Law Development Journal
ISSN : 2747-2604
Volume 3 Issue 2, June 2021, (240 – 247)

The Criminal Law Enforcement Against Crime Of Carding In Electronic Transactions

Cemban Galuh Sambodo[*)] and Sri Endah Wahyuningsih[**)]

[*)] Indonesian National Police, E-mail: cgaluhs_mh36@std.unissula.ac.id
[**)] Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang

Abstract
The approach method used in this research is normative juridical. This study uses a normative juridical research method using a literature study approach (library research) and statutory approach (statute approach) which in this case is related to Criminal Law Enforcement against Crime of Carding in Electronic Transactions. The data used in this study consists of primary data, secondary data, and tertiary data which will then be analyzed qualitatively. The results of this study indicate that the enforcement of criminal law against the crime of carding as a crime that uses technology is one type of crime that is transnational in nature, it is necessary to have rules that have broad jurisdiction, or an agreement with other countries is needed to be able to arrest and punish the perpetrators criminal acts in the jurisdiction of the State that has an international agreement with Indonesia and, law enforcement officers, adequate human resources are required, so the law enforcement officers can maximum to handle the criminal on the carding in electronical transactions.
Keywords: Law Enforcement; Carding; Electronics.

1. Introduction

Human civilization and technological progress are two coins that continue to be side by side, the development of human technology is also influenced by the progress of an era / era which will certainly affect every aspect of human life both positively and negatively. Along with the development of human times, it affects changes from negative aspects, one of which is crime in the modernization era. Crime is a social problem that is not only faced by Indonesia or certain communities and countries, but is a problem faced by all people in the world. Crime as said by Saiichiro Uno is a universal phenomenon, not only the number is increasing but also the quality is taken seriously compared to the past.[1]

The most frequently committed cyber crime is carding. Carding crime is fraud using credit card data. Carding crimes committed by the perpetrators or called carders can be categorized into 2 (two) forms, namely conventional or offline transactions and virtual or online transactions.[2]. Cybercrime is all criminal acts related to information systems, as well as communication systems which are a means for delivering/exchanging information with other parties.[3]

[1]Barda Nawawi Arief, 2007, *Kapita Selekta Hukum Pidana Tentang Sistem Peradilan Terpadu*. Undip Press. Semarang. p.11
[2]Jovan, 2006, *Pembobol Kartu Kredit Menyingkap Teknik dan Cara Kerja Para Carder di Internet*, Mediakita, Jakarta, p. 120
[3]Didik M. Arief Mansur dan Elistaris Ghultom, 2005, *Cyber law-Aspek Hukum Teknologi Informasi,* Refika Asitama, Bandung, p. 10.

The carding itself is a credit card crime, is a form of theft and fraud in the internet world that is carried out by the perpetrators using stolen credit cards or fake credit cards made by themselves. The goal, of course, is to buy goods illegally on multiple accounts from the actual credit card holder or to illegally withdraw funds from a bank account belonging to someone else.[4]

The development of carding among the public in particular to internet users, the domain owner should be held accountable for his actions. In the Indonesian legal system, the Gen Straf Zonder Schuld principle is adopted, namely that there is no crime without error to hold a person or a legal entity accountable.[5] Likewise, when we talk about the crime of carding, it cannot be separated from criminal responsibility.[6]

Prior to the enactment of the Electronic Information and Transaction Law, to enforce the carding crime, the articles in the Criminal Code were applied.[7] Supposedly to be able to guarantee the privacy of a person for special data or information in conducting online transactions on the internet, a special law is needed that regulates it.[8] So the government makes laws and regulations that contain protection of electronic information and transactions, in the form of Act No. 19 of 2016 concerning amendments to Act No. 11 of 2008 concerning Electronic Information and Transactions.

In Indonesia, the act of carding is very fast, unfortunately the criminal law system in Indonesia still provides opportunities due to the weakness of the system of supervision and law enforcement for this carding crime. The problem with this carding crime is a serious enough problem to be handled. Based on the description above, it attracted the author's interest to discuss "Criminal Law Enforcement Against the Crime of Carding in Electronic Transactions", this study aims to determine Law Enforcement against the Crime of Carding in Indonesia and Obstacles to Law Enforcement of the Crime of Carding in Indonesia.

