Jurnal Hukum dan HAM Wara Sains
Vol. 1, No. 02, Desember, pp. 100-112

Transnational Carding Crime Analysis Is Reviewed From International Criminal Law

Deardo Pieter Saragih[1], Astiya Putri Agussriani[2], Dera Andika S[3],Kevin Cesario Valentino Simanjuntak[4], Ganis Raditya Prabaswara[5]

[1] Universitas Pembangunan Nasional "Veteran" Jawa Timur dan 21071010080@student.upnjatim.ac.id
[2] Universitas Pembangunan Nasional "Veteran" Jawa Timur dan 21071010072@student.upnjatim.ac.id
[3] Universitas Pembangunan Nasional "Veteran" Jawa Timur dan 21071010070@student.upnjatim.ac.id
[4] Universitas Pembangunan Nasional "Veteran" Jawa Timur dan 21071010114@student.upnjatim.ac.id
[5] Universitas Pembangunan Nasional "Veteran" Jawa Timur dan 21071010089@student.upnjatim.ac.id

Article Info

Article history:

Received 06 Desember 2022
Revised 08 Desember 2022
Accepted 12 Desember 2022

Kata Kunci:

Kejahatan lintas batas negara, peretasan, penipuan kartu kredit, dan keamanan manusia.

Keywords:

Transnational crimes, hacking, carding, and human security.

ABSTRAK

Artikel ini bertujuan untuk mengetahui kejahatan lintas batas negara peretasan-penipuan kartu kredit terhadap keamanan manusia yang dalam hal ini membahas tentang contoh kasus yang pernah terjadi, mengetahui faktor dari penyebab terjadinya cyber fraud yang ditinjau dari fraud triangle theory, mengetahui tentang modus yang biasa digunakan oleh pelaku, mengetahui tentang yuridis hukum yang berlaku dalam masalah ini, dan dampak serta solusi dalam kasus ini. Kemajuan teknologi di era yang berkembang ini memberikan kemudahan namun juga memberikan kesempatan bagi orang yang tidak bertanggung jawab untuk melakukan tindak kriminal. Berbagai macam kejahatan terdapat di dunia maya salah satunya adalah tindak kejahatan penipuan kartu kredit. Kasus penipuan kartu kredit merupakan kasus yang cukup membahayakan sebab kasus ini memiliki kesulitan dalam pengungkapan pelaku yang melakukannya sehingga membuat kasus ini semakin marak terjadi dan menimbulkan keresahan di masyarakat. Kasus ini juga berpotensi untuk mengganggu keamanan manusia dan keamanan negara yang menjadi korbannya. Salah satu contoh kasus yang ada pada bulan september 2011 dengan pelakunya menggunakan modus pencurian data dari pemilik kartu kredit di sentral perbelanjaan dan spbu yang menghasilkan nominal sebesar 81 miliar.

ABSTRACT

This article aims to find out transnational crimes of hacking-carding against human security, which in this case discusses examples of cases that have occurred, knows the factors that cause cyber fraud in terms of fraud triangle theory, knows about the modes commonly used by perpetrators, knowing about the juridical law that applies in this matter, and the impact and solution in this case. Technological advances in this developing era provide convenience but also provide opportunities for irresponsible people to commit crimes. Various kinds of crimes exist in cyberspace, one of which is credit card fraud. The case of credit card fraud is a case that is quite dangerous because this case has difficulty disclosing the perpetrators who did it, making this case more widespread and causing unrest in the community. This case also has the potential to disrupt human security and the security of the country that is the victim. One example of the case in September 2011 with the perpetrator using the data theft mode from credit card owners at shopping centers and gas stations which resulted in a nominal value of 81 billion Keywords: Cross-border crime.

Corresponding Author:
Name: Deardo Pieter Saragih
Institution: Universitas Pembangunan Nasional "Veteran" Jawa Timur
Email: 21071010080@student.upnjatim.ac.id

1. INTRODUCTION

There is a fact that in today's modern life, humans cannot be separated from technological developments that make human life much easier. Advances in technology and information that exist today make it easy to communicate without any obstacles and social shifts that are so fast. There is an area in which a person can interact with other people but using the internet network on a computer or this place is called cyberspace which is a new artificial world resulting from technological advances in the field of computers and internet networks. Even so, advances in information technology can be likened to a double-edged knife, because apart from positive influences such as facilitating all daily activities, technological advances also have negative influences such as opening doors for criminals to carry out their actions.

