P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY

Volume 11, Issue 02, 2020, pp. 235-246

The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud

Ridwan Arifin[1], Hartini Atikasari[2], Waspiah[3]

[1] *Faculty of Law, Universitas Negeri Semarang, Indonesia*
ridwan.arifin@mail.unnes.ac.id
[2] *Faculty of Law, Universitas Negeri Semarang, Indonesia*
hartini@gmail.com
[3] *Faculty of Law, Universitas Negeri Semarang, Indonesia*
waspiah@mail.unnes.ac.id

Abstract

Introduction to The Problem: Since digital reform, business and trade sectors have begun to expand their network in cyberspace. Transactions carried out also no longer refer to ordinary things. The modern era of society indeed prefers a more efficient payment process, namely through a credit card. On the other hand, the advancement of digital technology also provides opportunities for perpetrators of crime in cyberspace. The fraud, which was initially carried out with the objects of written reports, began to move lanes towards data manipulation in the form of carding.
Purpose/Objective Study: This paper is intended to analyze and examine carding as cyber fraud in three legal studies: criminal law, business, and commercial law, and transnational criminal law. This study illuminates the intersection between criminal law, business and commercial law, law and technology, and international criminal law in carding cases.
Design/Methodology/Approach: The paper is normative legal research using a comparative approach and regulations related to carding and cyber fraud.
Findings: The study highlighted that carding as a manifestation of cyber fraud is also a transnational crime, which involves networks or groups across national borders to carry out certain illegal businesses or activities. Included in this case is the data theft on credit cards. Of course, this has resulted in a shift of public trust towards the credit card provider sector, namely banks, so that there is a need to strengthen the juridical pathway nationally and internationally.
Paper Type: General Review
Keywords: Carding; Cyber Fraud; Cyber Crime; Transnational Crime

Introduction

In the 21st century, the development of science and technology has produced a reasonably rapid progress scheme. Even so, these developments are not always able to have a positive impact on society. Apart from that, results in the digital world turned out to be influential actors in the business and trade sectors to expand their target markets into cyberspace. It was done to adjust or as a means of adaptation to

Article History
Submitted 6 July 2019 - Revision Required 10 July 2019 - Accepted 11 November 2019

JURNAL HUKUM
NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246
P-ISSN: 1412-6834
E-ISSN: 2550-0090

technological developments. It is also referred to as digital reform, a change from what was previously conventional to digital. The digital reform could be said as an impact of the current globalization, which affects the life sectors in society, especially in the fields of trade and technology.

Since the introduction of the internet in 1969 by APRA, computers have an essential role in daily activities by workers in the small business sector to large companies, both national and international (Featherly, 2016). Through the explosion of the digital world, actors in the business and trade sectors also began to use the internet as a trading base, including payment of business and trade transactions. The massive internet as a container in efficient and practical business and trade practices has led to new terms in business practices and commerce in cyberspace, such as e-commerce, e-banking, e-trade, etc.

Despite the positive effects, the virtual era is also providing negative impacts. The crimes that were initially carried out in traditional schemes also helped expand its territory towards the internet as a model for broadening crime in cyberspace. Meanwhile, banking crimes committed digitally and electronically become one of the challenges and problems for the banking security system in Indonesia. Electronic Banking is a new technology that has many advantages and has the potential for significant issues such as customers' hesitation to use the system (Fatima, 2011). Crime in banking is different from conventional one but has the same goal: getting information on the banking account, credit cards, and hacking the bank's database system and robbing it (AlMajed et al., 2016; Arifin, 2018).

In early 2018 there was a theft of debit card information using the skimming method, which occurred in 64 banks spread throughout the world, and 13 of them were Indonesian banks: private and public. The incident resulted in the impacted banks have to return customer funds reached 18 billion. It indicates the importance of prompt handling to overcome these problems in the future (Faridi, 2018).

Therefore, the credit card business is one of the profit machines of every bank and non-bank institution, both in gaining new customers and printing various business portfolios. However, the practice of the credit card industry in Indonesia is not entirely safe from the hands of ignorant or credit card criminals. Carding is a form of cybercrime that is still the modus operandi of perpetrators or fraudsters. In January 2004, Indonesia was named the number 1 country in top countries by percentage of fraudulent transactions and the number 3 country in top countries by the total volume of fraudulent transactions in research on internet security in the world (Verisign, 2005).

