramedia Pustaka Utama. Jakarta.

[13] Sholehuddin. 2003. Sistem Sanksi dalam Hukum Pidana: Ide Dasar Double Track System & Implementasinya. PT. RajaGrafindo Persada. Jakarta.