With the passage of time and the advancement of information technology, the crimes that are often committed by these perpetrators are known as cybercrime. Cybercrime is all models of crime directly related to computers, computer networks and their users, and traditional crime models related to computers. One example of cybercrime that often occurs among the public is crime in the banking sector, such as hacking accounts or manipulating the use of credit cards owned by other people. Manipulating the use of other people's credit cards or known as carding cannot be equated with the mode of snatching credit cards that occurs as usual, because this mode can be carried out by carders or card perpetrators without having to directly hold the victim's credit card. The perpetrator only needs the number from the victim's credit card, after which the number is known, the perpetrator can use the credit card according to his wishes. This crime is very detrimental because later the bill used by the perpetrator will still be addressed to the victim as the original owner of the credit card.

The increase in cases of this crime has resulted in many victims and this case has increased protests from the community, because this case occurs very often but it is difficult to reveal the person behind this crime. This crime case has attracted the attention of all circles, because this crime is relatively new but has become a terrible crime and can be a crime that is not trivial. This crime is also an example of inter-state crimes that have the potential to attack human security both individually and national security.

2. LITERATURE REVIEW

This study used literature study in which the data were obtained from books, articles, journals, and other concrete reading sources that support the writing of this research.

2.1 Data Protection and Personal Information Through the Indonesian Data Protection System (Idps)

Aswandi, Muchsin, Sultan, 2020: 167-190. First, we need a regulation relating to cybercrime and also the protection of personal data and information in Indonesia. Second, a system is needed that is able to overcome the problem of cybercrime, especially in the field of personal data and information management, namely the Indonesian Data Protection System (IDPS).

transnational crime and the implementation of Indonesian criminal law Hasan, 2018: 13-20. Transnational crime is a real threat to the Indonesian state in particular; whether in the form of terrorism, illegal logging, cybercrime, drug trafficking, drugs experienced significant developments. Handling and overcoming transnational crime are a very potential form of threatening people's lives in the fields of economy, socio-culture, order and security both nationally and regionally. This indicates that transportation, communication and information technology is the impact of technological modernization.

2.2 Legal Protection for Credit Card Holders in Banking Transactions

Pratiwi, Yetti, 2020: 206-223. That it has not been carried out properly due to transactions that have never been made before by the credit card owner but what has occurred is a notification from the bank regarding the credit card bill, the calculation of the credit limit or balance is incorrect so that the credit card holder cancels their shopping transaction, there are complaints from customers regarding interest rates that are not appropriate at the time of the agreement, this is clearly very detrimental to customers when making transactions and credit card bills exceed the price paid by consumers.

3. RESEARCH METHOD

The rule used in this research is the rule by describing data using technical analysis depiction of the data obtained, namely efforts to collect data based on existing data, without affecting the analysis, as well as describing rationally and objectively the relationship between the variables studied and the data. author's perspective. With this rule, it explains and describes how certain events or events occur in detail or in detail. Which in the rules of writing this research events or events can be resolved in accordance with existing methods or rules. Data collection in this research study used secondary data sources, the data of which used or used literature studies whose data were obtained from books, articles, journals and other concrete reading sources that support the writing of this research.

4. RESULTS AND DISCUSSION

Since the digital revolution, the business world has begun to network in cyberspace. Transactions that occur are also unusual. Modern society actually prefers a more efficient payment process: credit cards. Meanwhile, advances in digital technology also provide opportunities for criminals in cyberspace. Illegal credit card fraud or activity involving credit card fraud. The scam was initially based on written advertisements, but began to change the way data was manipulated in the form of cards. This crime or illegal use of a credit card is illegal and violates laws or regulations both nationally and internationally where the crime harms other people and threatens the security/cybersecurity of other people.

According to the British Police, cybercrime is any way of taking advantage of the convenience of digital technology to use computer networks for criminal purposes or for high-tech criminals. Cybercrime is also identified as computer crime. This type of card crime has two scopes: domestic and transnational. Cross-border carding, on the other hand, means that criminals commit crimes from other countries without any distance restrictions. Carding property is non-violence. That is, there is no visible interference, but it has a big impact on the victim. The US Department of Justice defines computer crime/sim hacking as "an offense that requires knowledge of computer technology to commit, investigate, and prosecute. One cause of carding is the public's lack of knowledge about possible cybercrimes. We also need to increase the strengthening of legal measures against cyber fraud as a cross-border crime, based on the legitimacy of new international law. This crime knows no boundaries. This means that the perpetrator and victim do not have to be in the same place or country. Example of the first credit card crime case in

Cases

Indonesia occurred in March 2013. Card customer credit and debit were stolen from various banks during transactions at The Indonesia Body Shop branches. The stolen data would be used to make duplicate cards processed in Mexico and the United States. The stolen data came from various banks such as Bank Mandiri and Bank BCA. Bank Mandiri found a number ah stolen customer credit and debit card details. Transaction losses due to data theft are estimated to reach disproportionate levels. Credit card crimes were uncovered when Bank Mandiri uncovered suspicious transactions.