Legal problems that are often encountered relate to the delivery of information, communication, or electronic transactions, especially in terms of evidence and matters on legal actions carried out through the automated system. Carding itself is a part of cybercrime in banking transactions that use the internet to deal, especially the

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246

online banking service system. The carding mechanism usually is done by perpetrators by illegally obtaining credit card data through the internet so it could be used to order any goods online.

Carding itself is illegal interception, which uses a credit card number without the physical presence of the card to shop at online stores (forgery). This mode can occur due to the weak authentication system used in ensuring the identity of ordering goods in online stores. Carding also recognized as a crime committed to stealing credit card numbers belonging to others and is used in trading transactions on the internet. Tej Paul Bhatla defined that credit card fraud occurs when someone uses someone else's credit card for personal reasons (interests) while the card owner and card issuer are not aware that the card is being used. Furthermore, the person uses the card without any connection to the cardholder or issuer and has no good intentions to contact the holder or make payments for purchases (Arief, 2003; Bhatla, 2003; Suseno, 2012).

Some examples of carding cases that have occurred in Indonesia, *first*, the Carding crime case appeared in March 2013. Several credit and debit card customer data from various banks were stolen when transacting at The Indonesian Body Shop outlets. The stolen data was used to make duplicate cards transacted in Mexico and the United States. The stolen data came from various banks, including Bank Mandiri and Bank BCA. Bank Mandiri found dozens of stolen data of credit and debit cards belong to its customers. The losses of the transaction through the stolen data are estimated at hundreds of millions of rupiahs. Credit card crimes are detected when Bank Mandiri discovers suspicious transactions. The cards are commonly used in Indonesia and suddenly used for purchases in Mexico and America. After checking the customers directly, it appears that the cards had never been used outside Indonesia (Thertina et al., 2013b, 2013a; Hasyim, 2013).

Second, in September 2011, the Jakarta Police succeeded in dismantling the credit card counterfeit syndicate with a substantial loss of 81 Billion Rupiahs. The syndicate breaks into credit card EDC data with two main modes. The first mode is stealing data from credit card EDC owners in shopping outlets or other transaction places. One of these data-stealing is EDC data theft from the public gas station at Kebayoran Lama, Jakarta, on August 18 to September 9 of 2011.

Encountering data theft as cybercrime is undoubtedly challenging. Aside from carding encompassing and relating to several cross-sectors, carding is also often done by transnational offenders, as an international crime. Handling transnational crime requires cooperation between countries. The crimes are no longer confined at one jurisdiction, but many. The situation leads to the difficulty of join forces between countries due to the sovereignty of each country, cultural differences, language, and differences in the legal system (Saleh, 2009; Kurniawan, 2014).

Credit card transactions are made for economic interest; thus, it can be related to business activities. However, the fault of card data thievery using information

Article History
Submitted 6 July 2019 - Revision Required 10 July 2019 - Accepted 11 November 2019

JURNAL HUKUM NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246
P-ISSN: 1412-6834
E-ISSN: 2550-0090

technology leads to criminal activity. Moreover, if the crime is done between countries, so, it is obvious to say that there are intersections between three kinds, which are business law, cyber law, and criminal law. The meetings between those fields are this article's point of discussion.

Methodology

This paper is normative legal research. The author compares several legal studies (Criminal Law, Commercial Business Law, Technology Law, and International Law) in Carding in Indonesia. The data obtained from various previous research sources, both print and online media. This study analyzes carding cases from the Indonesian Criminal Law Act, both General and Special Criminal Law, the Electronic Information and Transaction Law, the Banking Law, and various international conventions relating to carding (International Law).

Results and Discussion

Cybercrime in Various Legal Dimensions: The Intersections between Criminal Law, Business Commercial Law, Technology Law, and International Law

Carding as Cybercrime: A Legal and Terminology Dimension

Cybercrime comes from the word cyber, which means cyberspace or internet crime, which means crime (Rahardjo, 2002; Prasetyo, 2016). Cybercrime is an illegal act committed by an individual or a particular group in committing a crime in cyberspace; in other words, it is a crime that has been done in a virtual form. Efforts to deal with crime with criminal law are necessarily part of law enforcement efforts (especially criminal law enforcement). Therefore, it is often said that political or criminal law policies are also part of law enforcement (Sudarto, 1986).

