RESEARCH ARTICLE

Misuse of Credit Cards or Carding in Indonesia: How is the Law Enforced?

Adib Nor Fuad
Indonesian Technology Law Society Movement
✉ adibnorfuad@gmail.com

OPEN ACCESS

Citation: Fuad, A. N. (2021). Misuse of Credit Cards or Carding in Indonesia: How is the Law Enforced?. Law Research Review Quarterly, 7(1), 83-96. https://doi.org/10.15294/lrrq.v7i1.43165

Submitted : October 13, 2020
Revised : December 23, 2020
Accepted : January 15, 2021

ISSN **2716-3415**
Law Research Review Quarterly published by Faculty of Law, Universitas Negeri Semarang, Indonesia. Published quarterly on February, May, August, and November.

Abstract

Misuse of credit cards or cards is a negative impact of the times, the advancement of the internet, and the increasingly sophisticated information technology that has resulted in e-commerce activities in countries around the world including Indonesia. Several carding crime cases in Indonesia have troubled many credit card users. This research aims to analyze and examine the criminal law enforcement on misuse of credit cards in Indonesia. This paper highlighted and found that in overcoming crimes in cyberspace, the government issues special regulations for crimes in which the action uses electronic devices and internet networks, namely the Republic of Indonesia Law No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 1 of 2008 which regulates Information and Electronic Transactions or ITE. This regulation aims to suppress carding crimes that are increasingly happening in Indonesia.

Keywords: *Cybercrime; Misuse of Card; Criminal Law*

1. INTRODUCTION

Changes in times and technological developments are two things that are basically inseparable and are directly proportional to each other. Therefore, the more advanced an era is, the more technology used in that era will be developed, because it is based on the human mindset who always wants to create new things to facilitate every human job itself. The presence of the progress of the times has a major influence on various aspects of human life, both positive and negative aspects (Suseno & Barmawi, 2004).

Human awareness to get education and knowledge, brings these humans to always experiment and compete in developing technology in this modern era, such as computer and internet devices which were originally created for military or defence needs and have now been developed and are increasingly easy for all people to feel the product of an advance in human thought in the field of technology. The sophistication of computer technology has provided conveniences, especially in helping human work (Hermawan, 2015; Pirog & Roberts, 2007). The positive impact of advances in information technology can be seen in everyday life. Among other things, the convenience in daily work. The simplest example, we can see in the Word Processor program, such as Microsoft Word, Open Office. Besides, one of the products of science and technology is information technology or what is commonly known as telecommunication technology which has used the internet network. Telecommunication technology has helped mankind to interact with humans in other communities more easily, in the sense that this can be done without leaving the place or community where it is located and this activity can be done anywhere and anytime (Wahid & Labib, 2005).

The presence of the progress of the era is impactful negative users. Related to the existence of trading transactions via the internet or online, the crimes that are felt by users that often occur in Indonesia, one of which is a theft whose object is a card or what is often referred to as carding. Carding is fraud on a credit card, the perpetrator looks for information or someone's credit card number data that is still valid, with that the perpetrator can misuse it for his personal interests, such as spending on online media where the bill is charged to the original owner of the credit card, while the perpetrator is called a carder (Indradi, 2006; Pujiuono, 2020; Hartono, 2013). Based on the crime, the legal owner of the credit card will lose the money or balance on the credit card because it was misused by the criminal. by stealing the credit card owner's credit card account. This kind of account theft can be done by breaking through the security of online shops that the victim has previously made transactions with. If these online shops are not equipped with stronger security, more and more credit card accounts can be stolen by the perpetrator.

Referring to the facts of cybercrime that often occurs in Indonesia, we can conclude that cybercrime is a serious threat in the non-traditional security sector. Where a crime that uses computer devices and internet networks (cybercrime) in Indonesia, has entered the highest order in the world.

The term security is currently known as one of the capabilities of a country in defining the concept of a threat, which focuses on military aspects in its resolution. As stated by Walt, security studies are a phenomenon of war which is defined as, the study of threat, use, and control of the military force (Indradi, 2006; Fuady, 2005; Abidin, 2017). However, after the end of the cold war, the term security underwent a change in meaning, that security includes broader aspects such as environmental, social, cultural, human rights, economic and so on. This change in the concept and meaning of security, is due to the increasing progress that has occurred, such as globalization with a revolution in the scope of communication technology that allows no distance and is supported by the easier means of transportation in the world. This condition affects the development of problematic issues in global politics, including security issues in Indonesia.

