ATLANTIS PRESS

Advances in Social Science, Education and Humanities Research, volume 307

1st Social and Humaniora Research Symposium (SoRes 2018)

Tightening Loose Ends in Eradicating Card Fraud

(Reviewing card skimming case verdict in Denpasar, Indonesia)

Anton Hendrik S, Nian Qisthi K
Criminal Law Department, Faculty of Law
University of Surabaya
Surabaya, Indonesia
antonhendrik@staff.ubaya.ac.id, nianqisthi@yahoo.com

***Abstract*—Open codification system obligates the law enforcement aware of the special rule outside Criminal Code. Sometimes failure to do so happens. This paper reviews a court decision of a skimming case in Indonesia. The method is reviewing the court decision, provide special law and the reasoning that applicable to the case. The court used Article 363 Indonesia Criminal Code in card skimming case. In Indonesia criminal law proceeding, the court verdict based on the articles used in the indictment, which is based on investigation process, and judge are restrained by them. The review aims to determine the application of the law for similar case in the future and provide legal reasoning as reference for the law enforcement. The review uses statute and conceptual approach of normative legal study. The finding is the investigator since the beginning did not had adequate awareness of the skimming-related deterring norm in Law 11/2008, therefore binds the judge in law application. The law enforcement should use Law 11/2008 instead, to eradicate crime in securing information communication technology convergence regime.**

Keywords—court decision review; eradicate; fraud; skimming; verdict

I. INTRODUCTION

Skimming is a violation of confidentiality for someone's data and information. Sanusi explained further, it is specifically uses electronic data storage devices to read and record confidential data that is on magnetic stripe credit cards or debit cards, in some cases, connected to an ATM machine [1].

The skimming process is about transferring electronic documents/information from credit/debit cards to the perpetrator's computer, then proceed by utilizing the electronic data to create new credit/debit cards that resemble the victim's credit/debit card. Then, the perpetrator uses the cards as for their personal interests. There are also some criminals who sell electronic documents/electronic information that has been obtained from victims for personal advantages.

Skimming devices were first used in 2010 and became popular since then. Skimming investigations require a lot of technical know-how and time, often with little payoff. Some of these skimming operations are really extensive, essentially a modern form of organized crime [2]. With the substantial increase in bank acquiring transactions, debit/credit card frauds become ever more rampant. Backwardness in merchant's risk management is becoming one of the biggest obstacles for the development and profit generation of debit/credit card business [3]. Recent publicity around the world, including court cases, has raised questions about the safety of chip and PIN cards from fraudulent attack, for example by cloning [4]. It is very much the same as identity theft. Therefore, some of law enforcements in countries which have not familiar with information communication technology convergence regime identify the crime as theft.

A criminal case happened around 2010-2012, took place at Denpasar, Bali, Indonesia. The perpetrator used skimming method to steal data, generate debit and/or credit cards, and use them for illicit transactions. Denpasar District Court held the proceeding and the case verdict was used Indonesia Criminal Code, particularly of theft fellowship.

This paper reviews a court decision of a skimming case in Indonesia, looking what causes the judge using Criminal Code instead of Law 11/2008. Also looking on how the skimming methods are executed, how the law was implemented by the law enforcement, and what statute should be applied regarding the skimming methods, the concepts provided by scholars in using Law 11/2008 to eradicate skimming for the future reference in managing secure e-commerce.

II. METHODOLOGY

The review of in this article is a review for a case verdict by Denpasar District Court with case registration number 687/Pid.B/2012/PN.DPS. The case verdict applied Article 363 verse (1) 4 *jo.* Article 64 Indonesia Criminal Code and Article 3 *jo*. Article 2 verse (1) Law 8/2010 *jo.* Article 55 verse (1) 1 Indonesia Criminal Code. Article 363 verse (1) 4 Indonesia Criminal Code.

The correct law application determines legal certainty and eliminates disparity in justice enforcement. In ruling information communication technology regime, Indonesia had passed Law 11/2018. The statute has been important in deterring criminal offenses involving information communication technology.

