Jurnal Notariil

Jurnal Notariil, Vol. 6, No. 2, Nopember 2021, 106-111 P ISSN 2540 - 797X
Available Online at https://ejournal.warmadewa.ac.id/index.php/notariil E ISSN 2615 - 1545

EFFORTS TO OVERCOME CRIMINAL ACTS OF SKIMMING COMMITTED THROUGH ATMS IN THE PERSPECTIVE OF LAW NUMBER 19 OF 2016 CONCERNING EIT

Putu Eka Trisna Dewi[1]* and Ni Made Septiwidiantari[2]
[1]Lecturer at Graduate School of Law, Postgraduate Program, Universitas Ngurah Rai, Denpasar-Indonesia
[2]Sub-Directorate General V of Cyber, Special Crime Investigation of Polda Bali, Indonesia
Email: trisnadewi.ecak@gmail.com[1]* and septiwidiantari97@gmail.com[2]

How To Cite:
Dewi, P. E. T., & Septiwidiantari, N. M. (2021), Efforts to Overcome Criminal Acts of Skimming Committed through ATMs in the Perspective of Law Number 19 of 2016 concerning EIT, *Jurnal Notariil*, 6(2), 106-111. Doi: https://doi.org/10.22225/jn.6.2.2021.106-111

Abstract

Cybercrime is one form of the negative impact of the development of science and technology. One of the crimes in the form of Cybercrime, which in recent years has greatly disturbed the public, is skimming. Skimming crimes continue to increase and are unsettling the community. For this reason, serious efforts to overcome them are required. This study aims to examine the effort to overcome criminal acts of skimming committed through ATMs in the Perspective of Law Number 19 of 2016 concerning EIT. This study is legal research with a literature study. The research approaches used are the statute approach and the fact-based approach. The results of this study revealed that as an effort to tackle skimming crime, there are two ways that can be applied, namely preventive action (preventing crime from occurring) and repressive action (efforts taken after a crime has occurred). The repressive measures that can be taken in tackling the crime of skimming are to apply legal provisions in accordance with Article 30 in conjunction with Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning EIT.

Keywords: ATM; Preventive Measures; Repressive Measures; Skimming

1. INTRODUCTION

Cybercrime is a form of crime that occurs via the internet or cyberspace (Erdiansyah, 2007). It is a type of crime associated with the unlimited use of information technology and has strong characteristics with an engineering technology that relies on a high level of security and credibility of information submitted and accessed by internet users. Based on this fact, it can be put forward that the coverage areas of cybercrime include piracy, fraud, theft, pornography, harassment, slander, and forgery. One of the Cybercrime crimes having been very troubling for the public in recent years is skimming (Maskun, 2013).

Skimming is the activity of illegally duplicating information contained in a magnetic stripe found on a credit or ATM/ debit card with a device known as a skimmer (Setiawan, 2019). With a skimmer, the cybercriminals of skimming duplicate the magnetic stripe data on the ATM card into an unused ATM card. This process can be performed manually; such as the perpetrator returning to the ATM to retrieve a pre-prepared data chip and, when using a more sophisticated skimmer, the collected data can be accessed from anywhere wirelessly. Skimmers are not the only tool used by skimming criminals, they also use surveillance cameras to detect the finger movements of ATM card users when entering their ATM card PIN (Personal Identification Number) (Wahid & Labib, 2005).

In Indonesia, criminals of skimming can be charged with Articles 30, 32, 33 of

the Electronic Information and Transactions Law (hereinafter is referred to as EIT Law), Number 11 of 2008 in conjunction with Law Number 19 of 2016. Article 30 of the EIT Law reads:

Any person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems of other Persons in any manner whatsoever.

Any person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever with the intent to obtain Electronic Information and/or Electronic Documents.

Any person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever by breaching, hacking into, trespassing into, or breaking through security systems.

Article 32 of the EIT Law reads:

Any person who knowingly and without authority or unlawfully in any manner whatsoever alters, adds, reduces, transmits, tampers with, deletes, moves, hides Electronic Information and/or Electronic Documents of other Persons or of the public.

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.

Acts, as intended in paragraph (1), shall be acts that result in any confidential Electronic Information and/or Electronic Document being compromised such that the data becomes accessible to the public in its entirety in an improper manner.

Article 33 of the EIT Law reads "Any Person who knowingly and without authority or unlawfully commits any act resulting in faults on Electronic Systems and/or resulting in Electronic Systems working improperly". Article 30 (3) in conjunction with Article 46 (3) of the EIT Law reads:

Any person who knowingly and without authority or unlawfully accesses Computers and/or Electronic Systems in any manner whatsoever by breaching, hacking into, trespassing into, or breaking through security systems *(cracking, hacking, illegal access)*". Regarding criminal threats against perpetrators, it is regulated in Article 46 Paragraph (3), which reads: "Any person who satisfies the elements as intended by Article 30 paragraph (3) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding IDR. 800,000,000 (eight hundred million rupiah).