In addition to the threat and security instability due to the fast pace of technological development at this time, the people's need for convenience in carrying out daily activities has made credit cards a payment instrument that is increasingly popular in the world community and even Indonesia. Credit card as a means of payment is a type of APMK which has been in use for the longest time in this country since the 1980s. Initially, credit card holders were still limited to certain social groups and their use was intended for special payments. This development was actually driven by various factors relating to ease of use, practicality and cardholder self-image (Muhammad & Murniati, 2000; Ahmad, 2012). Therefore, it is necessary to have special handling in preparing and dealing with crimes committed by individuals who have special expertise in the field of technology.

2. METHOD

The author uses the case study method by taking the Carding cases which is currently rife in Indonesian society, and with the normative juridical method, which is based on the main legal material by examining the laws and regulations related to this research. In sampling was not carried out on people, but library materials, especially related to information regulations and electronic transactions. The data used are secondary data. Secondary data comes from library materials and legal materials that are accurate and valid. How to identify problems by collecting library data in the form of archives, official documents, other library data that is closely related to research problems, namely Analysis of Credit Card Abuse or Carding in Indonesia. The final result of data processing are qualitative, then analyzed by qualitative-normative methods, the method of interpretation in law. It is hoped that the results of this writing can be useful and as a reference for the knowledge of other readers.

3. RESULT AND DISCUSSION

A. Credit or Carding Misuse as Cybercrime in Indonesia

The term Carding is quite widely used in activities related to credit cards, for example e-commerce transactions. Why is it called carding, because in e-commerce website transactions the payment system is made using a credit card, and not a physical credit card, but it is enough to know the credit card numbers and the expiration date. Carding is fraud on a credit card if a perpetrator knows a person's credit card number is still valid, then the perpetrator can buy goods online where the bill is charged to the original owner of the credit card or victim, while the perpetrator is called a carder (Indradi, 2006). Another term for crimes of this type is cyber fraud, aka fraud in cyberspace (Raharjo, 2002). Carding has two scopes, namely, national, and transnational. National scope, is the carding actor committing his crime within the scope of a particular country and Transnational, is the actor carding across certain country borders. Furthermore, there are two ways to misuse credit cards (Ibrahim, 2004; Mansur, 2005), namely:

1) credit card is valid but not used in accordance with the regulations specified in the agreement agreed by the credit card holder with the bank as the credit card manager.
2) invalid credit card or fake credit that is used illegally as well.

Carding is a crime that is included in cybercrime. The forms of cybercrime that are generally recognized in society are divided into 3 (three) general qualifications (Arief, 2006), namely:

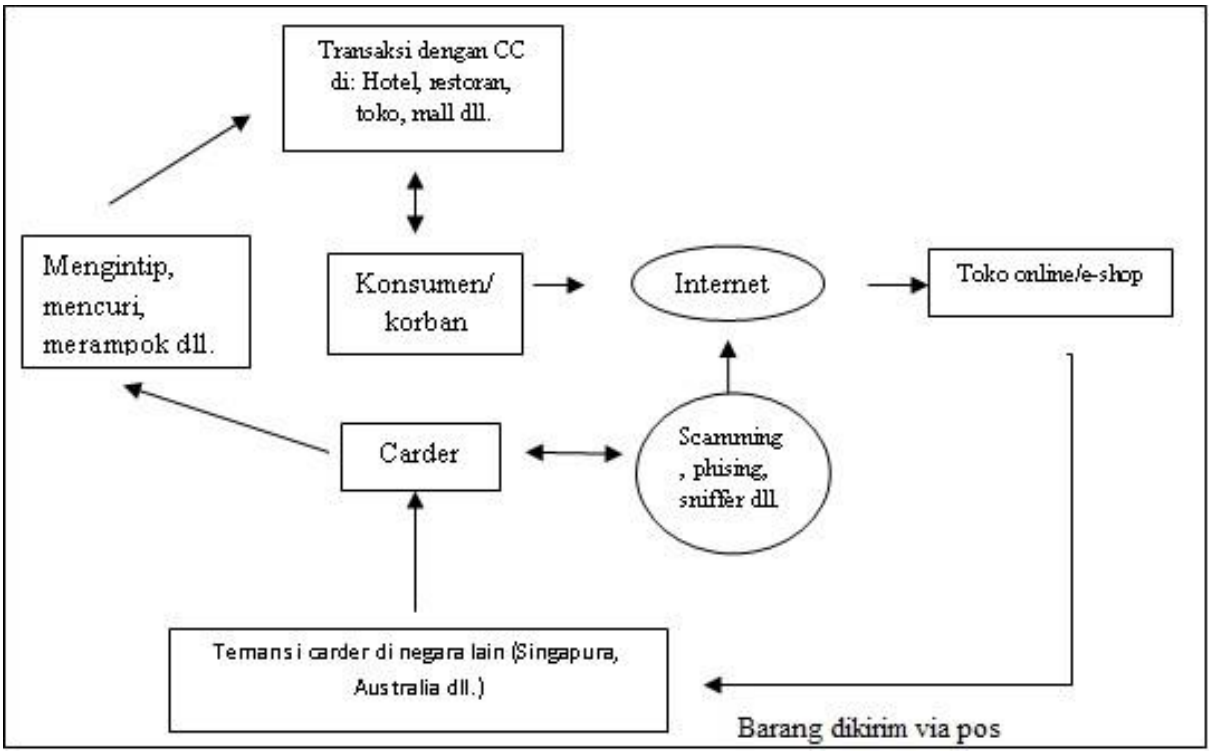
1) Evil cyberspace relating to the confidentiality, integrity and existence of data and computer systems.
2) Evil cyberspace that uses computers as a tool of crime.
3) Evil cyberspace relating to the content or content of data or computer systems.

Of the several forms of crime in cyberspace or what is often referred to as cybercrime that has been described above, it often occurs in Indonesia, one of which is the carding crime itself, this type of crime is more focused on buying and selling transactions whether it is carried out online (in network) or physically or directly.

Furthermore, carding is done by using a credit card belonging to another person whose number has been stolen to shop at a shop or shopping place that accepts payment using a credit card such as modern shopping places, malls, jewellery stores, and all places with logos. Master, Visa, Maestro, Cirrus, American-Express and other types. Credit card multiplication is done by reading the victim's credit card data using MSR (*Magnetic StripeCard Reader*), after which the data is written into a blank card or what is often called a fake card using MSR. The next step is to spend directly to various places that serve credit card payments (Muhammad & Murniati, 2000; Putra, 2016; Zuraidah, 2015).

Another case with the online method, carding is done by using a credit card belonging to another person or a victim or someone else's credit card number to shop at online shopping places. Credit card hacking technique aka carding, which is to steal transaction data from the manager of an online shopping service by a black hacker. Furthermore, the data on the credit card owner from this database is stolen by the perpetrator used for the transaction, then the bill will automatically go to the owner of the credit card or the victim of the carding crime.

In simple terms, the mode used by most carders is as follows:


Transaksi dengan CC di: Hotel, restoran, toko, mall dll.
Mengintip, mencuri, merampok dll.
Konsumen/ korban
Internet
Toko online/e-shop
Carder
Scamming , phising, sniffer dll
Temansi carder di negara lain (Singapura, Australia dll.)
Barang dikirim via pos

B. The Occurrence of Carding in Indonesia

The loss of time and space boundaries on the Internet changes many things. The rapid development in the use of internet services in the end invites the occurrence of crime, which is better known as Cybercrime. Indonesia as one of the most densely populated countries in the world cannot be separated from this problem (Arifah, 2011). Just as the needs of modern society in facilitating daily activities seem to be primary needs, because modern society is now starting to shift to carry out activities instantly and quickly. Such as the need for a payment instrument that users feel is more efficient, comfortable, and easy to use. This credit card payment tool is one of the most sought after or most in demand by the public. Based on the Bank Indonesia Payment and Money Circulation System Report Data or BI LSPPU, it is stated that, in 2009, the number of credit card holders in Indonesia had reached more than 12 million credit card holders from a total of 20 issuers in Indonesia.