The methods applied in this paper are normative legal study and case study based on the verdict, using statute and conceptual approach. The review involving literatures and statutes study and comparing them to the court's verdict toward

Copyright © 2019, the Authors. Published by Atlantis Press.
This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/).

the case, to find out correct legal reason in law application to eradicate skimming, which is a threat in holding a secure e-commerce transaction toward country development.

III. Results and Discussion

A. Key Concepts on Law 11/2008 Application to the Case

Suhariyanto quoting Alkatiry: Misuse of credit cards belonging to others on the internet is the largest cybercrime case related to the internet business world in Indonesia. Misuse of other people's credit cards is not complicated and can be done physically or online. Other people's names and credit cards obtained in various places (restaurants, hotels, or all places that make credit card payment transactions) are included in the purchase of goods on the internet [5].

Data collected from credit cards and debit cards are taken in several ways:

- By stealing credit cards. Perpetrators steal credit cards or obtain data related to an account, including credit card account numbers or other information needed by the credit card recipient (merchant) in a transaction;
- By embedding spyware parasites. These spyware parasites can perform identity theft and can trace credit card numbers when someone uses a credit card to shop. If the information coming from the credit card is taken by the perpetrator, the credit card holder can lose his money;
- A merchant shop officer copies the sale receipt from the item purchased by the customer with the aim of using it to commit a crime in the future;
- By skimming. Getting your personal data can be done with so-called "skimming". Skimming is the theft of information about a person who uses an electronic device called skimmer [4].

In identity related cybercrime there are four IDT (Identity Data Theft), ATO (Account Take Over), MTO (Merchant Take Over), and carding. Skimming is one of the IDT (Identity Theft Data). IDT considered as personal of others abuse, it includes skimming, that aims to use the identity data with the intention to commit fraud and or forgery [1]. The identity thief may open up a bank account or credit card account, take out a loan or acquire telephone and utility services, apply for social services, rent an apartment, buy a car, take out mortgage, etc. [4-7].

Skimming also can be considered as ATO (Account Take Over), because of the unauthorized usage of victim's account. The aim is to use and control someone's account illegally, or take over from a bank account [1]. In an account takeover, the criminal pretends to be lawfully card holder by using personally identifying data that was taken from stolen documents or media (such as that stored on the magnetic strip of an ATM card) and contacts the appropriate institution (the credit card issuer, for instance) to have the billing address changed. Then the thief reports the card as lost and requests that a replacement is mailed to the new address.

Skimming is a common method used to steal identities. Skimming devices are very small and can be easily hidden in a pocket, apron pouch, or under a counter. A card can be swiped through a skimmer, and all of the information on the magnetic strip, including the card's security code, is recorded and stored [6]. A skimmer could be some sort of merchant tool at the checkout cashier shaped like a matchbox or poker card box, placed hidden in the hotel cashier or shopping cashier. The numbers and PINs on credit or debit cards can be recorded or by the skimmer [1].

Skimming occurs when a device is placed over the card-reader (e.g. ATM Machine, card swipe tool). Skimming process duplicates the information embedded on the debit or credit card's magnetic strip. Some devices are more sophisticated included a camera or false panel to track the entry of the personal identification number (PIN) [7]. The perpetrators then retrieve their skimming device and encode the same magnetic strips onto an entirely brand new cards. Then the new cards will be used for fraudulent purchases as if the held the victim's physical cards themselves [7].

The purpose of skimming as described above are that the perpetrator uses the card skimming method to control someone's account or illegally take over the personal data of a person's credit card or debit card used for personal gain. After the perpetrator had successfully taken over someone's account illegally, and retrieved personal data on a person's credit card or debit card, the perpetrator commits a series of malicious actions which the final goals are damage a person's reputation and take the money in the cards account that had already taken over.

An organized use of the skimming schemes could result in the destabilization of the banks and the credit card industry being victimized. These schemes have already been attributed to the collapse of several businesses and were utilized to finance at least one terrorist attack (the Bali bombing). At a minimum the loss, which exceeds $10 billion a year in fraud and damage to computer networks, can being blamed for the rise of purchase prices to consumers and the rise of interest rates on credit cards [8].