2. Research Methods

The approach method used in this research is normative juridical.[9] Source of data used in this study are primary, secondary, and tertiary data sources. Furthermore, it will be related to the problems that will be discussed, namely: Criminal Law Enforcement Against the Crime of Carding in Electronic Transactions. The data collection method used to obtain data that has a relationship with the object of research is document review, while the data

[4] Sutan Remy Syahdeini, 2009, *Kejahatan dan Tindak Pidana Komputer*, PT Pustaka Utama Grafiti, Jakarta, p.82
[5]Erdianto Efendi, 2011, *Hukum Pidana Indonesia-Suatu Pengantar*, Refika Aditama, Bandung, p. 10
[6]Megat Kalti Takwa, Evi Deliana Ferawati, Pertanggungjawaban Pidana Terhadap Pemilik Domain Cara Melakukan *carding* Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Informasi dan Transaksi Elektronik, *JOM Fakultas Hukum*, Vol. V No. 2 (2018). p. 3, https://jom.unri.ac.id/index.php/JOMFHUKUM/article/view/22011
[7]Ade Ary Syam Indradi, 2006, *Carding Modus Operandi, Penyidikan dan Penindakan*, Grafika Indah, Jakarta, p. 91.
[8]Edmon Makarim, 2005, *Pengatar Hukum Telematika*, PT Raja grafindo Persada, Jakarta, p. 198.
[9]I Made Pasek Diantha, 2016, *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*, Prenada Media Group, Jakarta, p. 12

analysis method used is qualitative data analysis in this study including data reduction, data presentation and conclusion drawing/verification.

3. Results and Discussion

3.1. Law Enforcement Against the Crime of Carding in Indonesia

Law enforcement is an activity to harmonize the relationship of values outlined in the rules, views that are embodied in attitudes and actions as a series of final stages of value elaboration to create peaceful social life. The enforcement of the law is characterized by several factors that are closely related to each other, namely the law and its rules.[10]

Furthermore, law enforcement is criminal law enforcement is a part of the (criminal) law enforcement mechanism, so punishment, which is usually interpreted as "punishment" is nothing but a deliberately planned "policy process"[11]

Crime through information technology or what is often called cybercrime is a representation of international crimes that use hitech because the most prominent characteristics and crimes are borderless or do not know national borders. The technology is relatively high, meaning that only certain people are capable of committing this crime and are open resources mediators or can be a medium for various crimes, including crimes in banking, capital markets, sex, piracy of intellectual rights and terrorism and more precisely including transnational crimes.[12]

Carding crime is a crime that uses internet technology as the main means to illegally access a website system to obtain data on credit card customers. The goal is to spend illegally on a credit card that has been obtained or to obtain funds belonging to the credit card holder. Below is a description of the modus operandi that is currently often carried out by carders.[13]

In Black's Law Dictionary the definition of a credit card is:

"any card, plate, or other like credit devise existing for the purpose of obtaining money, property, labor or services on credit. The term does not include a note, check, draft, money order or other like negotiable instrument"

Which means: "whatever card, plate or similar card is used to obtain money, property/materials, labor or services on credit. This term does not include notes, checks, drafts, money orders or other instruments that can be cashed.[14]

---

[10]Teguh Prasetyo & Abdul Halim, 2005, *Politik Hukum Pidana*, Pustaka Pelajar, Yogyakarta, p. 111

[11]Feri Vernando Situngkir & Siti Rodhiyah Dwi Istina, The Enforcement of Criminal laws of Hate Speech in Social Media, *Law Development Journal*, Vol. 2 Issue 4. (2020). p. 544, http://jurnal.unissula.ac.id/index.php/ldj/article/view/13642

[12]Cahyo Handoko, 2017, Tinjauan Hukum Pidana Terhadap Cardin Sebagai Salah Satu Bentuk Cybercrime, *Tesis*, Universitas Muhamadiyah Surakarta, p. 5