The development of the number of credit card holders from 2000 to 2009 in Indonesia shows that the need for credit cards has increased in line with the advancement of the banking industry. The increasing trend in society, the number of cards during this period of time contributed to an increase in their use. On the value side, annual growth reaches 30%, meanwhile, on the volume side, it reaches 19%. This can be seen from Figure 1 (LSPPU BI, 2009; Panjaitan, 2012) below:

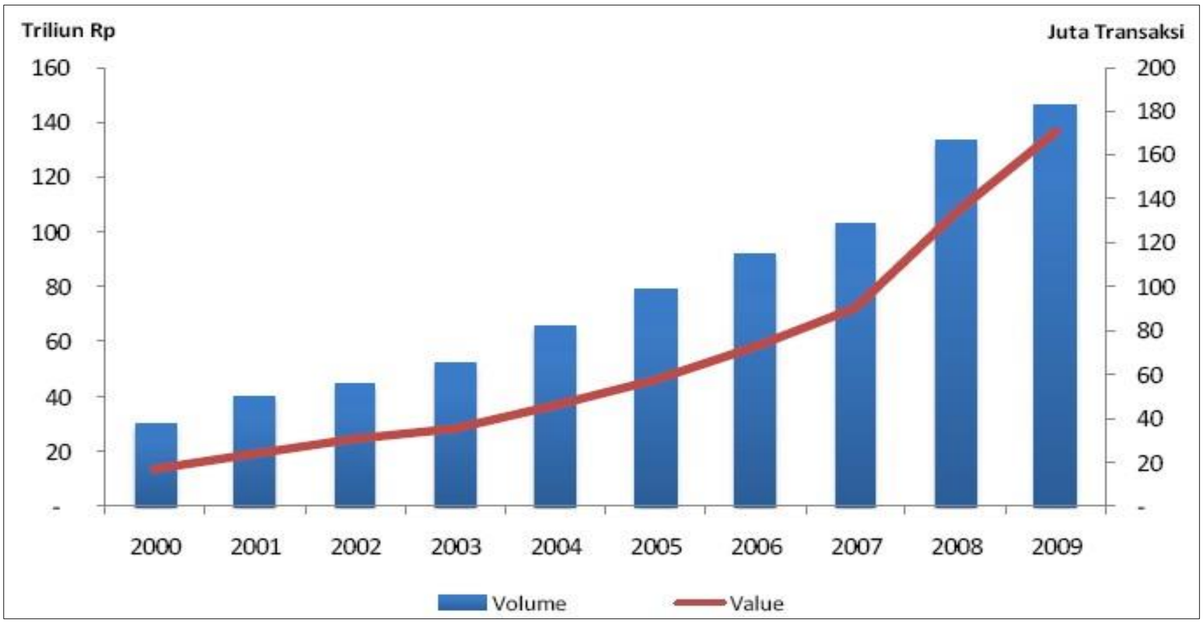


Figure 1 Total Value and Volume of Credit Card Transactions in Indonesia

Based on this table, it can be concluded that modern society wants things that are easier, more efficient, safer, and faster. However, the practice of the credit card industry in Indonesia is not completely safe from credit card criminals or hackers who are always looking for profit from their victims.

Carding as a type of cybercrime has become a crime that has troubled many credit card users in Indonesia, therefore the Indonesian Police (POLRI) responded by forming a special unit at the POLRI Headquarters level called the Directorate of Cyber Crime, which is manned by personnel are trained to handle cases of this kind, not only in investigation and investigation techniques, but also they master special techniques for security, and confiscation of evidence electronically (Mahfud MD, 2000).

The phenomenon of cybercrime has to be watched out for because this crime is somewhat different from other crimes in general. Cybercrime can be carried out without knowing territorial boundaries and there is no need for direct interaction between the perpetrator and the crime victim (Sudarwanto, 2009).

With so many credit card users in Indonesia, it will bring a crime described above, namely Carding, often law enforcement officials arrest the perpetrator who has troubled many of the credit card users in Indonesia. As was the case in Indonesia in March, The East Java Regional Police have succeeded in uncovering ITE crimes committed by spamming and carding. The mode used by the perpetrator in carrying out his crimes is by stealing other people's credit card data which is then used to buy goods through shopping stores on the internet with that credit card. The perpetrator of the carding crime was arrested by the East Java Regional Police. It is known that the perpetrator with the initials IIR is a 27-year-old resident of Bojonegoro and his friend, ZU, a resident of Malang, East Java.

