Carding Crime Analysis as A Form of Cyber Crime in Indonesia's Criminal Law

Novi Asih Muharam[1], Azis Budianto[2]
{novighezhaa@gmail.com}

Universitas Borobudur, Jakarta, Indonesia[12]

Abstract. The objective of this study is to learn much about the regulation. of the crime of carding in Indonesian criminal law and to find out more about efforts to overcome the crime of carding. The findings of this study show that the murder of frisking is controlled in Law No. 19 of 2016 amending Act No. 11 of 2008 concerning Digital Transactions, and that 've got for the violence of scoring besides the Rules on Digital Activities and Data can be devised in the Revised Penal code to use a vast depending upon the context of the publications stored in the Crpc. The control of frisking crimes in Indonesia is governed according to the modus operandi in the legislation, which is included in the Criminal Code, specifically Articles 362, 363, and 378 of the Criminal Code relating theft and fraud. Special rules well outside Sedition Act, namely Law No. 19 of 2016 amending Law No. 11 of 2008 concerning Relevant data and Digital Payments as lex experts, even those governed in Article 30 in relation to Article 46 as the robbery editorial, Press release 34 section (1) in relation to Article 50 as a story regarding thievery brought out in partnership by three or more individuals, and in Article 35 in tandem with Article 51 sentence (1) as an article theft carried out in collaboration by two or more people.

Keywords: Carding Crime; Cybercrime; Criminal Law

1 Introduction

The presence of the internet throughout the world is a sign that globalization is something that the world community cannot avoid.[1] Thus it can also be said that the internet and globalization are two interrelated things. The globalization of electronic and computer information technology has narrowed the world's area, shortened the distance of communication, and compacted the mobility of people and goods.[2] Everything is straightforward, easy, and fast. One of the growing global lifestyles is the use of credit cards. With a credit card in hand, everything is straightforward, easy, and fast when shopping or buying plane tickets, paying bills and bills, etc. Now there is no need to carry large amounts of money. "swipe." All affairs are in order.

Today's technological advances are sometimes not only used by the community in positive activities. However, it can also be used for making harmful activities such as development. Technological progress is also an opportunity for 'criminals' to commit crimes in cyberspace or other media, often known as cybercrime.[3]

Cybercrime is a crime in computers in general that can be interpreted as the illegal use of computers. Cybercrime is categorized into two types: limited cyberattack and broad

ICLSSEE 2022, April 16, Semarang, Indonesia

DOI 10.4108/eai.16-4-2022.2320085

cybercriminals. In a loose sense, cybercrime is a offence is committed upon illegal acts aimed at attacking computer systems. In contrast, in a broad sense, cybercrime includes crimes against illegal acts committed through computer networks and crimes using electronic means.

Computer Carding is a credit card fraud in which the culprit knows anyone's payment information that is still valid for use so that the perpetrator may buy products online whose bill can be addressed, one of the many forms of cyberattacks that happened in Indonesia. The credit card's original owner, whereas the perpetrator is known as a carder. Payment card fraud (fraud involving a credit card/debit card) is categorized as carding vocabulary, casual language, or legal speak.

This carding crime is more devoted to sales transactions, whether physical or online. Physically, carding is done by using other people's data or identities to be used for shopping at shopping places that accept credit card payments. Credit card duplication is done by reading credit card data using Magnetic StripeCard Reader. The data is written to a blank or fake card using Magnetic StripeCard Writer. Next

This card is used to shop at various places that serve credit card payments. Meanwhile, carding is done online by using other people's data or identities to shop at online shopping places. In addition, about the carding hacking technique, Specifically, a black hackers stole transaction data from the management of an online purchasing site. Consequently, the payment card boss's information from this data is used for payments by the scammer cracker, and the bill will automatically go to the credit card owner.

2 Research Methods

This is a part of study that takes place at a library. Literacy research is done with the use of literary (library), which includes publications, papers, and reporting on past research findings. Since it is focused on literatures of volumes, diaries, and descriptions of past study results, this study requires research work[4]. The technique employed is the Statutory Approach, which is related to the sort of study used, namely judicial decisions research. This method entails reviewing the rules and regulations pertaining to the difficulties (legal challenges) at hand. Since the main and key issue of study will be numerous legal laws in the modes and regulations employed by offenders of carding crimes, both physical and online, norm research needs to use a statute method.