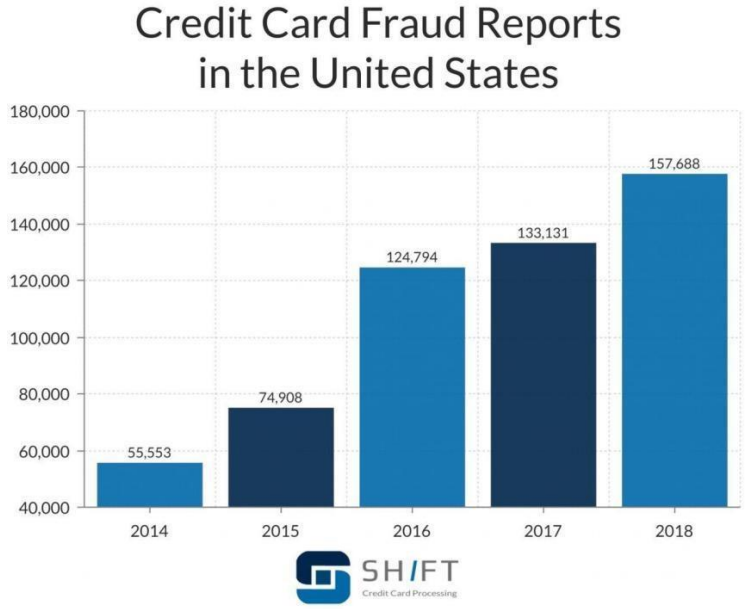
This card is commonly used in Indonesia and suddenly used for shopping in Mexico and the United States. After talking directly to the customer, we find out that the card has never been used outside of Indonesia. Then, in September 2011, Polda Metro Jaya disbanded a consortium of credit card thieves and suffered a huge loss of Rp. 81 billion. The syndicate compromised credit card EDC data in two ways. The first mode is stealing data from EDC credit card holders in shopping centers and other transaction locations. One such data breach was the theft of EDC data from gas stations in Kebayoran Lama, Jakarta, which occurred between 18 August and 9 September 2011.

Credit Card Fraud Statistics

- In 2018, $24.26 Billion was lost due to payment card fraud worldwide
- The United States leads as the most credit fraud prone country with 38.6% of reported card fraud losses in 2018
- Credit card fraud increased by 18.4 percent in 2018 and is still climbing
- Card not present fraud is now 81 percent more likely than point-of-sale fraud
- In 2018, Identity theft was the 3rd largest cause of fraud in the USA
- Identity theft makes up 14.8 percent of reported fraud
- Credit card fraud was ranked #1 type of Identity theft fraud
- Credit card fraud accounted for 35.4 percent of all identity theft fraud in 2018

- New account fraud percentage is up 24 percent from account fraud in 2017
- Takeover of existing accounts is down 6 percent compared to 2017
- Yahoo's breach in 2013 exposed 3 billion victims and is still the biggest single informational breach
- The Business Sector accounted for 46 percent of data breaches in 2018, including the Marriott International Breach

69 percent of fraud starts with a consumer being contacted by telephone or email, such as overdue loans or prize scams.



Data source: shiftprocessing.com (2021)

Image 1. Credit Card Fraud Reports in the United States

It's probably not news to you that fraud is a huge global and national problem. With the growth of the e-commerce industry and community, we will see credit card fraud rise at rates faster than ever. Here are some important facts about credit card fraud:

- Losses of $24.26 Billion in 2018 due to payment fraud worldwide.
- The USA is the global leader as the most credit card fraud prone country with 38.6 percent of reported fraud losses last year in 2018.

