Advances in Economics, Business and Management Research, volume 121
International Conference on Law Reform (INCLAR 2019)

Identity Theft and the Rules in Indonesia's Criminal Law

Said Noor Prasetyo[1*] Tongat[1] Nur Putri Hidayah[1]

[1]*Faculty of Law, University of Muhammadiyah Malang, Malang, Indonesia*
[*]*Corresponding author. Email: saidnoor@umm.ac.id*

ABSTRACT
in the digital era, electronic identity is something that is very important to protect because it is a representation of someone in an electronic system. Along with the development of information technology, this type of crime also developed with the emergence of cybercrime. One type of cybercrime that threatens someone's identity is identity theft. This crime always haunts us when surfing in cyberspace. Many criminals target identity as the key to accessing someone's personal accounts such as bank accounts, credit cards, and other accounts. This crime is a serious threat in the digital era, especially in Indonesia. This is due to a lack of awareness of citizens in protecting their identities and the existence of inadequate laws in providing protection. This situation is certainly a threat in strengthening the civil society in the digital era
Keywords: *identity theft, cybercrime, Indonesian criminal law*

1. INTRODUCTION

According to the Great Dictionary of Bahasa Indonesia, identity is the characteristic or special circumstances of a person or one's identity. Identity is seen in terms of the identity language derived from the English "identity" which can be interpreted as traits, signs, or identity. Identity is a special sign or characteristic of something, especially people, such as name, address, date of birth and so on. Identity is a characteristic that distinguishes someone from others. In banking, it is this identity that marks the existence of a person in a banking account.

In today's digital age, Internet users in Indonesia have begun to trust themselves to conduct financial transactions online. One of the consequences is the rising popularity of e-commerce and online shopping activities. Research from BMI Research even predicted that the number of online shopping transactions in Indonesia will reach Rp 50 trillion (2015), doubled (Rp 21 trillion) from 2014. Unfortunately, the user's confidence in doing financial transactions online is not accompanied by awareness of security and privacy in cyberspace. It is this unwillingness that cyber criminals use in order to obtain user data for their criminal activity. An example that happened some time ago was the malware incident Dyreza or Dyre. Malware targeting thousands of websites belonging to banking institutions is able to steal over US $1 million from corporate bank accounts, and even be able to steal user-owned login credentials and use them to conduct illegal transactions without Owner's knowledge. The incident is one of the biggest attacks targeting banking institutions.

The combination of user's agility and increasing online transaction activity make Indonesia as a soft target for cyber criminals. The number of attacks occurred in Indonesia in 2014 years ago, according to data Security Incident Response Team on Internet Infrastructure (Id-SIRTII), reached 48.8 million attacks. This amount is equivalent to nearly half of the total Internet users in Indonesia reaching 88.1 million. Of course, many of the direct or indirect impacts of this threat are caused. Looking from a macro perspective, this threat can adversely affect the viability of the trading industry, service providers, and online financial transactions.

The crime of identity theft is still relatively new. But this crime has caused many financial losses especially in the banking world. There is basically no loss if the person's identity is lost or stolen. However, the loss arises when the identity is used in committing crimes. Identity Theft is an introductory act as a means to commit a criminal offense.

Many countries, especially developed countries, have committed criminalization of this act given the magnitude of the harm that this crime can inflict. This is different from Indonesia, in particular, there are no specific arrangements regarding this identity theft in Indonesian criminal law. This does not mean that Indonesian criminal law is unable to reach this type of crime. In 2008, the Indonesian government imposed law number 11 year 2008 on electronic information and transactions. Many circles say that this legislation is a new regime in the law on Cyber.

Based on the background as outlined above, the problem formulation in this research is how identity theft arrangement in Indonesian criminal law?