Porkess & Mason explained there are four possible explanations of card fraud:

- A thief has stolen the money from the bank following a breach of the card's security conditions.
- The claimant is at fault. A thief has stolen the money without a breach of the card's security conditions. The bank is at fault.
- The claimant was responsible for the withdrawals and is making a dishonest claim. Clearly the claimant is at fault.
- The bank has made an error and so is at fault [4].

What is taken is the funds in the bank by using the customer's name unlawfully. In practice, it is the bank's money that is taken, and it is the bank's lost. Should this occurred, there will be dispute between bank customer as skimming victim with the bank. What the bank knows is the transaction

conducted by the customer, for the authorization of transaction is embedded to the customer.

Liu provided a risk profile of skimming. First, from the merchant size: The merchant size here is mainly reflected in two aspects: nature of the merchant company and operational floor area. Large merchants with standard management are comparatively safe, while the probabilities of fraud in smaller, newly established merchants are bigger. Whether the merchant has intention of fraud: Small, private merchants who sell antiques, ginseng & medicine etc. have bigger intention of fraud. Nature of operations: The probabilities of fraud at luxury consumption sites are bigger. Transaction time: The probabilities of fraud in non-business hours are bigger. Transaction amount: The probabilities of fraud in large, integral transaction amount are bigger. Transaction goods: The probabilities of fraud in goods that are small, high in price, and can easily turned into cash are bigger. Transaction frequency: The probabilities of fraud in frequent transactions in short period of time with large dollar value are bigger. Successive transactions on cards from different countries: The probabilities of fraud in successive transactions on cards from different countries in short period of time with large dollar value are bigger. Has failed transaction record: The probabilities of fraud in transactions on the same card after a certain transaction has failed [3].

General rule of theft is in Article 362 Indonesia Criminal Code. The qualifications are in Article 363 until Article 367. Before the existence of special rule (*lex specialis*), law enforcement used extensive interpretation of these article to be applied in case of theft related to information communication technology convergence.

The problem occurred in open codification system applied in country like Indonesia, is the law enforcement have to be aware of the existence of criminal law outside the criminal code.

What is considered as criminal act in the Law 11/2008 is defined in Article 27 to Article 35. As for the data theft, electronic information and/or electronic document theft, are ruled in Article 32 verse (2) of the Law 11/2008.

Article 32 verse (2) of Law 11/2008 states: "Any Person who knowingly and without authority or unlawfully in any manner whatsoever, moves or transfers Electronic Information and/or Electronic Documents to Electronic Systems of unauthorized Persons." The elements of Article 32 verse (2) described as follows:

- Any person;
- Knowingly:
- Without authority or unlawfully;
- In any manner whatsoever, moves or transfers Electronic Information and/or Electronic Documents;
- To Electronic Systems of unauthorized Persons;

Any person here refers to individual, whether an Indonesian citizen, a foreign citizen, or a legal entity listed in Article 1 paragraph 21 of the Law 11/2008. Knowingly is a proposition regarding the level of intention, which is in this context is deliberateness. The juridical consequence of this proposition existence, should other than deliberate action in this matter is not punishable.

Related to it, Prodjodikoro stated: Will theory is to consider deliberateness (*opzet*) exists if the actions and consequences of a crime are desired by the perpetrator. The shadow theory considers the act as deliberately conducted when the actor has a clear picture/imagination of the corresponding consequences will be achieved even from the commencement of the act, hence he adjusts his actions to the result [9].

It can be concluded that the theory of will means the perpetrator really desires to achieve the consequences which become the main reason of the criminal penalty, whereas the theory of shadow means that the perpetrator can only imagine the consequences that will occur, so that what the perpetrator really desires is the actions, not the consequences.

For 'unlawfully' concept here, there are two teachings that elaborate: *formele* and *materiele*. The *formele* teaching require a regulation or legislation violation. The nature of against the *formele* teaching is when an act fulfills all elements stated in the formulation of a criminal act, the act is a criminal act. This teaching adheres to the principle of legality as acts that are criminal charged in the written law. While the *materiele* teaching does not. The *materiele* teaching very much refers to appropriateness and decency. The nature of against the *materiele* teaching states that the nature of unlawfulness is not only stated in the law (written), but it must also be seen from the principles of the unwritten law. Unlawful nature can be eliminated based on the statutory provisions or unwritten law.