Credit and debit card fraud continues to climb over time

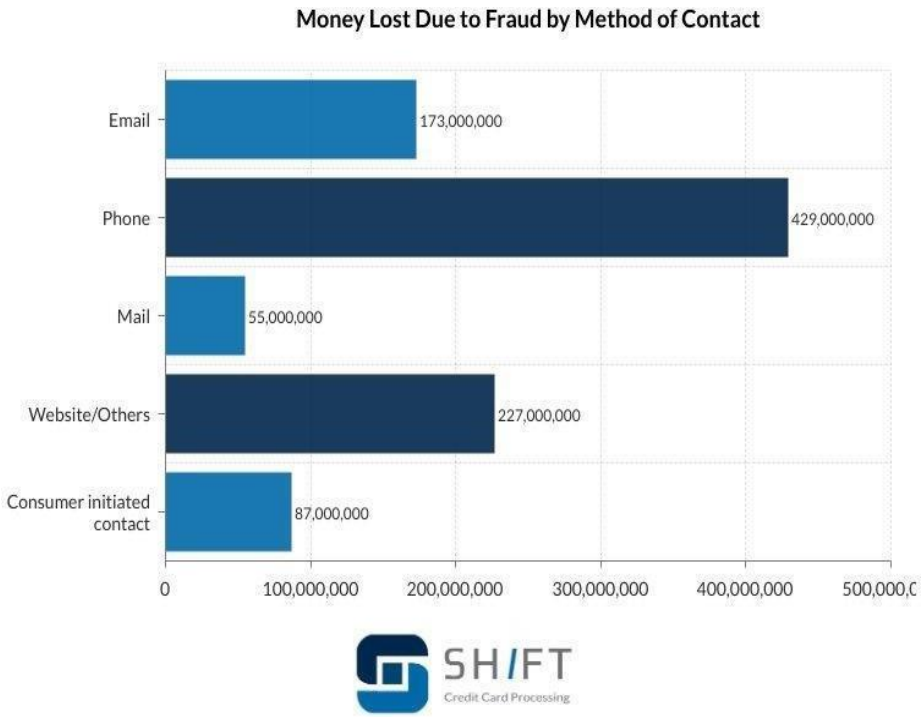
Data source: shiftprocessing.com (2021)

Image 2. Identity Theft Report

Identity Theft Statistics:

- In 2018, Identity theft was the 3rd biggest cause of all categories of financial fraud in the USA, just below Imposter Scams and Debt and Loan Collection fraud
- Identity theft made up 14.8 percent of consumer fraud complaints with reports of 444,602 reported cases in 2018
- Credit card fraud was ranked #1 kind of Identity theft fraud - accounting for 35.4 percent of all identity theft fraud in 2018
- Using identity information, creation of new accounts is up 24% from 2017
- Take over of existing accounts has decreased 6 percent from 2017

Credit card fraud is the most common and popular type of identity theft and makes up 35.4% of all identity theft reports.



Data source: shiftprocessing.com (2021)

Image 3. Report of Identify Theft by Age

Scams come from a variety of different services. According to the consumer sentinel network 2018, most of the consumers who were affected by fraud were contacted by scammers via phone or email and that losses of $429 million were incurred due to this kind of phone fraud.

Factors That Cause Cyber Fraud, If Viewed Based On The Fraud Triangle Theory,

there are three elements: opportunity, pressure, and downsizing. On the one hand, the loosening of the security system of fake online shop web platforms can lead to the spread of information about personal data. Second, pressure is seen as an incentive to deceive people because of their lifestyle. demands, economic powerlessness, gambling behavior, attempts to beat the system, and job dissatisfaction. Pressure as a form of dissatisfaction experienced by individuals obtains justice in return for environmental awareness. Creates the courage to commit crimes. Third, rationalization is a key component of many scams, prompting scammers to justify their actions. For

this reason, law enforcement with relevant laws and regulations is a serious problem in dealing with cybercrime incidents in Indonesia.

Typical Modus Opersation of Perpetrators

Delivery of fake web platforms created by cybercriminals. Web platforms, on the other hand, cover business and commercial activities such as selling clothing, food and catering. Since this is an account takeover, copyright infringement and abuse may occur to avoid having to pay for purchases using an unauthorized credit card account in the victim's name. The perpetrators did this because when the perpetrators entered their personal information at the bank, they provided enough personal information that they could escape by providing the information attached to the bank and of course the fake documents, because I had to get them.

Law Jurisdictions

in cybercrime overlap with a variety of legal issues, including criminal law, cyber law, information technology law, commercial law, and international law. Cybercrime (carding) criminal law also pays more attention to the verification process (proof) in this case. In commercial law, carding and credit cards, this refers to part of the contract, specifically Section 1338 KUHD. Under international law, carding as a cybercrime is governed by the Budapest Convention on Cybercrime in the Handling and Prevention of Cybercrime Cases.

Given the nature of cybercrime which is general and unlimited in nature and the use of high technology as a medium, criminalization policies in the field of information technology are very important for regional and international cybercrime prevention in the context of harmonization and unification of cybercrime regulations. efforts to develop the European Union Convention on Cybercrime is one of the international legal instruments that must be reviewed, and taken into consideration by European nations. The Budapest Agreement will enter into force after five ratifications, including three from the European Union.

According to ETS 185 – Cyber Crimes (Convention), 23.XI.2001/Budapest Convention, cross-border crimes in Hactivism Carding are covered by Article: Article 2 Illegal access, The parties involved in the authority regarding this cybercrime convention must make a decision or definite stance regarding this crime under national law to criminalize all or part of intentional unauthorized access to computer systems.