Skimming crimes that occur through ATMs have made people worry and feel anxious every time they make transactions using ATMs. The number of the cases of criminal acts of skimming is presented in Table 1 below.

Table 1
Criminal Acts of Skimming from 2018 to 2020

No	Year of Occurrence	Number of Cases
1	2018	4
2	2019	5
3	2020	13

Source: Sub-directorate General V (Cyber), Special Crime Investigation, Polda Bali

Table 1 shows that from 2018 to 2020, there were 22 criminal acts of skimming that occurred through ATMs, especially at BNI (Bank Negara Indonesia) ATMs, as shown in Table 2 below.

Table 2
Criminal Acts of Skimming Occurred at BNI ATMs

No	Date	Location
1	21 December 2018	BNI ATM at Restaurant Shinning Jewel, Jalan Danau Tamblingan, Denpasar
2	17 February 2020	BNI ATM at Pasar Baru Ubud, Jalan Raya Monkey Forest Ubud, Gianyar
3	3 March 2020	BNI ATM at Agung Cottage, Jalan Raya Legian Nomor 95 Kuta, Badung
4	5 June 2020	BNI ATM at Apotik Dian farma, having its address at Jalan Toyaning No. 8 Kedonganan, Kuta selatan, Badung

Source: Sub-directorate General V (Cyber), Special Crime Investigation, Polda Bali

A study about criminal acts of skimming has previously been conducted by some researchers. Ekawati (2018) in her study examined banking crimes that use the

skimming method and about legal protection for customers who are victims of skimming crime. The result of her study showed that crime skimming is an old mode of customer money burglary which is done by stealing customer data at the customer's ATM with skimmer techniques. Legal protection against customers who are harmed due to the crime of skimming can be carried out by criminal means, namely reporting to the police and the police's duty to arrest the perpetrators. Legal protection is given through civil law by way of the bank replacing the customer's money after clarifying the transaction against the customer's account. A study conducted by Setiawan (2019) also examined a similar study with this present study. Setiawan (2019) examined the development of modus operandi crime skimming in the case of bank burglary bank as a form of cybercrime (cybercrime) and efforts/legal steps in tackling crime use of information systems and electronic transactions. The results revealed that the modus operandi of criminal skimming in ATM bankruptcy as a form of cybercrime and the application of article in Law Number 11 Year 2008 regarding Information and Electronic Transaction as an effort/step in tackling the crime of Information System Use and Electronic Transactions. In addition, Natalia et al. (2020) also have previously conducted a similar study that uncovered the causes of the crime of burglary using skimming techniques based on Law No. 19 of 2016 and the criminal responsibility of the perpetrators of criminal acts of ATM burglary using skimming techniques based on Law no. 19 of 2016. The results indicated that the cause of the crime of burglary using skimming techniques is the negligence of the owner of the ATM card. In the crime of skimming ATM burglary, unawarely the victim usually has been video recorded when inserting the ATM pin and the magnetic tape has been recorded through a special device. In the results of this study, it was also stated that the crime of burglary with ATM machines using skimming techniques could be charged under Article 30 of the ITE Law, so that police officers have a legal basis to take action to investigate ATM card crimes and other electronic transactions.

The rise of skimming cases having occurred appears to be the motivating factor to this study to be done. Thus, based on the background and the previous studies provided above, this study aims to examine the effort to overcome criminal acts of skimming committed through ATMs in the Perspective of Law Number 19 of 2016 concerning EIT so that people no longer feel hesitant in using ATM facilities provided by the bank.

2. METHODS

This research is legal research with a literature study. According to Muhammad Nazir, a literature study is a technique of collecting data by conducting a review study of books, literature, notes and reports related to the problem being solved (Nazir, 2009:27). In addition, the research approaches used are the statute approach and the fact-based approach (Soekanto, 2007:140). The statute approach is intended to understand and comprehensively analyze the hierarchy of laws and regulations and the principles in-laws and regulations. It is applied by reviewing all laws and regulations having a relationship with the legal issues being handled (Marzuki, 2010:133). A fact-based approach is an approach that is used to find out the actual situation that occurs in the field.