This case developed from online transactions, using a modified credit card to commit crimes (Rinanda, 2018). The spamming and carding perpetrators committed crimes using smart phones. First, they signed in with fake accounts on Apple and Paypal. From this account, they can steal data in the form of credit card numbers and expiration dates. After the perpetrator succeeds in stealing, the perpetrator then spends it on shopping sites in cyberspace. The perpetrator will then sell these goods so that they can be used as money for the perpetrators' living expenses. Based on the perpetrators' information, they had successfully broken into credit cards totalling Rp. 500,000,000.

The perpetrator was charged under Article 30 paragraph (2) and / or Article 32 paragraph (1) RI Law No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 1 of 2008 concerning Information and Electronic Transactions (ITE) and Article 46 (2) of Law of the Republic of Indonesia No. 19 of 2016 concerning amendments to Law of the Republic of Indonesia No. 1 of 2008 concerning Electronic Information and Transactions, with a maximum imprisonment of seven years and a maximum fine of Rp. 700 million.

C. *Law Enforcement Efforts Against Carding Players in Indonesia*

Cybercrime which is basically the impact of technological developments that have changed the habits of society from a conventional nature to a habit that is more modern or can be called a high technology society (Putra, 2016). *Cybercrime* can be called a crime related to the interests of a person or group of people. There is someone who uses or is used to expand the reach of cybercrime. The interests of business, politics, culture, religion and so on can be motives, reasons and arguments that make a person and a group of people fall into cybercrime (Ismail, 2009).

Based on the current state of cybercrime that is rife in Indonesia, we can see that cybercrime by means of Carding is a serious threat to the non-traditional security sector as described above. Crime using computer equipment and internet networks (cybercrime) in Indonesia, is among the highest in the world (Mehda, 2015). Factors causing the rate of development of cybercrime tend to increase from year to year (Mansur & Gultom, 2005), namely:

1) Public Legal Awareness
   There is a lack of legal awareness among the people in responding to cybercrime activities. This is due, among others, to the lack of understanding and knowledge of the public regarding the types of cybercrime. This lack of understanding and knowledge causes the efforts to overcome cybercrime to experience obstacles. In this case, the constraints are related to legal structuring and the process of public monitoring of any activity that is suspected of being related to cybercrime.
2) Safety factor
   The criminals will feel a sense of security when they are carrying out the action. This is because the internet is generally used in relatively closed places. As a result, when the perpetrator is committing a crime, it is very rare for people to know about it. If the perpetrator has committed a crime, the perpetrator can easily erase all traces of the crime that has been committed. When the perpetrator is caught, it is difficult for law enforcement officials to find evidence of the crime.
3) Law Enforcement Factors
   Law enforcement factors are often one of the causes of the rampant cybercrime. This is motivated by the lack of law enforcement officers who understand the ins and outs of information technology, so that when a criminal is arrested, law enforcement officials find it difficult to find evidence that can be used to ensnare the perpetrator, especially if the crime committed has a very complicated operating system.

Another factor in influencing someone to commit this carding crime is the necessity of life, as has been reported in various mass media and electronic media which shows that someone commits a crime, including theft of various types, due to insufficient economic needs. someone thinks that stealing can make ends meet, but for whatever reason stealing cannot be justified and needs serious attention because it cannot be separated from community life and can disturb the stability of social harmony (Firmansyah, 2012).

Furthermore, criminal law as social control is used to tackle crimes in the form of violations of norms related to the use of potentially criminal information technology, in order to provide protection to the public from the dangers of these crimes (Supanto, 2016).

In Indonesia, at the beginning of this carding case, in its handling of carding it was categorized as a crime of theft, in which the definition of theft according to the law and its elements has been formulated in Article 362 Indonesian Penal Code (KUHP) that: *Whoever takes an object entirely or part of the property of another person, with the intention of being illegally owned, is threatened with theft, with a maximum imprisonment of 5 years or a maximum fine of nine hundred rupiahs*". In this crime, then after the existence of the ITE Law, which specifically regulates cases of crimes in cyberspace, one of which is carding crimes which can be criminalized by applying Article 31 paragraphs 1 and 2 which discusses hacking. Because one of the steps or practices is to get other people's credit card numbers by or hacking into official websites of institutions that provide credit cards to penetrate the security system and steal the card numbers.