Article 3 Illegal wiretapping, the parties involved in the authority regarding cybercrime conventions in accordance with their national laws, prohibit unauthorized interception by means of technology, carry out transmission of computer data information from non-public which is then entered into the mechanism or pattern of the computer which which must provide certainty against cybercrime regarding illegal wiretapping.

Article 8 Computer-related fraud, the parties involved in the authority regarding the cybercrime convention must take legal certainty against fraudulent acts with this sophisticated system and related actions to determine the crime of said action with or through existing legal rules with awareness, pay attention to their rights and obligations as human beings.

International Criminal Law

1. Criminal Definition of International

Criminal International criminal law is a set of rules and legal principles governing international crimes committed by legal subjects to achieve a certain goal. This term indicates that the legal principles and principles are truly international, so neither national nor domestic. The truly

international principles and principles of criminal law are legal principles and principles which can be found in the form of international agreements whose substance (both directly and indirectly) regulates international crimes. For example, the 1948 Genocide Convention, the 1973 Apartheid Convention, conventions on terrorism, such as the 1977 European Convention on Combating Terrorism, and others. Meanwhile, the term international crime indicates the existence of a criminal event that is international in nature, or that crosses national borders, or that concerns the interests of two or more countries. Crimes that can be classified as international crimes are crimes regulated in conventions such as genocide, apartheid, terrorism, and others.

2. Carding Crime When viewed from the Aspect of International Criminal Law

The phenomenon of information technology crime is a relatively new form of crime when compared to other forms of conventional crime. Information technology crimes emerged at the same time as the birth of the information technology revolution. As stated by Ronni R. Nitibaskara that: "Social interaction that minimizes physical presence is another feature of the information technology revolution. With this kind of interaction, deviance from social relations in the form of crime will adapt its shape to that character.

Cybercrime is a representation of international crimes that use hit-tech because the most prominent feature and crime is that it is borderless or knows no national boundaries. Relatively high technology means that only certain people are capable of committing this crime and open resources are mediators or can become media for various crimes including crimes in the fields of banking, capital markets, sex, intellectual property piracy and terrorism and more precisely including trans-national crime.

Data crackers who have economic motives or deliberately cheat shopping on e-commerce websites using other people's credit card numbers, are against the law. The crime of illegally using someone else's credit card for a transaction and so on is a digital crime. Laws or positive legal instruments are the final instrument in determining the success or failure of an investigation because the wrong application of legal offenses will counteract the investigation being carried out. Even though the investigators are capable and understand the profile and culture of the hackers/prekers, the techniques and modus operandi of the hackers/prekers are supported by even a sophisticated laboratory.

In the Stufenbau Theorie put forward by Hans Kelsen it is said that "law regulations as a whole are derived from norms that are at the top of the pyramid, and are increasingly diverse and spreading. Law enforcers have a strategic role in the application of law/effectiveness of a rule of law. Every legal professional must have legal knowledge as a determinant of the quality of professional legal services. Law enforcement includes components of the criminal justice system consisting of police, prosecutors, judges, advocates and correctional institutions.

For cases of hacking or entering other people's computer networks illegally and modifying (deface), the investigation is faced with complex problems, especially in terms of evidence. Many witnesses and suspects are outside the jurisdiction of Indonesian law, so it is very difficult to carry out investigations and prosecutions, not to mention the problem of very complicated evidence related to information technology and digital codes that require good human resources and forensic computer equipment.

In the case of other cases such as porn sites and gambling, the perpetrators do hosting/registration abroad which has a different jurisdiction from our country because

pornography is a general Standard of Investigation, Investigation and Prosecution by the Indonesian Police and gambling is not a crime in America and Europe even though the address used is in Indonesian and the operator of the website is in Indonesia so we cannot take any action against them because the website is universal and can be accessed anywhere. Many rumors circulated that informed that there was a break-in of private banks online by hackers, but the victims covered up the problem. This is related to the credibility of the bank concerned, who is afraid that if this case is spread, it will undermine the public's trust in the bank.

Carding's crimes are covered by Indonesian criminal laws

Law in force in Indonesia itself, it has a method of guaranteeing a state life regarding a Carding crime which we can see that the action is included in an act of Cybercrime in this case not only the Criminal Code applies because in Indonesia there is an ITE Law which regulates a crime of Cybercrime. Regarding this matter, in the Carding case, it is necessary to have a regulation regarding digital evidence, it is known that this is not contained in the Criminal Code, with this we can find that the rules regarding such evidence can be found in Articles 5 and 44 of the ITE Law and this is based on article 184 of the Criminal Procedure Code. Then following up on the Carding case, the perpetrator can be charged with Article 263 paragraphs 1 and 2 of the Criminal Code. If we analyze based on the article, we can find objective and subjective elements. In article 263 paragraph 1 of the Criminal Code which includes objective elements a. Actions: fake, make fake. b. the object: a letter that can give rise to a right, an agreement, a debt discharge and is intended as evidence in a matter. c. causes a consequence. Then regarding the subjective element, namely having an intention which orders or uses against other people to use it as if the contents are true or not false. Then it can also be found in article 378 of the Criminal Code, the objective elements can be known a. action: move. b. driven: people. c. the action is aimed at: other people handing over objects, giving debts, and writing off receivables. then d. about a way: using fake names, gimmicks, fake dignity and strings of lies. Regarding the subjective element, namely aiming to enrich themselves, using deception, fake identities and some lies.