2. METHOD

The method of approach used in this research is the normative juridical method of approach. Specifically, the

authors use the approach of legislation (of Approach) conducted by studying all laws and regulations that are relevant to the legal issues being addressed, as well as the conceptual approach (The conceptual approach) [1] Also known as research for doctrinal law that uses secondary data[2] Secondary Data In this research consist of primary legal materials consisting of all Indonesian criminal law regulations that have to do with identity theft, secondary legal material consisting of books and journals on Identity theft and tertiary legal material consisting of Dictionary of both language dictionaries and legal dictionaries and encyclopedia. To get every required data, the author uses literature studies and documentation. Any data obtained will be analyzed using qualitative descriptive analysis method.

3. RESULTS AND DISCUSSION

A. Overview of Identity Theft

There are some definitions of identity theft, including those given by the Canadian Privacy Commissioner, that:
Identity theft is the unauthorized collection and use of your personal information, usually for criminal purposes. Your name, date of birth, address, credit card, Social Insurance Number (SIN) and other personal identification numbers can be used to open credit card and bank accounts, redirect mail, establish cellular phone service, rent vehicles, equipment, or accommodation , and even secure employment [3].
It is also presented by The Department of the Solicitor General Canada and United States Department of Justice, that Identity theft refers to all types of crimes where a person takes and uses a person's personal data in a illegal manner by committing fraud to economically gain [4]. Jonathan Clough in his books Principles of Cybercrime explains his identity theft:
"Refer to those specific offenses which address the unauthorised acquisition and distribution of identity information. These are preparatory offenses, which seek to punish the misuse of identity information irrespective of whether that information is ultimately used in the commission of an shareholdings. Each jurisdiction bases its offenses around a central concept of ' identity document ' or ' identity information [5].
Clough's opinion can be translated that identity theft refers to certain violations involving illegal acquisitions and distribution of information about identity. This breach constitutes a preparatory crime, which seeks to punish the misuse of identity information regardless of whether the information is ultimately used in a criminal offence. Based on Clough's opinion, identity theft is a preparatory criminal act. The object of this criminal offence is the victim's identity data either in the form of identity documents, as well as data of victim identity information. The reason for this crime is called a preparatory criminal act because the object of crime is not the main goal of the perpetrator. The main objective of the perpetrator obtaining the victim's identity data is to gain access to credit cards, debit cards, bank accounts, etc. and use them (illegally) to get financial benefits.
In line with what the Clough presented, in the Encyclopedia of Cybercrime compiled by Samuel C. McQuade explains that as a goal of committing identity theft, actors generally need it to do two things. First, they must obtain unique personal information belonging to the victim, such as name, address, date of birth, telephone number, credit card number, or social security number. Secondly, they must use such information illegally for fraudulent purposes. In some countries, the perpetrators do not actually have to use the victim's information to commit fraud, only having one's information after being illegally acquired is enough to be considered a crime. Such fraud can be credit card fraud, telephone or utilities fraud and also bank fraud [6].
According to Identity Theft and Assumption Deterrence Act of 1998 [7] The United States, the Deeds Tegolong as Identity Theft are deeds intentionally sending or using, without legal authority, an identity of another person with the intent to perform, or to help do or conspired, conduct unlawful activities. Based on the explanation as mentioned above, then it can be found an understanding that identity theft is a person's actions to obtain either by taking or distributing/transferring data regarding an identity (such as name, address, date of birth, phone number, credit card number, credit card expiry date, CcV number, credit card usage limit) belonging to the other person (victim) against the right or unauthorized with the intention to do or used to commit a crime. However, whether identity data is ultimately used to commit crimes or not, it is still considered a crime.
Identity theft's terminology is used in a broad sense. This means that the use of the term not only refers to identity theft, but also refers to the use of other means such as fraud. As presented by McQuade that identity theft, also referred to as identity fraud, is a criminal act where one individual misrepresents himself by pretending to be someone else [6]. It is also delivered by the Canadian Internet Policy and Public Interest Clinic (cippic[1]) which mentions:
"The term" identity theft ",... Refers broadly to the combination of unauthorized collection and fraudulent use of someone else's personal information. It thus encompasses a number of activities, including collection of personal information (which may or may