Additionally, according to the British Police, cybercrime is all kinds of use of computer networks for criminal purposes or high-tech criminals by abusing the ease of digital technology (Wahid & Labib, 2005). Also, cybercrime is often identified as computer crime. The U.S. Department of Justice provides the understanding of computer crime as "…any illegal act requiring knowledge of computer technology for its perpetration, investigation, or prosecution." It can also be stated as "an illegal use from a credit or debit card, or similar payment instrument, to fraudulently obtain money or property" (Gema, 2013; FBI, 2018).

People in this digital era began to depend their lives on the internet as a medium of efficiency. Public trust in online transactions is the reason for the increasingly widespread use of credit cards for purchases. It is not only the development of the ease transaction but also the leaking of online data, which is the potential to be stolen away from its owner. One of the stolen data, maybe the most, is from a credit card in which the crime of stealing this data commonly named as carding (credit card fraud). Card fraud is the fraudulent acquisition or use of debit and credit cards, or card details, for financial gain. Organized crime groups are involved in sophisticated card

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246

fraud because they are motivated by the potential monetary benefits. Card fraud may also be linked with other organized crimes such as money laundering and different cyber-enabled fraud types. Identity fraud is committed when a criminal uses someone else's personal information to commit a crime. Identity crime is a crucial enabler to other crimes. It can take many forms, including: *first,* the theft of personal identity information and related financial information; *second,* assuming another person's identity for fraudulent purposes; *third,* producing false identities and financial documents to open other crimes (Australian Criminal Intelligence Commission, 2019).

In terms of legal perspective, the law is a form of configuration for the human civilization jointly developed through the community (Andryanto, 2019). Meanwhile, crime is a form of deviation from human morality. When examined based on this structure, we often find that victims of cyber fraud have not met legal certainty. Moreover, the encountered-case of cyber fraud has the potential to cause transnational crime. It is undoubtedly a problem, considering that the Indonesian state is still not in its full efforts in conducting cybersecurity to silence the offense in cyberspace. On the other hand, President of the Republic of Indonesia, Joko Widodo, emphasized that this country is not fully capable of combining trade activities with e-commerce as a technological advance (Manurung, 2014). The statement is supported by the minimum of public knowledge on potential crime in virtual space.

Based on data from the Consumer Security Risks Survey 2016 conducted by B2B International and Kaspersky Lab, it was revealed that five percent of global users lost their money due to online fraud. The average loss they suffered was 6 million rupiahs (Kaspersky, 2015, 2016). It has led to a crisis of trust between the business sector actors and banks. The business actors have felt that the banks are unsafe for securing online payments. The untrust leads to 47% of business and trade sector players are demanding the banks to tighten the cybersecurity. The advance of technology that should make the transactions easiest and safest has become the threat of crime (Kaspersky, 2015).

The lack of concern of the banks to the victims of carding is also one of a factor the law enforcement of this crime is low. Additionally, strengthening the legal channels regarding cyber fraud as a transnational crime also needs to be enhanced by the legitimacy of new international laws. This crime is borderless, which means that the perpetrator and the victim do not have to be in the same location or country (Schneider, 2013; Bossard, 1990; Décary-Hétu & Leppänen, 2016; Malika, 2018).

Based on reports from Digital Commerce, Indonesia is a country with a high level of e-commerce fraud, around 35%. Compared to other countries, Venezuela has a fraud rate just below Indonesia, which is 33%, South Africa 25%, Brazil 11%, and Romania is only 10% (Kaspersky, 2015).