On the unlawful concept being prescript in the norm, Chazawi stated that: Any act set as prohibited by including it in the legislation (become a criminal act), regardless of whether the element of unlawfulness is included or not in the formulation, then the criminal act has the nature of against the law, in other word unlawfulness is an absolute element of criminal act. The 'unlawful' concept in this article co-prescript with the phrase of 'without authority'. Authority depict a lawful manner of a conduct, without authority giving a sense that there is an absence of lawful manner in an action. Authority is related to public law, that give legal basis for public official to do their duties within the corridor of the law. In this case, it is obvious that the perpetrators are not public officials, therefore it is not relevant to use this phrase. Instead, focused on the 'unlawful' is a better idea. Even more, the *materiele* concept of it provides broad possibility for the perpetrator to be sanctioned.

In this article, what is protected is personal data of the rightful owner and/or holder. Electronic information and/or electronic documents had to be used rightfully by the lawful owner or holder. Moving itself means placing it to another place. Transfer is an act of moving something to another place or someone to another person. According to Sitompul: "Such movement or transfer doesn't have to make the Electronic Information or Electronic Documents no longer in place." [10]. Can be concluded that as long as there is a new placement of information or electronic document, there is transfer. If the movement or transfer is done by sending data by e-mail or

transferring data using USB drive, it can be subject to the provisions of Article 32 verse (2), because of the existence of phrase 'in any manner whatsoever'.

The final element of Article 32 Verse (2) to electronic systems of unauthorized persons, Sitompul explains that, "The element of to electronic systems of unauthorized persons is that the recipient has no right to receive electronic information and/or electronic documents sent or given by the sender." [10].

For cybercrime facilitators related is regulated in Article 34. Article 34 verse (1) of Law 11/2008: "Any Person who knowingly and without authority or unlawfully produces, sells, causes to be used, imports, distributes, provides, or owns: a. Computer hardware or software that is designed or specifically developed to facilitate acts as intended by Article 27 to Article 33.

The elements in Article 34 verse (1) a can be described as follows:

- Any person;
- Knowingly:
- Without authority or unlawfully;
- Produces, sells, causes to be used, imports, distributes, provides, or owns Computer hardware or software that is designed or specifically developed to facilitate acts as intended in Article 27 to Article 33.

Some of the elements in this article is very much the same as Article 32 verse (2). The difference is at the operative words. The next elements are 'produces, sells, causes to be used, imports, distributes, provides, or owns computer hardware or software that is designed or specifically developed to facilitate acts as intended in Article 27 to Article 33'. Of this phrases explained by Chazawi and Ferdian [11]:

- Produce, literally is an act in any way to have an item (product) made or manufactured or create an item to come into existence. The act of producing will be completed when the goods (products) have been produced or issued.
- Sell, is one of the legal acts of buying and selling. While on the other hand there is an act of buying. Legal action (legal engagement) of buying and selling is an agreement between two parties, where one - the seller binds himself to hand a material, and the other party - the buyer pays the promised price. The act of selling is completed if the sell and purchase are done. In other word there is a buyer who already purchased the material.
- Causes to be used, means causing/creating goods for own use. It is explained that the act in any form and method that makes an object that previously did not exist becomes exist, and the object is intentionally created, specifically designed to facilitate the acts referred in Article 27 to Article 33.
- Import means the entry of goods from abroad into the country. Importing is an act in any way to object that in this case is hardware or software that was originally outside the jurisdiction of Indonesia. If at the beginning the producer/causer/creator has own it outside the Republic of Indonesia jurisdiction, the act of import occurs right after the producer/causer/creator brings the goods into the territory of Indonesian law jurisdiction.
- Distribute, means to share or send something to several places. So, what is meant by distribute here is to share or give or send computer hardware or computer software to several people or to several places. The act of distributing is completed when the object of a criminal act that in this case is computer hardware or computer software has been distributed/given and received or in the possession of several people or in several places.
- Provide, means it is ready to, exist or already exist. Providing is an act in any way to an object by placing the object in such a way so that it is available to be used at any time. Before the act of providing is completed, computer hardware or software items are not available yet. With any way and form of they become available, ready for use at any time. Criminal act of providing computer hardware or software is done when these items become available, without them being used for a purpose. For that is the meaning of provide, to have not done any deeds to the provided object.
- Have, has the meaning of owning property rights over an object in this case is computer hardware or computer software, whether the object is in the power of the maker or other people. The measure of having does not have to be solely based on property rights according to law (civil), it can be in the form of a right to enjoy the use of something freely and to be free to do anything with it with full sovereignty. It is also not merely a right that the ownership must be formally proven with certain formal letters. But the fact that the hardware or software is in power and or is used by the maker freely is enough. Like a man using his own goods.