Then if we use Article 30 of the ITE Law which can ensnare carders, we can find objective and subjective elements. Regarding objective elements: a. deeds; access. b. object: electronic system, computer equipment. c. a condition accompanied by a right to visit from the property of another. Then the subjective element, namely a. there is a purpose found. b. happened unlawfully. In the implementation of the Carding case, if you want to be subject to a sentence, you are required to carry out a verification process in which there is a requirement in accordance with the proof system contained in the Criminal Procedure Code. With article 183 of the Criminal Code this can be found later also not forgetting that Indonesia implements a negative proof system. Therefore, a sentencing process that occurs can be carried out if it follows the rules of the game from Indonesian criminal law, then do not forget that there are Indonesian criminal principles. In a conception of criminal law applied in Indonesia, there are several principles which have an influential correlation in carrying out the law systematically and properly, therefore we will discuss the application of a principle that exists in Indonesian criminal law;

Material principles are principles that have been regulated clearly and permanently in the Criminal Code. Which is divided into Principles with the enactment of criminal law when the action occurs. The principle where the criminal law takes place; consists of the territorial principle, active and passive nationalism and the principle of universality. The principle of non-reactive in which the

law is something that becomes the basis for criminal acts. The principle of legality does not apply to a person who is punished for an act if it is not determined in advance in the law.
The principle is formally which can be interpreted that the Criminal Code is not regulated but, in its implementation, it must be in accordance with the Criminal Code.

Therefore, an application of criminal principles in Indonesia is highly expected to be implemented in a criminal processing activity that occurs, as is the case for cybercrime not only looking at the provisions of the Criminal Code but must look at the ITE Law contained in the country of Indonesia.

Solution

The 1969 Vienna Convention is not only a reformulation or codification of customary international law in preventing carding as a transnational crime, but needs to be further developed. However, the Vienna Convention also justifies the existence of customary international law in relation to agreements, especially regarding rules or principles that do not yet exist in the Vienna Convention. Carding Crime is a transnational crime, so in preventing this carding crime we cannot be separated from the 1969 Vienna Convention. Cybercrime is included in the list of types of crimes that are international in nature, this is based on the Convention Against International Organized Crime in particular, it will certainly have its own problems, regarding the existence of jurisdiction. Based on the general principles of International Relations, the state has ultimate sovereignty over what is in its territory. Therefore, a country cannot act on the territory of another country outside its sovereignty without the approval of the regional ruler. Several countries apply the principle of extraterritoriality to their domestic law.

This extraterritorial principle applies if the result of a violation affects more than one party. Another condition that can lead to the application of extraterritoriality is if it is not regulated by the locality where the violation occurred, but the violation is detrimental to other parties. The application of extraterritoriality is clearly regulated in Article 2 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic Transactions. Where in the law it is explained that the regulation of ITE in a country is mandatory for everyone who violates both domestically and abroad if the action has an impact on Indonesia. This extraterritorial need, because carding offenses can harm people and the national interests of a country. Therefore, the regulation on the use of ITE must include actions that are carried out outside the territory of Indonesia but have an impact or can be detrimental to the Indonesian state.

Carding is a transnational crime, the applicable jurisdiction is extraterritorial jurisdiction to make, apply and enforce the laws imposed by that country. Related to the prevention of transnational crime with the principle of aut dedera aut judicare. This principle is regulated in Article 24 paragraph 3 of the Convention on Cybercrime, one of which is as a means of developing international cooperation in a peaceful manner. This makes Indonesia obligated to prevent transnational crimes; therefore, Indonesia recognizes the Convention on Cybercrime as one of the international legal instruments. which need to be examined and used as a benchmark in creating positive legal norms. The norms in the Convention on Cybercrime have been adopted into the ITE Law to prevent carding in Indonesia. Specifically related to illegal access, illegal wiretapping, data tampering, system damage, device misuse, computer-related counterfeiting, and child pornography.