Article History
Submitted 6 July 2019 - Revision Required 10 July 2019 - Accepted 11 November 2019

JURNAL HUKUM NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Some legal provisions in the context of law enforcement to overcome the existence of cybercrime, especially in the field of fraud in Indonesia itself has been regulated in the Electronic Transaction Information Act (i.e., *Undang-Undang Informasi dan Teknologi Elektronik,* abbreviated as ITE Law), Criminal Code (i.e., *Kitab Undang-Undang Hukum Pidana,* abbreviated as KUHP), and Commercial Law (i.e., *Kitab Undang-Undang Hukum Dagang*, abbreviated as KUHD). While in global regulations, arrangements related to cybercrime have been regulated in the Budapest Convention of Cyber Crime (currently known as Convention on Cybercrime (CoC)). Thirty-nine parties have attended the Convention of Cybercrime as of December 2012, including 35 European Countries, Australia, Dominican Republic, Japan, and the USA. There are 11 signatories, namely: European countries, Canada, South Africa, and eight countries invited to approve the convention, namely: Argentina, Chile, Costa Rica, Dominican Republic, Mexico, Panama, Philippines, and Senegal so that there are a total of 58 state parties or parties that are committed to becoming parties to the Convention of Cybercrime (Tosoni, 2018; Mittal & Sharma, 2017).

Carding: Modus Operandi and Driving Factors

The Criminal Code (KUHP) mentions several articles covering the notion of fraud in Article 362 concerning the thievery. However, the proof is key in the trial process, which will determine the fate of the defendant. If the results of the evidence are not sufficient to prove guilty of the defendant, the defendant is acquitted. Otherwise, if the defendant is determined by the evidence mentioned in Article 184 of the Criminal Procedure Code, the defendant must be found guilty and sanctioned. Therefore, the judges must be careful in assessing and considering the evidence (Yustisia, 2010; Alisan, 2019; Sulaeman, 2017).

Understanding fraud is such a generic term. It embraces various means, which are sorted to the act of getting an advantage over another by false. The essence of carding as cyber fraud is fraud by stealing the identity from a credit card or debit card to conduct online purchasing. In other words, the perpetrator will transact using the card information he took from the cardholder (Albrecht et al., 2012; Hopwood et al., 2012; Pearson & Singleton, 2008).

In the same context, some studies revealed that the misuse of credit cards could be done in two ways. First, credit cards are valid but are not used under specified rules on the agreement agreed upon between the credit card holder and the bank as the credit card manager. Second, using unauthorized/fake credit cards illegally (Tajpour et al., 2013; Omar et al., 2014; Anastasia & Santoso, 2020; Pratama & Salam, 2019). The usual modus operandi for the perpetrator is sending a fake web platform created by the perpetrators of cyber fraud. On the other side, the web platform contains business and trade activities such as clothing, food, and board sales. It is a takeover of an account so that it can be called piracy or misuse of funds with particular objectives as an effort to escape the responsibility of shopping payments (Saragih & Siahaan, 2016; Santoso et al., 2018).

P-ISSN: 1412-6834
E-ISSN: 2550-0090

JURNAL HUKUM NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246

Additionally, the modus operandi of carding in daily applications is also evident through the opening of an invalid credit card account with the name of the victim. The perpetrators did it because he had to obtain sufficient personal information so that when filling in the personal data at the bank, the perpetrators managed to escape in giving statements and, of course also fake documents attached to the bank (Heryadi et al., 2016; Saragih & Siahaan, 2016; Sutedja, 2019).

Factors that cause cyber fraud, if reviewed based on the Fraud Triangle Theory, there are three components, namely: opportunity, pressure, and rationalization (Abdullahi & Mansor, 2015; Kassem & Higson, 2012). First, the option is present as part of the loosening of the security system on a fake online store web platform, the spread of information about personal data, etc. Second, the pressure is recognized as incentives that encourage people to commit fraud because of lifestyle demands, powerlessness in financial matters, gambling behavior, trial and error to defeat the system, and job dissatisfaction (Pratama & Salam, 2019). Pressure as a manifestation of discontent received by an individual leads to courage in committing the crime to obtain justice, in the form of rewards for gaining recognition of the surroundings. Third, rationalization is an essential component in many frauds, and it causes fraudulent actors to justify their actions (C. O. Albrecht et al., 2018; Suryandari et al., 2019).