The sound of article 31 which explains about acts that are considered to be against the law according to the ITE Law in the form of illegal access: Article 31 paragraph 1: "*Every person intentionally and without right or against the law intercepts or eavesdrops on electronic information and / or electronic documents in a computer and / or electronic system in a certain way belonging to another person*." Article 31 paragraph 2: "*Every person intentionally or without right or against the law conducts interception or electronic transmission and / or electronic documents that do not have a public status from, to and within a computer and / or certain electronic system belonging to another person, whether it does not cause change, removal and or* *termination of electronic information and or electronic documents transmitted.* "

So far, carding cases in Indonesia can be resolved with the old regulations, namely article 362 in the Criminal Code and Article 31 paragraphs 1 and 2 in the ITE Law. In handling carding cases, special regulations are needed to regulate carding crimes, so that cases like this can be reduced and even no longer exist because it is very detrimental to the people who use them. However, in addition to special regulations, it must also be supported by system security both software and hardware, stronger and stronger guidelines against hacker threats, and making policies related to computer-related crime and support from special institutions (Ahmada, 2012; Sidik, 2013).

5. CONCLUSION

This research concluded that with the progress of the times, the human mindset will increasingly advance to compete in technological science to facilitate all human activities. So, the advancement of technology has provided a very broad source of information and communication from what humans already have. The internet activities cannot be separated from the human factor and its legal consequences also touch humans in society who are in the physical world, then there is a thought about the need for legal rules to regulate activities in cyberspace. Furthermore, in the development of a society that is experiencing rapid changes and advances due to globalization and technology, especially information technology, it is necessary to have legal regulations that can regulate human activities in relation to the use of information technology, so that in using or utilizing it, it does not harm or can be harmed personally. With the rise of cybercrime, the Indonesian government seeks to overcome and suppress these crimes, because most and the majority of the population in Indonesia have used and depend on technology.

5. DECLARATION OF CONFLICTING INTERESTS

The authors state that there is no potential conflict of interest in the research, authorship, and/or publication of this article.

6. FUNDING

None

7. ACKNOWLEDGEMENT

None

8. REFERENCES

Abidin, D. Z. (2017). Kejahatan dalam Teknologi Informasi dan Komunikasi. *Jurnal Processor*, *10*(2), 509-516.

Ahmad, A. (2012). Perkembangan Teknologi Komunikasi Dan Informasi: Akar Revolusi dan Berbagai Standarnya. *Jurnal Dakwah Tabligh*, *13*(1), 137-149. https://doi.org/10.24252/jdt.v13i1.300.

Arief, B. N. (2006). *Tindak Pidana Mayantara dan Perkembangan Kajian Cyber Crime di Indonesia*. Jakarta: Rajawali Pers.

Arifah, D. A. (2011). Kasus Cybercrime di Indonesia. *Jurnal Bisnis dan Ekonomi*, *18*(2), 185-195.

Buzan, B. (2008). *People, States & Fear: An Agenda for International Security Studies in The Post-Cold War Era*. New York: Ecpr Press.

Firmansyah, D. (2012). Upaya Polri Dalam Penanggulangan Tindak Pidana Pencurian Sepeda Motor Dengan Kekerasan (Studi Pada Kepolisian Sektor Pakuan Ratu). *Jurnal Poenale, 2*(4), 413-422.

Fuady, M. E. (2005). "Cybercrime": Fenomena Kejahatan melalui Internet di Indonesia. *Mediator: Jurnal Komunikasi*, *6*(2), 255-264. https://doi.org/10.29313/mediator.v6i2.1194.

Hartono, B. (2013). Penerapan Sanksi Pidana Terhadap Tindak Pidana Carding. *Pranata Hukum*, *8*(2), 168-177. http://jurnal.ubl.ac.id/index.php/PH/article/view/197.

Hermawan, R. (2015). Kesiapan Aparatur Pemerintah dalam Menghadapi Cyber Crime di Indonesia. *Faktor Exacta*, *6*(1), 43-50. http://dx.doi.org/10.30998/faktorexacta.v6i1.217.

Ibrahim, J. (2004). *Kartu Kredit: Dilematis antara Kontrak dan Kejahatan*. Jakarta: Refika Aditama.