3. RESULT AND DISCUSSION

Based on the objective of this study, this part discussed the effort to overcome criminal acts of skimming committed through ATMs. Skimming is an activity of illegally duplicating the information contained in the magnetic stripe found on credit or ATM/debit cards. This implies that skimming takes the form of an activity related to the perpetrator's attempt to illegally steal data from the magnetic tape of an ATM/debit card in order to have control over the account of the target victim. The user's ATM card burglary through skimming techniques was first identified in 2009 at a Citibank ATM, Woodland Hills, California. At that time, it was known that the skimming technique was carried out by using a device attached to an ATM machine slot (where to insert an ATM card) with a device known as a skimmer. A skimmer refers to a device for breaking into customer data that is installed in the mouth of an ATM. The tool will copy the data of the ATM card users when they insert the ATM card through the skimmer. With that, the perpetrator having put the skimmer in the hole where the ATM card is inserted will have control over the data of the ATM card owner. "The modus operandi is to copy user data from the magnetic stripe on the ATM card. The magnetic stripe is a wide black stripe on the back of an ATM card (Alfitra, 2014).

In 2018, there were 4 cases of skimming crimes. Then, in 2019 the number of cases increased to 5 cases and in 2020 it increased 2-fold to more than 13 cases. The criminal acts of skimming through ATMs, specifically at BNI ATM on December 21, 2018, occurred in the area of Restaurant Shinning Jewel at Jalan Danau Tamblingan, Denpasar. In March 2020, two cases occurred, namely at the BNI ATM at Agung Cottage, which is at Jalan Raya Legian, Number 95 Kuta, Badung and at the BNI ATM in Pasar Baru Ubud, at Jalan Raya Monkey Forest, Ubud, Gianyar. The same case also occurred at a BNI ATM at Jalan Raya Tegalalang, Gianyar, namely in April 2020. In June 2020, a similar case also occurred at a BNI ATM at Dian Farma Pharmacy, which is located at Jalan Toyaning No. 8, Kedonganan, South Kuta, Badung.

The occurrence of ATM burglary is inseparable from the negligence of the ATM cardholder itself. In the cases of criminal acts of breaking into ATMs by skimming, the victim usually has unknowingly been recorded with a video recorder when entering the ATM PIN and magnetic tape has also been recorded through a special device. Every ATM user is advised to keep their PIN confidential so they will not become victims of ATM burglary. In an effort to tackle skimming crime, there are two methods commonly used, namely preventive action (preventing crime from happening) and repressive action (efforts made after a crime has occurred).

Preventive actions refer to actions taken to avoid or prevent the possibility of a crime from occurring. For this reason, Bank Negara Indonesia (BNI) takes preventive actions by providing education to customers that are delivered directly or face to face when customers make transactions at the bank concerned. The procedures include:

Every user is advised to protect the confidentiality of the PIN of their ATM card by covering it with their hand before entering the PIN and then entering the PIN.

Each user is educated to pay close attention to the physical condition of the ATM card and its surroundings. Customers are expected to act actively to immediately report to the authorities if they find suspicious conditions.

When making transactions using ATM/ Debit cards in collaboration with banks, each user is expected to pay attention to the condition of the Electronic Data Capture (EDC) at each of these merchants. If there are suspicious devices attached to the EDC or other suspicious things, every customer is advised not to proceed with transactions but immediately report to the nearest bank or to the authorities.

According to Simanjuntak and Chairil Ali, preventive measures that can be taken in tackling skimming crimes are: first, before using an ATM, users are advised to thoroughly observe the condition of the ATM first, from the keyboard to the hole where the ATM card is inserted. If any part is suspicious or looks damaged, the user is advised to leave the ATM machine and contact the bank concerned. Second, each user is advised to only transact at ATMs that have surveillance cameras installed by the bank. Third, users are advised to transact at ATMs crowded by many people, such as ATMs located in front of the bank or the one supervised by security. Fourth, when entering the PIN, users are educated to always cover the PIN typing board with their hands or lean close to the ATM card PIN typing board. Fifth, users are advised to always activate SMS/e-mail banking on their cellphones and check their bank account balances regularly. If there is an unknown reduction in the balance, the user must immediately report to the bank. If there is a debit transaction in the customer's account that is not carried out by the owner, the owner is encouraged to contact the bank to report the suspicious transaction and to immediately block the ATM card and delete all e-banking data at which the ATM card is registered (Simanjuntak & Ali, 1980:399).

The second method, which can be implemented to overcome the crime of skimming, is to apply repressive measures. This action refers to all actions taken by law enforcement officials after the occurrence of a criminal act. Repressive measures are more focused on individuals who commit criminal acts, namely by imposing appropriate sanctions (criminals) for their misconducts (Soejono, 1976:32).

Like the case occurring at the ATM of BNI at Dian Farma Pharmacy on Jalan Toyaning No. 8 Kedonganan, South Kuta – Badung, the perpetrators of skimming crimes installed a surveillance camera on the ATM machine to record all activities each customer does during transactions so that the perpetrators could obtain information of the ATM card PIN for all customers who have used the ATM.

Perpetrator of skimming crimes is charged with Article 30 in conjunction with Article 46 of Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 concerning EIT.