The seven elements mentioned above are forms of action that are only intended for two objects, they are computer hardware and software. The intention of the perpetrator must be aimed at the existence of objects that are specifically designed or developed to facilitate the act of Article 27 to Article 33. Computer hardware and software are the two objects in an integral manner, inseparable entity that works in electronic systems. The electronic system itself as described in Article 1 paragraph 5 of the Law 11/2008 is "A series of electronic devices and procedures that function to prepare, collect, process, analyze, store, display, announce, transmit, and/or distribute Electronic Information."

B. Court Decision Review

Since December 2010, FT recruited the cashiers from certain mall and restaurant in Kuta Bali area, ZA and IP, which is the coffee shop cashier and FT ordered the cashiers/employees to open Microsoft Word or NotePad if the consumer is paying using Debit/Credit Card then the card is swiped back to Barcode Magnetic Reader machine then

magnetic data will appear in Microsoft Word file or Notepad. If at the cash register computer there is no Barcode Magnetic Reader, then FT trained ZA and IP to use Skimmer (Card Device model MINI DX3). The victim only need to swipe their card and skimmer will record every data from the debit card. This is electronic information theft, particularly identity, for the electronic information embedded personally to card account holder.

FT ordered ZA and IP to peek and memorize the customer's PIN number when the customer is paying using card. The file containing PIN and the electronic information of the cards saved as Microsoft Word files and also stored them in USB disc and then the data was sent to FT.

FT obtained the data from ZA and IP from August 2011 until March 30, 2012. The amount of data taken by FT approximately 150 (one hundred fifty) data. The data was given to FT by SMS, by 4G USB drive that belongs to FT, and also received the data via e-mail. FT later sold those data to R, and some are used to made Debit cards and Credit cards by FT.

The process of debit and credit cards making was firstly, FT installed the 206 U Magnetic Stick Reader (MSR) Software in the FT's Laptop, then FT opened the software of Magnetic Strip Reader, then the data in numbers and symbols that FT derives from ZA and IP inserted into the program. Then FT used the program to write data then swiped the existing magnetic card so that the data will transferred to magnetic card by swiping it, then the card can be used to perform financial transactions such as Debit card or Credit card original owned by the customer. This is an identity theft, particularly account take over (ATO).

That is why it is partially reasonable for Denpasar District Court applied Article 363 verse (1) 4 Indonesia Criminal Code, for before the enactment of Law 11/2008, law enforcement used interpretation to apply the Criminal Code to deter criminal offenses related to information communication technology. Article 363 verse (1) 4 Indonesia Criminal Code is of theft involving more than 1 person as the perpetrators, as the skimming involved 3 persons as perpetrator.

Article 64 Indonesia Criminal Code is of more than one and continuous criminal actions. It also applied because FT conducted more than one offense, and they could be considered as one continuous act. It is important, for the penal *steles* is different as if the offense is only one very act.

Article 3 *jo*. Article 2 verse (1) Law 8/2010 applied for the offenses involving money laundering. The illicit profit they got from skimming, the perpetrator put into financial system. The motive is not necessarily to launder the money, distribution and/or transfer is also punishable.

Article 55 verse (1) 1 Indonesia Criminal Code is of more than one involving actors. Article 363 verse (1) 4 does not need this norm, for itself already ruled of more than one perpetrator. This article is for Law 8/2010.

Examining the articles applied in this case are not necessarily wrong, but it is obviously inaccurate, and they are inconsiderate the existence of special rule. For, Indonesia had had Law 11/2008 already, which is applicable to the case.