not be undertaken in an illegal manner), creation of false identity documents, and fraudulent use of the personal information".
That the term "identity theft", refers broadly to the combination of illegal collection/retrieval and use of fraudulent means of personal information of others. Thus includes a number of activities, including the collection of personal information (which may be done illegally or may not), the creation of false identity documents, and the use of fraudulent personal information. Referring to both opinions, the notion of "theft" does not only refer to acts of theft (a narrow meaning). The term "theft" is used in a broad sense (not just theft). That is, the identity theft is a deed of obtaining/obtaining the identity of others illegally. This action can be done by means of theft, fraud, buying on the "black market", tapping, darkening, and so forth throughout the deed is to obtain/acquire/master the identity data of others against the law. Obtaining personal information is the first step of the crime of identity theft. The goal is to get enough information about the victim to be able to transact on behalf of the victim.

B. Urgency Setting Identity Theft in Indonesian Criminal Law

As has been outlined in the previous section that identity theft is a preparatory criminal act. The purpose of this criminal offence is to obtain/obtain personal information or identity data either in physical form (identity document) as well as personally identifiable information (in the form of electronic data).

C. Various Modes in Identity Theft and Arrangement in Indonesian Criminal Law

Various modes in Identity Theft and arrangement in Indonesian criminal law
Identity theft's terminology is used in a broad sense. This means that the use of the term not only refers to identity theft, but also refers to the use of other means such as fraud. As presented by McQuade that identity theft, also referred to as identity fraud, is a criminal act where one individual misrepresents himself by pretending to be someone else [6]. It is also delivered by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) which mentions:
"The term" identity theft ",... Refers broadly to the combination of unauthorized collection and fraudulent use of someone else's personal information. It thus encompasses a number of activities, including collection of personal information (which may or may not be undertaken in an illegal manner), creation of false identity documents, and fraudulent use of the personal information"[8].
That the term "identity theft", refers broadly to the combination of illegal collection/retrieval and use of fraudulent means of personal information of others. Thus includes a number of activities, including the collection of personal information (which may be done illegally or may not), the creation of false identity documents, and the use of fraudulent personal information.
Personal information can be gathered from a variety of sources and by a variety of methods, some of which are relatively simple and low-technology (such as: Reading obituary; stealing letters from homes, offices and mailboxes; breaking offices or vehicles to Steal files; Steal items and bags, and tear apart trash bins in the home and office) and other more sophisticated methods (such as: stealing or hacking into a computer; impersonating clients when calling insurance companies, credit card companies, using the services Online information brokers, and duplicate magnetic strips on the back of the card). This method can be done either directly or virtually via the Internet, phone line or mobile phone. The method used is always evolving. If law enforcement can do better identification of commonly used methods, the perpetrators of the theft immediately switch to the new method. Personal information is not only directly obtained by thieves, but can also be purchased from third parties, such as phishing site operators or employees who have stolen information. Online "Network Carder" has emerged as a place where identity thieves can buy and sell personal information stolen by illega [6].
Along with the development of technology, the perpetrators of identity theft also develops the techniques that they use to get credit cards as well as personal information/credit card holders to trick security systems from credit cards that are always developed. Below will the authors describe some techniques that are commonly used by actors to obtain the personal identity of the cardholder and its arrangements in Indonesian criminal law.

1. Theft of wallets, mobile phones, computers and other personal information sources

Wallets, bags, mobile phones, computers (especially laptops) and other storage sources can be stolen, can also be lost or lagged and later discovered by people who have malicious intentions. In these items there are credit cards, debit cards, cheques, driver's licenses, account information, social insurance numbers and other personal information data. All this and other parts of personal information can be in the hands of thieves in one action. The card can be left in the restaurant, at the cashier, or at the ATM machine, where the card can be taken by thieves.[6]
Generally every person who has a credit card keeps his or her credit card in the wallet. By taking a wallet or

victim bag , the perpetrator also get a credit card, debit CARD, ID card, driver's license, and other identity card stored in the wallet. Perpetrators can also take credit cards/debit cards belonging to victims who are left at the CASHIER or at the ATM machine.