An investigative process is not the responsibility of just one country, but countries need international cooperation to resolve this Carding problem. Article 24 of the Extradition Convention

provides the widest range in solving cybercrime cases to the fullest. This article explains that in the event of a violation, each state party must take other necessary actions to establish a policy for the violation. Where one party can take whatever steps are necessary, without exception regarding criminal jurisdiction carried out by other parties based on their own national law.

Efforts to prevent carding crimes require regulation by modeling international legal norms, by adopting the principles of cybercrime control. As a result of carding crimes that cross the jurisdictional determination of a country, a country has the right to exercise jurisdiction over the perpetrators. Therefore, the legal principle that can prevent carding crimes is the principle of extraterritoriality, accompanied by the principle of international cooperation contained in the provisions of the cybercrime convention. The provisions of the Cybercrime Convention can be used when developing legal norms that can prevent crime mapping, before that Indonesia must ratify the agreement to establish cooperation, and that is the purpose of the agreement.

Impact of carding

Carding is a crime which is the result of a technological development in this era that is very fast and rapid. The ongoing technological developments make it easy for everyone to access anything via the internet, with the convenience or superiority of the internet itself, it makes an individual deliberately take advantage of the negative impacts of technological developments. With the development of technology, it has greatly changed a pattern of habits for the whole world, both developing and developed countries, making it a breakthrough that has benefits for all sectors, one of which is the economic sector which combines with these technological developments. There is a loophole that can be exploited by an individual to commit a crime by means of which the person can take advantage of the weakness of the system which causes an extraordinary impact on technology users if left unchecked, therefore we review some of the impacts that occur with carding crimes, namely:

A. Causing public unrest in using credit cards.

In daily life, the use of credit cards in Indonesia, for example, has a large number of users. Based on data sourced from Bank Indonesia (BI), it was noted that the number of credit cards in circulation in Indonesia reached 16.58 million units in June 2022. This number increased by 0. 84% compared to June 2021 which amounted to 16.56 million credit cards. It can be seen that if the use of large credit cards greatly influences people's behavior in fulfilling and carrying out economic needs if a crime occurs, it will cause unrest for most credit card users in Indonesia.

B. Disappearance of public money without clarity.

By taking advantage of the convenience of carrying out an action illegally by a person who easily penetrates data belonging to a credit card user, it causes confusion among the public about their money, in other words, that their money is carried out in a way that is done to launch an action, which in terms of transactions on online sites. In its implementation, the rights and obligations of the community in using credit cards are contained in the Consumer Protection Act No. 8 of 1999 Chapter III Article 4.

C. Binding the number of fraud cases.

The rise of activity in crime cases makes fraud cases undeniable with the existence of a fraud making that public awareness and fear determine how to take an attitude in carrying out an action in the future with an increase in the number of fraud cases making carding in its implementation strictly prohibited in all parts of the world.

D. Fading public trust in financial services in their own country or other countries.

The occurrence of a carding makes how to take a firm stance both from the country itself and with other countries so if a conflict occurs between countries it is a sign that the situation is not very good because the state should guarantee that security and privacy for credit card users, especially for financial services which has implemented provisions that should be beneficial to both parties without exception in countries where consistent and transparent monitoring is carried out in order to foster a sense of community trust that was originally fading so that it can be reshaped conclusion Technological progress certainly brings good things to human life such as the presence of

5. CONCLUSION

Internet which makes it easier for us to get and provide information, but technological advances can turn bad if there are people who abuse this. One of them is cybercrime in the banking sector, namely the manipulation of using credit cards or hacking into other people's accounts without rights, which can also be referred to as carding. this crime can be committed by the perpetrator even though the perpetrator does not directly hold the card and the perpetrator can do it even though he is in a different country from the victim. This is of course troubling the community because victims can suffer losses.

This crime is made possible because of opportunities, streamlining, and pressure. One of the perpetrators' efforts to take over the victim's credit card account is to create a fake site that requires the victim to fill in data that will later be used by the perpetrator to take over the account. Countries certainly have sovereignty regarding the laws that apply in their country, so other countries cannot take action. This can be an obstacle in finding and arresting perpetrators, but there are countries that apply the principle of extraterritoriality that allows other countries to take action on other countries. Cross-country hacktivism carding crimes have listed in the Budapest Convention, 23.XI.2001 in the convention there are provisions that allow for extradition, this of course makes it easier to catch and find the perpetrators. So in dealing with cross-border carding crimes, cooperation between countries is needed.