3 Results and Discussion

Cybercrime is a criminal activity that uses It is illegal to use internet access or data centers without authorisation, either by changing it or destroying the computer facilities it enters, which can cause harm to other people. Because of that, there is a need for the regulation of cybercrime. In particular, namely carding crimes or crimes categorized as cybercrimes using the internet electronic media facilities. So the following is a table of carding crime arrangements in Indonesian criminal law based on its modus operandi.[5]

There are several ways that hackers/carders use to get this data, including SQL Injection, SQL Injection can be interpreted as an attack on a site by entering malicious commands through input media such as boxes or URLs, and phishing is a way to steal someone's data using a "subtle" way without the victim realizing that the data has been stolen. In general, phishing is done to steal email login data, credit cards, online payment tools, etc. To perform this technique, knowledge of programming languages is required; as a start, he also did spam to run the phishing. Spamming is an act of sending messages to recipients repeatedly without the recipient's will, namely some spam such as blog spam and email spam.[6]

One of the functions of the law is to ensure the smooth running of the national development process while at the same time securing the results that have been achieved; It must be ready to shield home internet customers' interests while also taking bold action versus cybercriminals. So, it is essential for the government to pass Law No. 19 of 2016 amending Law No. 11 of 2008 relating to Digital Transactions, which conducts surveillance, blocks fraudulent sites, and designs an excellent system to protect the public. From the threat of cybercrime.

Carding crime is a crime where the computer is a tool to commit the carding crime; where this carding crime is a Crime is a sort of abuse. Carding is a crime committed by stealing card numbers. Credit belonging to someone else and used in trade transactions on the internet. Criminal law is a set of rules that regulates 3 elements, namely rules regarding criminal acts, criminal responsibility and verbal processes of law enforcement if a crime occurs, which actions are threatened with criminal sanctions.

A credit card is a card issued by a particular bank to a user as a means of payment using a card. Credit cards offer two different functions to consumers, namely as a means of payment and a source of credit, so that users can buy goods and services from companies that accept the card without paying cash.

The goal of this study is to figure out how laws work in Indonesia against fraud in cybercrime and what regulations are the basis for law enforcement officers to overcome fraud in the form of online buying and selling. The authors conclude that: 1. In theory, internet scams is like traditional scam. The legal arrangement regarding the criminal act of fraud is still limited in the use of the Criminal Code. It is based on Law Number 11 of 2008 concerning Information and Electronic Transactions. Law enforcement officers often experience difficulties and obstacles in ensnaring perpetrators of fraudulent crimes. 2. This criminal act of fraud can be charged with Article 378 of the Criminal Code as a criminal act of fraud or Article 28 paragraph (1) of the ITE Law regarding the regulation regarding the spread of false and misleading news that harms consumers. Or it can be charged based on both articles at once, namely, 378 of the Criminal Code in conjunction with Article 28 paragraph (1) in conjunction with Article 45 paragraph (1) of Law No. 11 of 2008 concerning fraud and or ITE crimes.

So the law currently used in regulating cyber crime is Modifications to Law No. 11 of 2008 Regarding Data and Digital Payments, Law No. 19 of 2016, because with the rapid development of information technology, it is necessary to pay attention to efforts to improve and improve the National Criminal Code, namely: 1. The increasing number of new crimes that arise as a result of advances in information technology (cyber crime), the evidence required must be in accordance with the development of science and technology (IPTEK).), either by adding other evidence based on technology, such as evidence in the form of electronic mail (electronic mail) and electronic records; 2.

One of the characteristics of cybercrime is the use of global telematics networks (telecommunication, media and informatics). The global aspect creates conditions as if the world has no boundaries (borderless) this situation results in the perpetrators, victims and places of crime (locus delicti) occurring in different countries. Therefore, to anticipate this, the application of the Criminal Code must be expanded; 3. To formulate and determine actions that can be subject to criminal sanctions in a relatively new and fast-moving world, of course, is not an easy job. Therefore, to ensnare perpetrators who commit crimes in cyberspace (cyber crime), legal interpretation institutions (interpretation) can be used. This is intended to avoid the emergence of a legal vacuum.

So the conclusion is that regulatory efforts in dealing with cyber crime cases, especially carding crimes, The Current Law has lots of articles that criminalize cyber crime by using extensive interpretation methods of the articles contained in the Criminal Code. The articles that can be imposed in the Criminal Code that criminalize cybercrimes, especially carding crimes, include Article 362 for the carding case where the perpetrator steals someone else's credit card because it isn't physically possible since only the card info is shown taken using the card generator software. on the internet to get as much profit as possible.

Then Article 363 paragraph (1) number 4 is the same as Article 362 regarding theft, but the theft is carried out by two or more people in alliance. Article 378 for carding cases where the perpetrator commits fraud by pretending to buy a product or item on the internet by using the data or credit card identity of another person whose bill is addressed directly to the original owner of the card to conduct transactions in e-commerce.