That is why law enforcement, through the proper laws and regulations, has become a severe issue in Indonesia to overcome cybercrime cases. The need to regulate and legislate the rules in cyber activities is based on several concerns. First, protecting government integrity and maintaining the reputation of a country. Second, helping countries avoid being a surge for criminals, such as terrorists, organized crime, and fraudulent operations. Third, assisting the states in preventing the designation as a comfortable place to store applications or data on the results of cybercrime. Fourth, increasing market confidence because of the existence of legal certainty that can protect interests in the business. Fifth, protecting classified data (classified), secrets, personal information, criminal court data, and public data that are deemed necessary to be protected. Sixth, protecting consumers and assisting law enforcement in preventing corruption. Seventh, enhancing national security and reducing vulnerability from terrorists attacks and actions done by those with bad intentions. Eighth, protecting the business world from business risks such as loss of market share, reputation damage, fraud, lawsuits from the public, and civil or criminal cases. Ninth, as a means to punish perpetrators of crimes in the field of information technology. Tenth, increasing the opportunities to recognize the electronic records as legal evidence in court in ordinary criminal cases such as thievery, fraud, murder, kidnapping, or computer crime or the act committed using the Internet (Setiyadi, 2003; Arifah, 2011; Napitupulu, 2017).

Business Sector and Its Challenges on Carding and Cyber Fraud Cases

In Indonesia, from data obtained by the SingTel Communication Group from Singapore, in 2013, online business transactions in Indonesia were doubled. During

Article History
Submitted 6 July 2019 - Revision Required 10 July 2019 - Accepted 11 November 2019

JURNAL HUKUM NOVELTY
Volume 11, Issue 02, 2020, pp. 235-246
P-ISSN: 1412-6834
E-ISSN: 2550-0090

the first semester, there were more than 19 million export, import, and domestic trade transactions through the internet in Indonesia, with a value of USD 478 million or around 5.1 trillion Rupiahs (Zuraida, 2015; Prabheesh & Rahman, 2019; Achsan et al., 2020). Considering the immense potential of carding in Indonesia and the global world, it is the business and trade actors' job in the private sector (banks) to overcome cyber fraud in their business. Thus, people will safely act their online business activities without worrying about their credit or debit card data would be stolen (Saputra, 2016; Karo & Sebastian, 2019; Hatta et al., 2018).

Businesses and commerce in the online platform are required to have reliable system security. The security system should be build due to the existence of operative crime by transnational crimes perpetrators of cyber fraud and crush credit card accounts that can be hijacked by the perpetrators. In minimizing cyber fraud in the business and trade sectors, efforts are needed from the community. First, keeping private data confidentially, such as self-identity, credit card numbers, etc. Second, being selective against fake online web store platforms. Third, avoiding malware or other spam messages sent by the web or particular parties. Fourth, before using a site, check the software or encryption first (Saragih & Siahaan, 2016).

In connection with this, banks as issuers of credit cards have responsibilities to solve the problems related to credit card fraud. Referring to the Bank Indonesia Circular Letter No. 13/28/DPNP, it states that the bank has four pillars as a fraud control system: prevention; detection; investigation, reporting and sanctions; and monitoring, evaluation, and follow-up (Idris, 2019).

Legal protection or bank responsibility towards customers as consumers can be done before the transaction (pre-purchase) or after (post-purchase). Consumers' legal protection could be made before the purchase (pre-purchase) by protecting consumers through legislation that has been made. Through this legislation, consumers are expected to obtain protection before the transaction because there have been restrictions and provisions governing transactions between consumers and business actors. Second, voluntary self-regulation, which is carried out before the trade. In this way, the business actor is expected to voluntarily make regulations for himself to be more careful and vigilant in carrying out his business (Gunawan, 1999; Rokhim et al., 2018; Abubakar & Handayani, 2019).

Conclusion

This paper highlighted that carding in the context of cybercrime is intersecting various legal issues, such as criminal law, cyberlaw, information and technology law, business law, and international law. In Criminal Law, carding as cybercrime has been regulated, whether directly or indirectly, in the Indonesian Criminal Code (Article 362, Article 363, and Article 378). However, the criminal law on cybercrime (carding) also paid more attention to the verification process (proof) in this case. In Commercial Law, carding and a credit card, alluding to the agreement section, especially on Article

JURNAL HUKUM NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 11, Issue 02, 2020, pp. 235-246

1338 KUHD. In the international law context, the carding as cybercrime has been stipulated on Budapest Convention on Cybercrime.