[13]Novryan Alvin K. 2014. *Pencegahan Kejahatan Carding sebagai kejahatan Transnasional menurut hukum Internasional*. Fakultas Hukum Brawijaya. Malang, p. 6

[14] Johannes Ibrahim, 2004, *Kartu Kredit-Dilematis Antara Kontrak dan Kejahatan*, Refika Aditama, Jakarta, p.9

Carding is credit card fraud if the perpetrator knows someone's valid credit card number, then the perpetrator can buy goods on-line whose bill is addressed to the original owner of the credit card, while the perpetrator is called a carder.[15]

Carding crimes have two scopes, namely national and transnational, nationally carding perpetrators are within the scope of one country, while transnational is carding perpetrators do it across national borders. According to John Ibrahim[16] Credit card abuse can be done in two ways, namely:

- The credit card is valid but is not used according to the regulations specified in the agreement agreed by the credit card holder with the bank as the credit card manager.
- Unauthorized/fake credit cards used illegally too.

Internationally cyber law is used for legal terms related to the use of information technology. Based on the special characteristics found in cyberspace, where regulation and law enforcement cannot use traditional methods, some experts are of the view that activities in cyberspace should be regulated by separate laws, as the growth of the law of merchant (*Lex Mercatoria*) in the Middle Ages. . So there are several theories that can be used in cyber law, including:[17]

- *The Theory of the Uploader and the Downloader* Based on this theory, a country can prohibit in its territory, uploading and downloading activities that are thought to be against its interests. For example, a country may prohibit anyone from uploading gambling activities or other destructive activities within the country's territory, and prohibit anyone within its territory from downloading such gambling activities.
- *The Law of the Server Theory*. This theory treats the server where the webpages are physically located. According to this theory, webpages located on servers at Stanford University are subject to California law.
- *The Theory of International Spaces.* Cyberspace is considered the fourth space. The analogy lies not in the physical similarity, but in the international nature.

Meanwhile, the international legal instrument that currently receives the most attention related to cyber crime is the Convention on Cyber Crime of 2001 which was initiated by the European Union. Even though this Convention was originally made by European Regional organizations, in its development it is possible to be ratified and accessed by any country in the world that has a commitment in efforts to overcome cyber crime.

The considerations for establishing this convention are as follows:[18]

- That the international community is aware of the need for cooperation between countries and industry in combating cybercrime and the need to protect legitimate interests within a country and the development of information technology.

---

[15] Ade Ary Syam Indradi, 2006, *Carding: Modus Operandi, Penyidikan dan Penindakan*, Pensil, Jakarta, p.36

[16]Op.cit., p. 84

[17]Mehda Zuraida, Credit Card Fraud (*Carding*) dan Dampaknya Terhadap Perdagangan Luar Negeri di Indonesia, *Jurnal Analis Hubungan Internasional*, Vol 4. No.1. (2015) p. 1634. http://journal.unair.ac.id/downloadfull/JAHI8825-43c28a9ecdfullabstract.pdf

[18]Mehda Zuraida, Ibid. p. 1634-1635

- The current convention is needed to curb the misuse of computer systems, networks and data to commit criminal acts. Thus, there is a need for legal certainty in the investigation and prosecution process at the international and domestic levels through an international cooperation mechanism that can be achieved, trusted and quickly.
- Currently, there is an increasingly real need to ensure a conformity between the implementation of law enforcement and human rights (HAM) and the 1996 United Nations Covenant on political and civil rights which provide protection for freedom of opinion such as expression, which includes the freedom to seek, receive and impart information and opinion

In the event that the crime of carding in Indonesia has been regulated regarding the crime of carding in Act No. 19 of 2016 as amended to Act No. 11 of 2008 concerning Information and Electronic Transactions, there are 2 Articles that can be used to ensnare the perpetrators of the crime of Carding. , namely in Article 31 and Article 35 which reads:

Article 31

(1) Every Person intentionally and without rights or against the law intercepts or intercepts Electronic Information and/or Electronic Documents in a certain Computer and/or Electronic System belonging to another Person.
(2) Every Person intentionally and without rights or against the law intercepts the transmission of Electronic Information and/or Electronic Documents that are not public from, to, and within a certain Computer and/or Electronic System belonging to another Person, both of which do not cause any changes or which causes changes, omissions, and/or termination of Electronic Information and/or Electronic Documents that are being transmitted.
(3) Except for the interception as referred to in paragraphs (1) and (2), interception is carried out in the context of law enforcement at the request of the police, prosecutors, and/or other law enforcement institutions stipulated by law.
(4) Further provisions regarding the interception procedure as referred to in paragraph (3) shall be regulated by a Government Regulation

Article 35

Every Person intentionally and without rights or against the law manipulates, creates, changes, deletes, destroys Electronic Information and/or Electronic Documents with the aim that the Electronic Information and/or Electronic Documents are considered as if the data is authentic.

3.2. Barriers to Law Enforcement for Carding Crime in Indonesia

The crime of carding is a transnational crime so that the applicable jurisdiction is an extraterritorial jurisdiction to establish, implement and enforce legal provisions that have been established by a country. In terms of overcoming transnational crimes, the principle of *aut dedere aut judicare* is known, which means "Every State is obliged to prosecute and prosecute perpetrators of

international crimes and is obliged to cooperate with other countries in arresting, detaining and prosecuting and prosecuting international criminals.

The Indonesian Criminal Code does not yet regulate legal jurisdiction over crimes in the cyber world so that it will have an impact on the protection of a person's privacy rights.[19] In the cyber world, the problem of protecting personal rights (privacy rights) is closely related to the protection of one's personal data because currently the development of technology in the internet world has progressed very rapidly so that people can access one's personal data without the knowledge of the parties involved.

People who violate this provision can be sued for the losses caused. As stated in Article 26 of Act No. 19 of 2016 as amended to Act No. 11 of 2008 concerning Information and Electronic Transactions that:

- Unless otherwise stipulated by the Laws and Regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the consent of the person concerned.
- Any person whose rights are violated as referred to in paragraph (1) may file a lawsuit for the losses incurred under this Law.
- Each electronic system operator is obliged to delete irrelevant electronic information and/or electronic documents under his control at the request of the person concerned based on a court order.
- Each electronic system Operator is required to provide a mechanism for deleting electronic information and/or electronic documents that are no longer relevant in accordance with the provisions of laws and regulations.
- provisions regarding the procedure for deleting electronic information and/or electronic documents as referred to in paragraph (3) and paragraph (4) are regulated in a government regulation."

In dealing with carding criminal cases, there are factors that become obstacles. These constraints become a task that must be fulfilled so that in handling cases of criminal acts of theft of data and credit card information this does not cause problems in conducting investigations into criminal acts of theft of data and credit card information.

The existence of cybercrime in cyberspace creates its own difficulties in the law enforcement process. Difficulties that arise for example in determining the location of the case (*locus delicti*). The location becomes difficult to determine when from their country, the perpetrator steals data from foreign citizens. Investigators also had difficulty finding witnesses who saw or heard of the incident. Another difficulty arises in terms of gathering evidence. The collection of this evidence requires no small amount of money because it must use adequate technology and be operated by skilled human resources.[20]

Referring to the opinion of Richard Boscovich, senior lawyer from the Digital Crimes unit, there has to be a corresponding statute in another country from which you are requesting information. If you look at international treaties, it

[19]Ahmad M. Ramli. 2009, Perencanaan Pembangunan Hukum Nasional Bidang Teknologi Informasi dan Komunikasi. Badan Pembinaan Hukum Nasional Republik Indonesia, Jakarta, p. 45.
[20]Josua Sitompul, Cyberspace, Cybercrime, Cyberlaw: Tinjauan Aspek Hukum Pidana, PT. Tatanusa, 2012, p. 103

has to be a crime in both countries for you to even get that evidence in or back to your own jurisdiction.[21]

The handling of transnational crimes requires that it be carried out not only by one country but through cooperation between countries. Crime no longer stops at the border. However, along the way, the cooperation between countries sometimes encounters difficulties because it is related to the sovereignty of a country, differences in culture, language and differences in the legal system.