The credit card that has been mastered by the perpetrator can use it directly for transaction. Looking at the characteristics of the perpetrator's deeds, perpetrators act as taking a wallet belonging to another person (either partially or wholly) without permission with the intention to possess or master it.

a. Retrieving electronic data/information stored in a storage device of an electronic device

Along with the development of information technology, especially in the field of banking and trade, does not close the possibility of someone using a cell phone and or his laptop to make transactions, both trading (e-commerce) and Banking (e-banking). The electronic trading transaction Data can be stored in storage.

Such electronic devices can be acquired by stealing, or pretending to be electronic device repair technicians such as mobile phones (especially smartphones) and computers. Actors can search for any transaction data stored in each of these tools, especially credit card data. With its expertise, perpetrators can retrieve the credit card data stored in the transaction history stored in each electronic device. Thus, perpetrators can master the credit card's electronic data belonging to the victim. With the credit card electronic data, the perpetrator can do several things such as using it to transact as a means of payment in e-commerce, actors can also input credit card electronic data into the card Using a new tool or commonly called counterfeiting card. Further discussion of such matters will be discussed further in the next section.

b. Skimming (magnetic strip duplication)

On the magnetic band on the credit card is recorded data/information about the credit card. This Data is read by a skimmer found in a friction machine (EDC) on the checkout transaction process. Using a similar tool, the perpetrator can read and record any data contained in the magnetic ribbon of the credit card that swiped on the device.

By swiping the card through a skimmer, the thief can copy the information stored on the magnetic tape of the debit card or credit card and use it in making additional cards (fake cards) for fraudulent purposes [6]. A skimmer is a tool for recording/retrieving (or reading, pen) The data of a card. The way the tool works is to copy the data contained in the card's macnetic ribbon when swiping on the device [9]. So, skimming is a person's attempt to copy the data/information contained in the magnetic tape of the card, whether it is a debit card, credit card or another card using a skimmer.

This action is usually done by the cashier of a store that accepts payment instruments using a credit card. In the payment process, the buyer submit his/her credit card to the cashier. Next, the cashier swiping the credit card on a tool called EDC (Electronic Data Capture). The tool reads and Sekalligus records the electronic data contained in the Ribbon for subsequent credit card authentication.

The mode often performed by the cashier "naughty" is after the cashier swiping the credit card on the EDC during the payment process, the cashier swiped back for a second time on another skimmer that has been provided by the cashier to record card data Without the cardholder's knowledge. Once the credit card is swiping on the skimmer, every important credit card data will be recorded and stored and of course it has all the data. Basically, this scheme of deed has similarities with the previous sections. In this way, perpetrators retrieve data or credit card information stored in the magnetic strip of the credit card.

c. Letter theft

Theft of mail is a very easy way to steal personal information. The letter can be stolen from the mailbox in the home and office and from garbage as well as from the Recycle Bin. The letter provides an excellent source of personal information-such as bank notices and credit cards, SIM renewal, credit card filing applications, electricity bills and so on. It can provide important details, such as the name of the victim's bank, account number, signature, DRIVER's license number, credit card number and its limitations. Based on the CALPIRG survey of American law enforcement officers, 68% of the officers surveyed were known that the theft of mail as a primary concern was related to identity theft.

1. Insider Theft (theft by insiders)

Insider theft is the theft of personal data done by people in an agency. Identity theft is often derived from people in an institution holding personal information. Every worker has the potential to perform this deed because of the magnitude of the data of a bank, the government and the company holds a lot of personal information while supervision against them is very minimal especially against former workers. The Data includes ATM card numbers, PIN codes, credit card numbers and card expiry dates, passwords, account information, and other personal information.