Carding occurs by the perpetrator (carder) by obtaining credit card data illegally by utilizing information technology (Internet) by using other people's credit card numbers to order goods online.[7] Communication was initially built via email to inquire about the condition of the goods and make transactions. After an agreement is made, the perpetrator gives his credit card number and the seller sends the goods. Carding is defined as an unlawful reception of a credit card number and the subsequent use of that number to buy at online retailers without the card being physically present. This state can arise as a result of a flaw in the authenticator used to verify the identity of customers buying items from an online retailer.

Legal problems that are often faced in carding crimes are related to the delivery of information, arrangements, communications, and transactions electronically, especially in proving matters related to acts in the courts acted upon through the electronic system.[8] Carding itself is a part of cyber crime in online transactions that use internet facilities as a basis for transactions, especially online service systems. So yet, only Part 378 of the Civil Code and Section 51 column (1) in connection with Article 35 or Article 48 in conjunction with Article 32 of the ITE Act are used to handle frisking cases in Indonesia.

Efforts to overcome the crime of carding using Penal facilities are repressive legal efforts, namely all actions taken by law enforcement officials after the occurrence of a criminal act. legal policy in tackling crime, among others, by using criminal law or legislation, which focuses on taking action and eradicating crimes that occur. The crime of carding will be processed through the applicable legal mechanism.[9] Police officers coordinate with relevant agencies to reveal the crime of carding, but it must be in accordance with the facts or results of investigations and investigations. In connection with the above, in carrying out the duties of investigation and investigation, the police ranks coordinate with other law enforcement officers, for example, the Prosecutor's Office makes demands in accordance with the articles indicted to impose sanctions on perpetrators who are legally proven and convinced that they have committed a criminal act.[10]

Repressive measures are also mentioned as special prevention, namely an effort to emphasize the number of crimes by giving punishments (criminals) to perpetrators of crimes and also trying to carry out actions by correcting the perpetrators who committed the crime. So correctional institutions are not only places to educate prisoners to no longer be evil or commit crimes that have been committed but also make perpetrators useful for society in the future.[11]

Efforts to overcome the crime of carding using non-penal facilities are legal measures that are preventive in nature, namely all efforts made to reduce the space for movement and opportunities for carding crimes. This effort includes outreach activities to the public regarding the crime of carding in particular and cyber crime in general so that the public can find out widely, then patrols/raids at internet cafes, and coordinates with relevant agencies and the community.

So the conclusion of the effort to tackle crime is to have two ways, namely repressive action (business after the crime) and preventive (preventing before the crime). First, penal countermeasures are countermeasures that focus more on actions taken after the crime has occurred by enforcing the law and imposing penalties for crimes that have been committed.[12] In addition, through this penal effort, the actions taken in the context of tackling crime include fostering and rehabilitating criminals.

These two non-penal countermeasures are able to create a collaboration as a manifestation of the implementation of tasks. Quasi attempt is public safety that takes place before a crime takes place, hence it's also known as preventative or preventive measures. This should take precedence over repressive efforts. This is very important to increase early prevention efforts against the possibility of a potential disturbance of security and public order and public services.

Efforts made by law enforcement officers against the crime of carding are repressive efforts, namely efforts that emphasize the criminal process against the perpetrator after the crime has occurred, thus creating a deterrent effect on the perpetrator so as not to commit the crime. While other efforts are preventive efforts, namely efforts that are preventing actions.

So it can be concluded that the use of criminal law and legislation in tackling criminal acts, especially carding crimes as a form of cyber crime is still very much needed at this time, considering that criminal law and legislation in addition to having a repressive side also has a preventive side to prevent it from happening. All people who obey the rule of law do not participate in committing crimes or will think twice if they want to commit crimes.

4 Conclusion

Carding crimes are governed by Law No. 19 of 2016 amending Law No. 11 of 2008 on Electronic Information and Transactions, arrangements for dealing with cyber crime cases, especially carding crimes, The Current Law has numerous articles, that criminalize cyber crime by using Extensive interpretation method, apart from the ITE Law, carding crime activities can be formulated in the Criminal Code, Sections 362, 363, and 378 of the Civil Code, which deal with cybercrimes, respectively, then in Indonesia the regulation of the crime of carding is regulated according to its modus operandi in a special law outside the Criminal Code, namely the ITE Law as a lex specialist, among others, it is regulated in Article 30 in conjunction with Article 46 as an article regarding theft in the Carding case, Article 34 paragraph (1) in conjunction with Article 50 as an article regarding theft carried out in cooperation by two or more people in alliance, Section 35 in connection with phrase (1) of Article 51 or Art 32 in conjunction with line (1) of Article 48 as an article regarding fraud in the Carding case with the mode of obtaining other people's credit card data and conducting online transactions. The criminal sanctions emphasized are imprisonment and fines, as confirmed in Article 45 – Article 52 of the ITE Law. In relation to the crime of carding in Indonesia, the sanctions imposed on the accused are based on the ITE Law as lex specialis. However, it is possible that the Criminal Code can also be used as a lex generais, depending on the judge's assessment of the facts of the trial and the evidence presented.