References

Abdullahi, R., & Mansor, N. (2015). Fraud Triangle Theory and Fraud Diamond Theory. Understanding the Convergent and Divergent for Future Research. *International Journal of Academic Research in Accounting, Finance and Management Science*, *5*(4), 38–45.

Abubakar, L., & Handayani, T. (2019). Implementation of the Principles for Responsible Banking in Indonesian Banking Practices to Realize Sustainable Development Goals. *3rd International Conference on Globalization of Law and Local Wisdom (ICGLOW 2019).*

Achsan, W., Achsani, N. A., & Bandono, B. (2020). Impact of Macroeconomic Condition on Credit Card Default in Emerging Economy: Empirical Evidence from Indonesia. *International Journal of Finance and Banking Research*, *6*(3), 37–43.

Albrecht, C. O., Holland, D. V, Skousen, B. R., & Skousen, C. J. (2018). The Significance of Whistleblowing as an Anti-Fraud Measure. *Journal of Forensic & Investigative Accounting*, *10*(1), 1–13.

Albrecht, W. S., Albrecht, C. C., & Albrecht, C. O. (2012). *Fraud Examination*. Cengage Learning.

Alisan, R. R. A. (2019). The Role of Digital Forensics in Proof of Illegal Content Crimes. *Kader Bangsa Law Review*, *1*(2), 80–91.

AlMajed, N., Maglaras, L. A., Siewe, F., Janicke, H., & Zadeh, P. B. (2016). Prevention of crime in B2C E-Commerce: How E-Retailers/Banks protect themselves from Criminal Activities. *EAI Endorsed Transactions on Security and Safety*, *3*(7).

Anastasia, N., & Santoso, S. (2020). Effects of Subjective Norms, Perceived Behavioral Control, Perceived Risk, and Perceived Usefulness towards Intention to Use Credit Cards in Surabaya, Indonesia. *SHS Web of Conferences*, *76*, 01032.

Andryanto, C. (2019). Law Enforcement Against Fraud and/or Embezzlement (Study of KSP Intidana Central Java, Indonesia). *JILS (Journal of Indonesian Legal Studies)*, *3*(1), 47–74. https://doi.org/https://doi.org/10.15294/jils.v3i01.23205

Arief, B. N. (2003). *Kapita Selekta Hukum Pidana*. Citra Aditya Bakti.

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

Arifin, R. (2018). Law Enforcement in Banking Criminal Act Involving Insiders. *Jambe Law Journal*, *1*(1), 55–90.

Australian Criminal Intelligence Commission. (2019). *Fraud*. https://www.acic.gov.au/about-crime/crime-types/fraud

Bhatla, T. P. (2003). *Understanding Credit Card Frauds*. Cards Business Review.

Bossard, A. (1990). *Transnational Crime and Criminal Law*. Office of International Criminal Justice, University of Illinois at Chicago.

Décary-Hétu, D., & Leppänen, A. (2016). Criminals and signals: An assessment of

Article History
Submitted 6 July 2019 - Revision Required 10 July 2019 - Accepted 11 November 2019

Volume 11, Issue 02, 2020, pp. 235-246
P-ISSN: 1412-6834
E-ISSN: 2550-0090

criminal performance in the carding underworld. *Security Journal*, *29*(3), 442–460.

Faridi, M. K. (2018). Kejahatan Siber dalam Bidang Perbankan. *Cybersecurity Dan Forensik Digital*, *1*(2), 57–61.

Fatima, A. (2011). E-Banking Security Issues – Is There A Solution in Biometrics? *Journal of Internet Banking and Commerce*, *16*(2), 67–84.

FBI. (2018). *Credit Card Fraud*. https://www.fbi.gov/scams-and-safety/common-fraud-schemes/credit-card-fraud

Featherly, K. (2016). *ARPANET: United States Defense Program*. Encyclopedia Britannica, inc.

Gema, A. J. (2013). *Cybercrime: Sebuah Fenomena di Dunia Maya*. Interpol Indonesia. http://www.interpol.go.id/en/transnational-crime/cyber-crime/89-cybercrime-sebuah-fenomena-di-dunia-maya.