In relation to credit card, the person who is in charge of the person who works in the agencies related to credit card transactions, such as credit card issuer either bank or non-bank, and also the acquirer party. These parties have each cardholder's personal data that should be kept confidential. In this technique, perpetrators (people in) take or rather copy any credit card data in the power of the institution wheredia bekerja tanpa seijin instansi yang bersangkutan.

d. Purchasing stolen personal information (sale and purchase of stolen personal Data)

This is one of the easiest ways to get personal information without raising suspicion from the victim. Personal information can be obtained through "network Carder" and other "underground" networks specializing in the trading of personal information. Personal information available from this source is usually the result of theft made by an inner person or theft of personal data that utilizes the weaknesses of computer network security systems [5].

Based on the aforementioned description, carding actors or credit card fraud buy data or personal information relating to credit cards from data thieves/credit card electronic information. This has been the author of tangent in the previous section where the perpetrator of personal data theft credit card can sell such data in the Carder network. This network is a covert network that trades personal data or information including personal data of criminal liability credit cards.

e. Social engineering

Social Engineering is an effort to obtain information by committing fraud that makes use of human weaknesses that easily believes in others [9]. According to Mc Quade Social Engineering is an act of manipulating or committing fraud to convince someone or some person to provide personal data or financial data or data/information related to security, or to provide access to such personal or financial data storage [6].

Unlike other methods, it does not manipulate technology against computer hardware or software weaknesses, and does not require much technical expertise. Instead, these methods exploit weaknesses – such as human carelessness or desire to be cooperative – to gain access to legitimate identity information networks. This way relies on human talents/skills, such as engaging personalities, persuasive approaches, etc..[10]

In this method, perpetrators trick potential victims with a into approach with either appearance, or waffle. The purpose of this method is that prospective victims will notify each personal data of their credit card. Usually, actors pretend to be from official institutions and usually also from credit card issuing banks. With its into ability, perpetrators can make credit card holders believe in identity actors so that by realizing the candidate victims to notify each personal data of the credit card owned by the victim.

f. Phishing, pharming

Phishing is fraudulent with the Internet-based by sending spammed e-mails to one or more people, companies or organizations, with the intention of making the receiver believe (hooked) so as to voluntarily provide or Disclosing information about the recipient's self, especially with respect to personal and confidential information such as ID, account number, credit card number, Password, PIN (Personal Identification Number), etc., as requested or Mentioned in the e-mail [9]. The e-mail is a fake e-mail that looks like it comes from a large company such as a bank, a credit card issuing company, an on-line store, etc., thus making the recipient of the e-mail believe and provide Voluntarily requested information [11] This method is intended to commit fraud by relying on the recipient's inability to distinguish fake emails, messages, websites, and other online content, from legitimate-they are all designed to appear with legitimacy [12].

Pharming is an exploit that directs users to a fake site by poisoned DNS (DNS Poisoning) with a false IP address. When compared to Phishing, Pharming is more sophisticated, because the link looks like the original city address. Even with a thorough examination of the URL will not be seen suspicious things because the IP address of THE URL has changed IN DNS [13]. Victims will not feel suspicious because the address of the site that he opens exactly matches the original website address. So the victim will easily enter his credit card data. Once the data is entered, the victim's credit card data is already in the possession of the actors. Basically, phishing and pharming have a common trait with social engineering, where the three are equally fraudulent deeds. The difference lies in the way it is used. The social engineering relies solely on persuasive skills of perpetrators without the need for technical skills related to technology. While in phishing and pharming using these technical skills.