In Indonesia, the law application by judge is restrained by prosecutor's indictment. The prosecutor's indictment is based on the findings in investigation process. There is no possibility for the judge to use other law than what is indicted. Therefore, the shortage of law that applied for a case are sometimes occurred, and the judge proceed the trial and decide using Article 363 verse (1) 4 *jo.* Article 64 Indonesia Criminal Code and Article 3 *jo*. Article 2 verse (1) Law 8/2010 *jo*. Article 55 verse (1) 1 Indonesia Criminal Code. While, there is special rule in Law 11/2008 can be applied for the particular case, since the *tempus delicti* is 2010.

FT is the intellectual actor of the crime of unlawful transfer of information electronic to unauthorized person/party. The initial idea and the orders toward ZA and IP are from FT. Criminal sanction in violation of the provision of Article 32 verse (2) of Law 11/2008 is set forth in Article 48 verse (2) which stipulates: "Any Person who fulfills the elements as referred to in Article 32 verse (2) shall be sentenced to imprisonment at most 9 (nine) years and/or a maximum fine of Rp. 3,000,000,000.00 (three billion rupiah)."

It is also obvious that FT facilitate ZA and IP with skimmer device. That is why Article 34 verse (1) a *jo*. Article 50 can be imposed. In this particular, FT provides, or owns Computer hardware or software that is designed or specifically developed to facilitate acts as intended by Article 32 verse (2).

According to Chazawi and Ferdian, "The criminal act in Article 34 verse (1) a shall be deemed as completed when only the prohibited acts are done. The proof can be seen at the logic of the act along with the tools or media and the way of doing it." [11]. Criminal sanctions if someone violate the provisions of Article 34 verse (1) a of the Law 11/2008, which is stated in Article 50 which determines: "Everyone who fulfills the elements referred to in Article 34 verse (1) a shall be imprisoned with a maximum imprisonment of 10 (ten) years and/or a maximum fine of Rp. 10,000,000,000.00 (ten billion)." It is understandably the sanction in Law 11/2018 as special rule is more severe.

IV. CONCLUSION

The case verdict based on the articles used in the indictment, and judge are restrained by them. Since the *tempus delicti* is 2010, the law enforcement should use Law 11/2008, particularly Article 32 verse (2) *jo.* Article 48 verse (2) and Article 34 verse (1) a *jo*. Article 50. The failure of Law 11/2008 application is not necessarily on the judge, since the investigation process those laws had not been used for the case. For future reference, skimming case similar to the case reviewed, those articles mentioned can be applied.

REFERENCES

[1] A. Sanusi, Cyber Crime. Jakarta: Milestone, 2011.

[2] J.G. Lee and G.G. Scott, Preventing Credit Card Fraud: A Complete Guide for Everyone From Merchants to Consumers. New York: Rowman & Littlefield, 2017.

[3] T. Liu and S. Liu, "Fraud detection model & application for credit card acquiring business based on data mining technology," Adv. Comput. Sci. Res., vol. 50, 2016.

[4] R. Porkess and S. Mason, "Looking at debit and credit card fraud," Teach. Stat., vol. 34, no. 3, pp. 87–91, 2012.

[5] B. Suhariyanto, Tindak Pidana Teknologi Informasi (Cybercrime). Jakarta: Raja Grafindo Persada, 2012.

[6] S.K. Hoffman and T.G. Mcginley, Identity Theft, vol. 134, no. 4. California: Greenwood Publishing Group, 2010.

[7] J. Waters, "ATM Skimming: How to Spot, Avoid," 2010. [Online]. Retrieved from https://www.wsj.com/articles/SB10001424052748704442404575542652417958106.

[8] S.E.J. Hilbert, "Hacking for Profit: Credit Card Fraud A Beginners Guide," 2004.

[9] W. Prodjodikoro, Asas-asas Hukum Pidana di Indonesia. Bandung: Refika Aditama, 2003.

[10] J. Sitompul, Cyberspace, Cybercrimes, Cyberlaw. Jakarta: Tatanusa, 2014.

[11] A. Chazawi and A. Ferdian, Tindak Pidana Informasi & Transaksi Elektronik (Penyerangan Terhadap Kepentingan Hukum Pemanfaatan Teknologi Informasi dan Transaksi Elektronik). Malang: Media Nusa Creative, 2015.