Gunawan, J. (1999). *Hukum Perlindungan Konsumen*. Universitas Katolik Parahyangan.

Hasyim, F. P. (2013). *Visa Investigasi Pencurian Data Kartu Kredit*. TEMPO. https://bisnis.tempo.co/read/469205/visa-investigasi-pencurian-data-kartu-kredit/full&view=ok

Hatta, M., Rajamanickam, R., Abdullah, D., & Hartono, H. (2018). Efforts to Overcome Cyber Crime Actions in Indonesia. *Journal of Physics: Conference Series*, 012081.

Heryadi, Y., Wulandhari, L. A., & Abbas, B. S. (2016). Recognizing debit card fraud transaction using CHAID and K-nearest neighbor: Indonesian Bank case. *Proceedings - 11th 2016 International Conference on Knowledge, Information and Creativity Support Systems, KICSS 2016*, 1–5. https://doi.org/10.1109/KICSS.2016.7951441

Hopwood, W. S., Leiner, J. J., & Young, G. R. (2012). *Forensic Accounting and Fraud Examination*. McGraw-Hill.

Idris, H. D. P. (2019). Kebijakan dalam Penanggulangan Penyalahgunaan Kartu Kredit. *Lex Privatum*, *7*(4), 15–25.

Karo, R. K., & Sebastian, A. (2019). Juridical Analysis on the Criminal Act of Online Shop Fraud in Indonesia. *Lentera Hukum*, *6*(1), 1–14.

Kaspersky. (2015). *Global I.T. Security Risks Survey*. Kaspersky Lab. http://go.kaspersky.com/rs/802-IJN-240/images/Global I.T. Security Risks Survey Ent.pdf

Kaspersky. (2016). *Consumer Security Risks Survey 2016*. Kaspersky Lab. https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08233604/B2C_survey_2016_report.pdf

Kassem, R., & Higson, A. (2012). The New Fraud Triangle Model. *Journal of Emerging Trends in Economics and Management Sciences*, *3*(3), 191–195.

Kurniawan, N. A. (2014). *Pencegahan Kejahatan Carding Sebagai Kejahatan Transnasional Menurut Hukum Internasional*. Universitas Brawijaya.

Malika, A. (2018). *Pengaturan Hukum Internasional Terhadap Kejahatan Carding (Penggunaan Ilegal Kartu Kredit) Sebagai Bentuk Cybercrime*. Universitas

JURNAL HUKUM
NOVELTY
P-ISSN: 1412-6834
E-ISSN: 2550-0090
Volume 11, Issue 02, 2020, pp. 235-246

Sumatera Utara.

Manurung, H. (2014). Joko Widodo National Leaderships on Indonesia's World Maritime Policy. *SSRN Electronic Journal*, *2510986*. https://ssrn.com/abstract=2510986 or http://dx.doi.org/10.2139/ssrn.2510986

Mittal, S., & Sharma, P. (2017). A review of international legal framework to combat cybercrime. *International Journal of Advanced Research in Computer Science*, *0976–5697*.

Napitupulu, D. (2017). Kajian Peran Cyber Law Dalam Memperkuat Keamanan Sistem Informasi Nasional. *Deviance Jurnal Kriminologi*, *1*(1), 100–113.

Omar, N. A., Rahim, R. A., Wel, C. A. C., & Alam, S. S. (2014). Compulsive Buying and Credit Card Misuse among Credit Card Holders: The Roles of Self-Esteem, Materialism, Impulsive Buying and Budget Constraint. *Intangible Capital*, *10*(1), 52–74.

Pearson, T. A., & Singleton, T. W. (2008). Fraud and Forensic Accounting in the Digital Environment. *Issues in Accounting Education*, *23*(4), 545–559.

Prabheesh, K. P., & Rahman, R. E. (2019). Monetary Policy Transmission and Credit Cards: Evidence from Indonesia. *Buletin Ekonomi Moneter Dan Perbankan*, *22*(2), 137–162.

Prasetyo, S. N. (2016). Rumusan Pengaturan Credit Card Fraud dalam Hukum Pidana Indonesia Ditinjau dari Asas Legalitas. *Legality*, *24*(1), 101–119.