In phishing and pharming, perpetrators use Information technology as a tool, especially e-mail. By e-mail, perpetrators attract potential victims to provide personal data/information related to their credit card with a variety of reasons. These reasons can be promotional offers, system changes, system errors, and various other reasons with the name of the trusted institutions/agencies.

g. Man in the middle attack/ Interception (penyadapan)

Man in the middle attack is an attack in which a perpetrator intercepts the data and answers it, so it looks as if the answer comes from the intended recipient. A victim who is attacked may provide personal data – such as credit card information or bank account information – which can later be used to commit fraud [11]. Basically, "Man in the middle attack" is a tapping. The existence of the perpetrator is between two or more parties information networks. So that any information that runs can be known to the perpetrator, including any important information about a person's credit card.

4. CONCLUSION

Based on the results of the research and the languageN as the authors described in the previous chapter, the authors can take the error that identity theft in Indonesian criminal law is scattered in some laws. First, set in the Criminal CODE, Act No. 11 year 2008 on information and electronic transactions, Law No. 7 year 1992 Jo Act Number 10 year 1998 concerning banking, Law number 36 year 1999 about telecommunications. In the criminal CODE, identity theft is set out in article 362 of theft for the theft mode of the storage device in which the personal data stored by a person such as wallets, bags, cell phones, computers, and other storage devices, as well as letters, article 378 on fraud for social engineering, phishing and

pharming mode, section 480 of the admisation for the buying**.**
In the Act No. 7 year 1992 Jo Act No. 10 year 1998 on banking is set out in article 40 Jo Article 47 on the prohibition of opening secret banks for insider theft mode. In the Act No. 36 year 1999 of telecommunications article 40 is set about the prohibition of intercepting telecommunication transmission for man in the Middle attack (interception) mode specifically for wiretapping against the transmission of telecommunication conversation data , whereas for the transmission of electronic information data is set out in article 31 paragraph (1) and (2) of Law No. 11 of 2008 on electronic information and transactions.
Therefore, to ensure the certainty of law and justice, and to anticipate the danger of identity theft, then the government should make a special arrangement about identity theft is more comprehensive.

REFERENCES

[1] Peter Mahmud Marzuki, *Penelitian Hukum, Edisi Pertama Cetakan Kelima*. Jakarta: Kencana, 2009.

[2] Ronny Hanitijo Soemitro, *Metodologi Penelitian Hukum dan Jurimetri*. Jakarta: Ghalia Indonesia, 1988.

[3] Privacy Commissioner of Canada, "Fact Sheet: Identity Theft: What it is and what you can do about it." [Online]. Available: http://www.privcom.gc.ca/fs-fi/02_05_d_10_e.asp.

[4] Department of the Solicitor General Canada and United States Department of Justice, "Public Advisory: Special Report for Consumers on IDENTITY THEFT," 2011. .

[5] J. Clough, *Principles of Cybercrime*. New York: Cambridge University Press, 2010.

[6] S. C and McQuade, *Encyclopedia of Cybercrime*. London: Greenwood Press, 2009.

[7] PUBLIC LAW, "Identity Theft and Assumption Deterrence Act of 1998," *Section 3*, 1998. .

[8] Parkes and Wendy, "Techniques of Identity Theft (Working Paper No. 2, Identity theft series)," Ottawa, 2011.

[9] Vyctoria, *Bongkar Rahasia E-Banking Security dengan Teknik Hacking dan Carding*. Yogyakarta: Penerbit ANDI, 2013.

[10] Debra Littlejohn Shinder, *Scene of the Cybercrime: Computer Forensics Handbook*. Amerika Serikat: Sygress Publishing. Inc, 2002.

[11] B. Schell and Clemens Martin, *Webster New World Hacker Dictionary*. Indiana: Wiley Publishing. Inc, 2006.

[12] Shun-Yung Kevin Wang and Wilson Huang, "THE EVOLUTIONAL VIEW OF THE TYPES OF IDENTITY THEFTS AND ONLINE FRAUDS IN THE ERA OF THE INTERNET," *J. Criminol.*, vol. 1, no. 1, pp. 1–21, 2011.

[13] J. J. Parson and Dan Oja, *New Perspective on Computer Concepts 2014: Comprehensive*. Boston: Course Technology, 2013.