Article 30 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning EIT states that:

Any Person who knowingly and without authorities or against the law accesses a Computer and/or Electronic System belonging to other Persons in any manner whatsoever.

Any Person who knowingly and without authorities or against the law accesses a Computer and/or Electronic System in any manner whatsoever with the aim of obtaining Electronic Information and/or Electronic Documents.

Any Person who knowingly and without authorities or against the law accesses a Computer and/or Electronic System in any manner whatsoever by violating, cracking, transgressing, or breaking into the security system.

Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning EIT states:

Any person who satisfies the elements as intended by Article 30 paragraph (1) shall be sentenced to imprisonment not exceeding 6 (six) years and/or a fine not exceeding IDR. 600,000,000 (six hundred million rupiah).

Any person who satisfies the elements as intended by Article 30 paragraph (2) shall be sentenced to imprisonment not exceeding 7 (seven) years and/or a fine not exceeding IDR. 700,000,000 (seven hundred million rupiahs).

Any person who satisfies the elements as intended by Article 30 paragraph (3) shall be sentenced to imprisonment not exceeding 8 (eight) years and/or a fine not exceeding IDR. 800,000,000 (eight hundred million rupiah).

4. CONCLUSION

Based on the results of research that has been conducted on cases occurring at BNI ATMs, it can be concluded that the efforts made to overcome skimming crimes are preventive and repressive measures. The preventive measures that can be taken in tackling skimming crimes are: first, before using an ATM, users are advised to thoroughly observe the condition of the ATM first, from the keyboard to the hole where the ATM card is inserted. If any part is suspicious or looks damaged, the user is advised to leave the ATM machine and contact the bank concerned. Second, each user is advised to only transact at ATMs that have surveillance cameras installed by the bank. Third, users are advised to transact at ATMs crowded by many people, such as ATMs located in front of the bank or the one supervised by security. Fourth, when entering the PIN, users are educated to always cover the PIN typing board with their hands or lean close to the ATM card PIN typing board. Fifth, users are advised to always activate SMS/e-mail banking on their cellphones and check their bank account balances regularly. Meanwhile, the repressive measures that can be taken in tackling the crime of skimming are to apply legal provisions in accordance with Article 30 in conjunction with Article 46 of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning EIT.

REFERENCES

Alfitra. (2014). *Modus Operandi Pidana Khusus Di Luar KUHP: Korupsi, Money Laundering, & Trafficking* (Andriansyah, Ed.). Jakarta: Raih Asa Sukses.

Ekawati, D. (2018). Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan. *UNES Law Review*, *1*(2), 157–171. https://doi.org/10.31933/law.v1i2.24

Erdiansyah. (2007). *Pengaturan Cyber Crime Dalam Hukum Pidana Indonesia*. Universitas Islam Indonesia.

Marzuki, P. M. (2010). *Penelitian Hukum*. Jakarta: Kencana Predana Media Group.

Maskun. (2013). *Kejahatan Siber (Cyber Crime): Suatu Pengantar*. Jakarta: Kencana Prenada Media Group.

Natalia, C. D., Dewi, A. . S. L., & Widyantara, I. M. M. (2020). Sanksi Pidana terhadap Warga Negara Asing yang Melakukan Tindakan Pembobolan Anjungan Tunai Mandiri (Atm) dengan Teknik Skimming. *Jurnal Preferensi Hukum*, *1*(2), 37–41. https://doi.org/10.22225/jph.1.2.2340.37-41

Nazir, M. (2009). *Metode Penelitian*. Jakarta: Ghalia Indonesia.

Setiawan, D. A. (2019). Perkembangan Modus Operandi Kejahatan Skimming Dalam Pembobolan Mesin ATM Bank Sebagai Bentuk Kejahatan Dunia Maya (Cybercrime). *Era Hukum - Jurnal Ilmiah Ilmu Hukum*, *16*(2). https://doi.org/10.24912/erahukum.v16i2.4526

Simanjuntak, B., & Ali, K. (1980). *Cakrawala Baru Kriminologi (Suatu Konsep Dialog)*. Bandung: Tarsito.

Soejono, D. (1976). *Penanggulangan Kejahatan (Crime Prevention)*. Bandung:

Alumni.
Soekanto, S. (2007). *Pengantar Penelitian Hukum*. Jakarta: Universitas Indonesia Press.
Wahid, A., & Labib, M. (2005). *Kejahatan Mayantara (Cyber Crime)*. Bandung: PT Refika Aditama.
Undang-Undang Nomor 1 Tahun 1946 *jo* Undang-Undang Nomor 73 Tahun 1958 tentang Kitab Undang-Undang Hukum Pidana (KUHP).
Undang-Undang Nomor 11 Tahun 2008 *jo* Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (EIT). Lembar Negara Republik Indonesia, No. 251 tahun 2016.