Indradi, A. A. S. (2006). *Carding: Modus Operandi, Penyidikan, dan Penindakan*. Jakarta: PTIK.

Ismail, D. E. (2009). Cyber Crime di Indonesia. *Jurnal Inovasi*, *6*(3), 242-247.

Mahfud M.D. (2000). *Politik Hukum Nasional*. Bandung: Alumni.

Mansur, D. M. A. (2005). *Cyber Law: Aspek Hukum Teknologi Informasi*. Semarang: Tiga Serangkai.

Mansur, D. M. A., & Gultom, E. (2005). *Cyber Law Aspek Hukum Teknologi Informasi*. Bandung: Refika Aditama.

Muhammad, A., & Murniati, R. (2000). *Segi Hukum Lembaga Keuangan dan Pembiayaan*. Jakarta: Citra Aditya Bakti.

Panjaitan, L. T. (2012). Analisis Penanganan Carding dan Perlindungan Nasabah dalam Kaitannya dengan Undang-Undang Informasi dan Transaksi Elektronik No. 11 Tahun 2018. *IncomTech: Jurnal Telekomunikasi dan Komputer*, *3*(1), 1-26. http://dx.doi.org/10.22441/incomtech.v3i1.1111.

Pirog, S. F., & Roberts, J. A. (2007). Personality and credit card misuse among college students: The mediating role of impulsiveness. *Journal of Marketing Theory and Practice*, *15*(1), 65-77. https://doi.org/10.2753/MTP1069-6679150105.

Pujoyono, N. W. (2020). Penal Policy dalam Upaya Preventif Kejahatan Carding di Indonesia. *Jurnal Panji Keadilan: Jurnal Ilmiah Nasional Mahasiswa Hukum*, *3*(1), 86-98. https://doi.org/10.36085/jpk.v3i1.1183.

Putra, A. K. (2016). Analisis Hukum Yurisdiksi Tindak Kejahatan Siber (Cybercrime) Berdasarkan Convention on Cybercrime. *Jurnal Ilmu Hukum*, *7*(1), 22-54.

Raharjo, A. (2002). *Cybercrime: Pemahaman dan Upaya Pencegahan Kejahatan Berteknologi*. Jakarta: Citra Aditya Bakti.

Republic of Indonesia. (2008*). Law Number 11 of 2008 concerning Information and Transactions Electronic.*

Republic of Indonesia. *Indonesian Penal Code (Kitab undang-Undang Hukum Pidana).*

Rinanda, H. M. (2018, March). "Pelaku Spamming dan Carding dibekuk Bobol Kartu Kredit Rp. 500 juta", *News Detik Online,* retrieved from https://news.detik.com/berita-jawa-timur/d-3927140/pelaku-spamming-dan-carding-dibekuk-bobol-kartu-kredit-rp-500-juta.

Sidik, S. (2013). Dampak Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) terhadap Perubahan Hukum dan Sosial dalam Masyarakat. *Jurnal Ilmiah Widya*, *1*(1), 1-7.

Sudarwanto, A. S. (2009). Cyber-Bullying Kejahatan Dunia Maya Yang Terlupakan. *Jurnal Hukum Pro Justitia*, *27*(1), 1-16.

Supanto, S. (2016). Perkembangan Kejahatan Teknologi Informasi (Cyber Crime) dan Antisipasinya dengan Penal Policy. *Yustisia, 5*(1), 92-117. https://doi.org/10.20961/yustisia.v5i1.8718.

Suseno, S., & Barmawi, S. A. (2004). Kebijakan Pengaturan Carding dalam Hukum Pidana di Indonesia. *Sosiohumaniora*, *6*(3), 245. https://doi.org/10.24198/sosiohumaniora.v6i3.5532.

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cybercrime)*. Bandung: Refika Aditama.

Zuraida, M. (2015). Credit Card Fraud (Carding) dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia. *Jurnal Analisis Hubungan Internasional, 4*(1), 1627-1641.

Cybercrime is the greatest threat to every company in the world.

Ginni Rommety

ABOUT AUTHORS

Abid Nor Fuad, SH is a researcher and activist in the Indonesian Technology Law Society Movement. He graduated from the Faculty of Law Universitas Negeri Semarang, Indonesia. Besides his activities as a researcher he also actively advocates for some people, especially on cybercrime cases.