Efforts to tackle carding crimes are penal or repressive, Specifically, any activities conducted by law enforcers after a criminal charge has occurred. This effort is a legal policy in tackling crime and to emphasize the number of crimes by using punishment (criminal) or legislation, which focuses on taking action and eradicating crimes that have occurred, by imposing criminal sanctions and trying to take action by repairing the perpetrator. who commits a crime? Meanwhile, non-penal or preventive efforts to deal with carding crimes are a deterrence of crimes, that is done out already to the occurrence of the offence, namely all efforts made to reduce the space for movement and opportunities for carding crimes.

This is very important to increase early prevention efforts against the possibility of a potential disturbance of security and public order and public services. These efforts include legal counseling activities such as conducting legal awareness seminars in the community, patrols/raids in certain places where carding crimes are indicated, and coordinating with relevant agencies and the community with the aim of empowering community units and officials in tackling carding crimes.

References

[1] A. N. Guiora, Cybersecurity : geopolitics, law, and policy. London and New York: Routledge, 2017.

[2] A. Baker, D. Hudson, and R. Woodward, "Governing financial globalization: International political economy and multi-level governance," Gov. Financ. Glob. Int. Polit. Econ. Multi-Level Gov., pp. 1–242, 2005, doi: 10.4324/9780203479278.

[3] E. E. Supriyanto, H. Warsono, and H. Purnaweni, "Collaborative Governance in Investment Policy in the Special Economic Zone of Kendal Indonesia," Budapest Int. Res. Critics Inst. Humanit. Soc. Sci., vol. 4, no. 4, pp. 13697–13710, 2021, doi: https://doi.org/10.33258/birci.v4i4.3454 13697.

[4] Y. Xiao and M. Watson, "Guidance on Conducting a Systematic Literature Review," J. Plan. Educ. Res., vol. 39, no. 1, pp. 93–112, 2019, doi: 10.1177/0739456X17723971.

[5] C. Handoko, "Kedudukan Alat Bukti Digital Dalam Pembuktian Cybercrime Di Pengadilan," J. Jurisprud., vol. 6, no. 1, p. 1, 2017, doi: 10.23917/jurisprudence.v6i1.2992.

[6] E. R. Leukfeldt and T. J. Holt, "Cybercrime on the menu? Examining cafeteria-style offending among financially motivated cybercriminals," Comput. Human Behav., vol. 126, no. August 2021, p. 106979, 2022, doi: 10.1016/j.chb.2021.106979.

[7] H. Ho, R. Ko, and L. Mazerolle, "Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review," Comput. Secur., vol. 115, p. 102611, 2022, doi: 10.1016/j.cose.2022.102611.

[8] J. Brands and J. Van Doorn, "The measurement, intensity and determinants of fear of cybercrime: A systematic review," Comput. Human Behav., vol. 127, p. 107082, 2022, doi: 10.1016/j.chb.2021.107082.

[9] M. Palmieri, N. Shortland, and P. McGarry, "Personality and online deviance: The role of reinforcement sensitivity theory in cybercrime," Comput. Human Behav., vol. 120, no. February, p. 106745, 2021, doi: 10.1016/j.chb.2021.106745.

[10] V. L. Schul'Tz, V. V. Kul'Ba, A. B. Shelkov, and L. V. Bogatyryova, "Scenario analysis of improving the effectiveness of cybercrime investigation management problems," IFAC-PapersOnLine, vol. 54, no. 13, pp. 155–160, 2021, doi: 10.1016/j.ifacol.2021.10.437.

[11] D. C. Le Nguyen and D. W. Golman, "Diffusion of the Budapest Convention on cybercrime and the development of cybercrime legislation in Pacific Island countries: 'Law on the books' vs 'law in action,'" Comput. Law Secur. Rev., vol. 40, no. June 2020, p. 105521, 2021, doi: 10.1016/j.clsr.2020.105521.

[12] A. S. Selvik, M. M. Edvardsen, O. Laedre, and J. Lohne, "Opportunity Space for Work-related Crime from Procurement to Production," Procedia Comput. Sci., vol. 196, no. 2021, pp. 894–901, 2021, doi: 10.1016/j.procs.2021.12.090.