So that law enforcement does not merely mean the implementation of legislation, although in reality in Indonesia the trend is so, so the notion of law enforcement is so popular. In addition, there is a strong tendency to interpret law enforcement as the implementation of judges' decisions. It should be noted that these rather narrow opinions have weaknesses, if the implementation of the legislation or the judge's decisions actually disturbs the peace in social life.

4. Closing

Based on the discussion above, the authors conclude that in carrying out the enforcement of this carding crime, they can be charged with Act No. 11 of 2008 concerning Information and Electronic Transactions and international conventions that have been ratified. As well as obstacles in carrying out the enforcement of the crime of carding, because this crime is transnational in nature, it requires rules that have broad jurisdiction, or an agreement with other countries is needed to be able to arrest and punish perpetrators who commit criminal acts in the jurisdiction of countries that have international agreements with other countries. Indonesia.

5. References

Journal

[1] Takwa. Megat Kalti, Evi Deliana, Ferawati, 2018, Pertanggungjawaban Pidana Terhadap Pemilik Domain Cara Melakukan *carding* Berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Informasi dan Transaksi Elektronik, *JOM Fakultas Hukum*, Vol. V No. 2.

[2] Zuraida, Mehda, 2015. Credit Card Fraud (*Carding*) dan Dampaknya Terhadap Perdagangan Luar Negeri di Indonesia*, Jurnal Analis Hubungan Internasional*, Vol 4. No.1.

[3] Situngkir, Feri Vernando & Siti Rodhiyah Dwi Istina, 2020, The Enforcement of Criminal laws of Hate Speech in Social Media*, Law Development Journal*, Vol. 2 Issue 4.

Book

[1] Arief, Barda Nawawi .2007. *kapita selekta hukum pidana tentang sistem peradilan terpadu*. Undip Press. Semarang.

[2] Diantha, I Made Pasek. 2016. *Metodologi Penelitian Hukum Normatif dalam Justifikasi Teori Hukum*, Prenada Media Group. Jakarta.

[21] Lauren Moraski, 2011, Cybercrime Knows No Borders (online), http://www.infosecuritymagazine.com/view/18074/cybercrime-knows-no-borders-/, (01 June 2021)

[3] Efendi, Erdianto. 2011. *Hukum Pidana Indonesia-Suatu Pengantar*, Refika Aditama, Bandung.
[4] Ibrahim, Johannes. 2004, *Kartu Kredit-Dilematis Antara Kontrak dan Kejahatan*, Refika Aditama, Jakarta.
[5] Indradi, Ade Ary Syam. 2006. *Carding: Modus Operandi, Penyidikan dan Penindakan*. Pensil. Jakarta.
[6] Jovan. 2006. *Pembobol Kartu Kredit Menyingkap Teknik dan Cara Kerja Para Carder di Internet*, Mediakita, Jakarta.
[7] K, Alvin Novryan. 2014. *Pencegahan Kejahatan Carding sebagai kejahatan Transnasional menurut hukum Internasional*. Fakultas Hukum Brawijaya. Malang.
[8] M, Didik. Arief Mansur dan Elistaris Ghultom, 2005, *Cyber law-Aspek Hukum Teknologi Informasi,* Refika Asitama, Bandung.
[9] Makarim, Edmon. 2005. *Pengatar Hukum Telematika*, PT Raja Grafindo Persada, Jakarta.
[10] Prasetyo, Teguh & Abdul Halim, 2005, *Politik Hukum Pidana*, Pustaka Pelajar, Yogyakarta.
[11] Syahdeini, Sutan Remy. 2009. *Kejahatan dan Tindak Pidana Komputer*, PT Pustaka Utama Grafiti, Jakarta.

Thesis

[1] Handoko, Cahyo. 2017. Tinjauan Hukum Pidana Terhadap Cardin Sebagai Salah Satu Bentuk Cybercrime, *Tesis*, Universitas Muhamadiyah Surakarta.

Regulation

[2] Act No. 19 of 2016 concerning amendments to Act No. 11 of 2008 concerning Information And Electronic Transactions