REFERENCE

Arifin, R., Atikasari, H., & Waspiah, W. (2020). The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud. *Jurnal Hukum Novelty*, *11*(2), 235. https://doi.org/10.26555/novelty.v11i2.a15700

Aswandi, R., Muchsin, P. R. N., & Sultan, M. (2020). Perlindungan Data dan Informasi Pribadi Melalui Indonesia Data Protection System (IDPS). *Jurnal LEGISLATIF*, *3*(2), 167–190. https://journ

Budapest Convention on Cybercrime, 33 6 (2001). https://rm.coe.int/1680081561

Burgess, P. (2014). *Hukum Pidana Internasional – Referensi HAM*. Lembaga Studi & Advokasi Masyarakat. https://referensi.elsam.or.id/2014/09/hukum-pidana-internasional/

Credit Card Fraud Statistics [Updated September 2021] Shift Processing. (2021). Shiftprocessing.Com. https://shiftprocessing.com/credit-card-fraud-statistics/

DEWI, Y. (2020). *Pengaruh Peranan Spesialis Penipuan (Fraud Specialist) Terhadap Pendeteksian Penipuan Kartu Kredit Dan Dampaknya Pada Penerapan Pengendalian Internal (Studi Kasus Pada Bank XYZ di Jakarta)* [Universitas Mercubuana]. https://repository.mercubuana.ac.id/59603/

FEBRIANTO, K. C. (2013). *Dampak Transnational Crime Hacktivism – Carding Terhadap Human Security* [Universitas Muhammadiyah Malang]. https://eprints.umm.ac.id/27803/

Handoko, C. (2017). *Tinjauan Hukum Pidana Terhadap Carding Sebagai Salah Satu Bentuk Cybercrime*. Universitas Muhammadiyah Surakarta.

Hasan, M. I. (2018). KEJAHATAN TRANSNASIONAL DAN IMPLEMENTASI HUKUM PIDANA INDONESIA. *LEX CRIMEN*, *7*(7). https://ejournal.unsrat.ac.id/index.php/lexcrimen/article/view/21341

Isharyanto. (2016). *Politik Hukum* (1st ed.). Kekata Grup. https://layanan.hukum.uns.ac.id/data/RENSI file/Buku ISHARYANTO/18. BUKU POLITIK HUKUM %282016%29.pdf

Kurniasari, Y. (2017). *Perlindungan Hukum Terhadap Korban Tindak Pidana Carding* [Universitas Islam Indonesia]. https://dspace.uii.ac.id/handle/123456789/6586

Kurniawan, A. B., & Soeskandhi, H. (2022). Perlindungan Hukum Kepada Pengguna Elektronik Banking Atas Kejahatan Carding Ditinjau Dari Undang-Undang Informasi Dan Transaksi Elektronik. *SUPREMASI : Jurnal Hukum*, *5*(1), 64–87. https://doi.org/10.36441/SUPREMASI.V5I1.865

Kusuma, A. S. (2021). Human Security dalam Hubungan Internasional: Sebuah Pengantar. In *Human security dalam hubungan internasional*. Pustaka Ilmu. https://www.researchgate.net/publication/358929457

Kusumawardana, H., Hariadi, W., & Anindito, T. (2021). Tinjauan Yuridis Carding Sebagai Kejahatan Transnasional Terorganisir. *Wijayakusuma Law Rewiew*, *3*(1), 38–43. https://e-journal.unwiku.

Persadha, P. (2020). Hacktivism Sebagai Upaya Menyampaikan Suara Lewat Ruang Siber Di Indonesia. *Jurnal Penelitian Ilmu-Ilmu Sosial*, *21*(2), 72–77. https://doi.org/10.33319/SOS.V21I2.65

Pratiwi, D. R., Yetti, & Afrita, I. (2020). Perlindungan Hukum Terhadap Pemegang Kartu Kredit Dalam Transaksi Perbankan. *Legal Standing: Jurnal Ilmu Hukum*, *4*(2), 206–223. https://journal.umpo.ac.id/index.php/LS/article/view/3092/1592

Riyanto, A. (2020). Perlindungan Hukum Terhadap Nasabah Kartu Kredit. *PETITA*, *2*(2), 133–143. https://doi.org/10.33373/PTA.V2I2.3996

Setiyawan, W. B. M., Churniawan, E., & Faried, F. S. (2020). Upaya Regulasi Teknologi Informasi Dalam Menghadapi Serangan Siber (Cyber Attack) Guna Menjaga Kedaulatan Negara Kesatuan Republik Indonesia. *Jurnal Usm Law Review*, *3*(2), 275. https://doi.org/10.26623/julr.v3i2.2773

Suwardi, S. S., & Kurnia, I. (2019). *Hukum Perjanjian Internasional* (Tarmizi (Ed.); 1st ed.). Sinar Grafika.

Zuraida, M. (2015). *Credit Card Fraud (Carding) Dan Dampaknya Terhadap Perdagangan Luar Negeri Indonesia* [Universitas Airlangga]. http://repository.unair.ac.id/id/eprint/17616