Pratama, S. A., & Salam, A. (2019). Tinjauan Yuridis Pertanggungjawaban Hukum Kartu Kredit Pemerintah di Indonesia. *Jurnal Hukum & Pembangunan*, *49*(3), 710–742.

Rahardjo, B. (2002). *Keamanan Sistem Informasi Berbasis Internet*. PT INDOCISC–Jakarta.

Rokhim, R., Adawiyah, W., & Faradynawati, I. A. A. (2018). Financial Consumer Protection in Indonesia: Towards Fair Treatment for All. In *An International Comparison of Financial Consumer Protection* (pp. 201–224). Springer.

Saleh, Z. (2009). The impact of identity theft on perceived security and trusting E-commerce. *The Journal of Internet Banking and Commerce*, *8*(2), 1–11.

Santoso, R., Erstiawan, M. S., & Mujayana, M. (2018). Review of Virtual Currency Potential as a Payment Instrument in Legal Aspect in Indonesia. *International Journal of Business and Management Invention (IJBMI)*, *7*(12), 57–64.

Saputra, R. W. (2016). A survey of cybercrime in Indonesia. *2016 International Conference on ICT For Smart Society (ICISS)*, 1–5.

Saragih, Y. M., & Siahaan, A. P. U. (2016). Cyber Crime Prevention Strategy in Indonesia. *SSRG Int. J. Humanit. Soc. Sci*, *3*(6), 22–26.

Schneider, F. (2013). The financial flows of transnational crime and tax fraud in OECD countries: what do we (not) know? *Public Finance Review*, *41*(5), 677–707.

Setiyadi, M. W. R. (2003). *Urgensi Cybercrime Law sebagai Perlindungan bagi Pengguna Teknologi Informasi Pendekatan Kebijakan Publik dalam Menjawab Kebutuhan Terhadap Perangkat Legal Untuk Memerangi Kejahatan di Bidang*

Article History
Submitted 6 July 2019 - Revision Required 10 July 2019 - Accepted 11 November 2019

Volume 11, Issue 02, 2020, pp. 235-246
P-ISSN: 1412-6834
E-ISSN: 2550-0090

Teknologi Informasi (Cybercrime) (Cybercrime Seminar).

Sudarto, S. (1986). *Kapita Selekta Hukum Pidana*. PT Alumni.

Sulaeman, S. (2017). The Application of Criminal Sanctions Against Violations of Cybercrime. *Indonesia Prime*, *2*(1), 56–67.

Suryandari, N. N. A., Yuesti, A., & Suryawan, I. M. (2019). Fraud Risk and Earnings Management. *Journal of Management*, *7*(1), 43–51.

Suseno, S. (2012). *Yurisdiksi Tindak Pidana Siber*. Refika Aditama.

Sutedja, I. (2019). Detection of Frauds for Debit Card Transactions at Automated Teller Machine in Indonesia Using Neural Network. *In Journal of Physics: Conference Series*, 012076.

Tajpour, A., Ibrahim, S., & Zamani, M. (2013). Identity Theft Methods and Fraud Types. *IJIPM: International Journal of Information Processing and Management*, *4*(7), 51–58.

Thertina, M., Putri, A., & Rina, D. (2013a). *Data Kartu Kredit di The Body Shop Dicuri*. TEMPO. https://koran.tempo.co/read/ekonomi-dan-bisnis/304254/data-kartu-kredit-di-the-body-shop-dicuri?

Thertina, M., Putri, A., & Rina, D. (2013b). *Data Kartu Kredit Ini Dicuri untuk Belanja di AS*. TEMPO. https://bisnis.tempo.co/read/467917/data-kartu-kredit-ini-dicuri-untuk-belanja-di-as/full&view=ok

Tosoni, L. (2018). Rethinking Privacy in the Council of Europe's Convention on Cybercrime. *Computer Law & Security Review*, *34*(6), 1197–1214.

Verisign. (2005). The Verisign Report: Industry Update. *Internet Security Intelligence Briefing*, *3*(2), 1–13.

Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. Refika Aditama.

Yustisia, M. (2010). Pembuktian dalam Hukum Pidana Indonesia terhadap Cyber Crime. *Pranata Hukum*, *5*(2), 77–90.

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