JURNAL MAGISTER HUKUM UDAYANA
(UDAYANA MASTER LAW JOURNAL)
Vol. 11 No. 1 May 2022
E-ISSN: 2502-3101 P-ISSN: 2302-528x
http: //ojs.unud.ac.id/index.php/jmhu

Law Enforcement in The Process of Investigation on The Crime of Skimming by Foreign Nationals

I Made Wahyu Chandra Satriana[1], Ni Made Liana Dewi[2]

[1]Faculty of law, Dwijendra University, E-mail: wahana.chandra@gmail.com
[2]Faculty of Law, Dwijendra University, E-mail: wahanadewi80@gmail.com

Info Article
Received: 21st July 2021
Accepted: 10th May 2022
Published: 12th May 2022

Keywords:
Investigation; Criminalact; Skimmin

Corresponding Author:
I Made Wahyu Chandra Satriana,
E-mail: wahana.chandra@gmail.com

DOI:
10.24843/JMHU.2022.v11.i01.p02

Abstract
This study aims to analyze the law enforcement process at the level of investigation of skimming crimes by foreign nationals in the jurisdiction of the Bali Police; and Factors that support and hinder the law enforcement process at the investigation level of skimming crimes by foreign nationals in the jurisdiction of the Bali Regional Police. The research method used is a empirical legal research. The results showed that law enforcement process at the level of investigation of skimming crimes by foreign nationals in the Bali Regional Police jurisdiction was carried out based on Perkap No. 6 of 2019 which includes receiving police reports, making investigative administrations, examining victims and witnesses, collecting evidence and conducting case titles that end in the examination process in court; and factors that support and hinder the law enforcement process at the level of investigation of skimming crimes by foreign nationals in the Bali Regional Police jurisdiction, including (a) supporting factors which include their own legal (act factors) and public factors; (b) inhibiting factors include legal themselves (statutory factors), law enforcement, and facilities that support law enforcement, community and legal culture factors.

1. Introduction

The development of the modern world today has brought the banking sector as a financial institution that always strives to provide excellent service to its customers by utilizing modern technology. As one of the institutions that deal with financial problems, banking basically has a financial intermediary function that is owned by the community (financial intermediary), both as a fundraiser and as a distributor of funds owned by the community which is the lifeblood of the financial sector whose main focus is very important.[1] One of the uses of technological sophistication in the banking world as a progressive action taken by banks in increasing the reach of networks and the development of the marketing world which has begun to shift from the use of physical buildings as offices or branches, has now shifted to the use of electronic transactions (e-banking). Through Automated Teller Machines (hereinafter referred to as ATM), cellular phones (phone banking) and internet networks (internet banking) in

[1] Imron Anwari, "Penerapan Hukum Pidana Kini Dan Masa Mendatang" (Genta Publishing, Yogyakarta, 2014). p. 83.

conducting financial transactions.[2] The presence of internet technology is an unavoidable need to support national development. The use of internet network technology in people's lives which is very well known and is used at any time in a financial transaction is an ATM with a security network in the form of certain codes known as Personal Identification Number (hereinafter referred to as PIN) owned by the customer of the bank concerned.[3]

An ATM card is a card that is owned by every customer who opens a new account at a bank to make it easier for customers to carry out transactions. There are several banking transactions that can be done using an ATM card, namely withdrawing or depositing money, and now it is equipped with an auto debit facility with the aim of making it easier for customers to shop at minimarkets; supermarkets; outlets that have electronic data capture (EDC) machines. EDC is a machine used for shopping without using cash. The use of ATM cards is actually an attempt by the government to limit people from always using cash in shopping and transactions. The use of this ATM card is intended to provide practical services and ensure security.[4] One of the technological products issued by banks in the form of an ATM card, equipped with various technological sophistication and security systems in it is expected to provide continuous service to customers without holidays or time lags in one day, but in practice there are still shortcomings.[5] The existence of deficiencies contained in this ATM card has an impact on the losses experienced by customers. There are customers who are surprised by the fact that the value of the balance in their bank account has decreased, without knowing and realizing when, where and who made the transaction, because to the knowledge of the customer concerned he never felt that he had made the transaction shown in the print out of savings book. Loss of customer funds that occurs in ATM is something that has a negative impact on the development of internet, especially banking technology.

The progress of a human civilization which is indicated by the progress of science and technology, immediately brings progress to certain crimes that are relatively new which are complex in nature with various types of actions that are diverse and relatively new.[6] One of the negative forms of technological progress, one of which is the existence of a crime called cyber crime. The progress of the types of crimes that follow the advancement of technology has an influence on legal changes, whether we like it or not, it must be updated according to the times, especially in the process of proving in court, one of which concerns the use of electronic evidence in the proof process. The presence of Law Number 11 of 2008 concerning Information and Electronic Transactions and has been updated with Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Electronic

[2] Nazarudin Tianotak, "Urgensi Cyberlaw Di Indonesia Dalam Rangka Penangan Cybercrime Disektor Perbanka," *Jurnal Sasi* 17, no. 4 (2011). p. 21.
[3] Roni Sambiangga, "Sistem Keamanan ATM (Automated Teller Machine/Anjungan Tunai Mandiri)," *Teknik Informatika Sekolah Teknik Elektro Dan Informatika Institut Teknologi Bandung*, 2014, 1–10. p. 36.
[4] Ade Arthesa and Edia Handiman, "Bank Dan Lembaga Keuangan Bukan Bank," *Jakarta, PT Indeks Kelompok Gramedia*, 2006. p. 258-259.
[5] Dr Kasmir, "Dasar-Dasar Perbankan Edisi Revisi 2014," *Jakarta: Rajawaloi Pers*, 2015. p. 182.
[6] Abdul Wahid, "Kejahatan Mayantara (Cyber Crime)," 2005. p. 33-36.

Transactions (hereinafter referred to as UU ITE), is a positive response from the government to respond to changing times in the era of digitalization as it is today.

Rapid progress in the field of information technology and the internet today has an impact on banking services to its customers. Banking is expected to provide the best services, such as: security in transactions, ease in service and effectiveness in providing various facilities needed by customers by utilizing electronic banking media (e-banking).

The existence of facilities provided by banks such as electronic banking, will greatly facilitate their customers to carry out various banking activities such as checking savings balances, purchasing credit, paying electricity, Regional Water Company, purchasing internet quotas, transfers between banks, transactions using internet technology and so on. With this electronic banking, consciously making human life more practical and efficient. Various activities related to finance, especially transactions in the banking world that are connected to the internet network can be easily accessed anywhere at any time without being constrained by distance, time and place. Each customer can carry out various transaction activities and get the desired banking facility services by using a laptop or mobile phone connected through the internet network without going to the bank. These various banking activities and transactions can be done anywhere and anytime without worrying about it being late at night or on holidays.

Technological advances in providing banking facilities that are most often and commonly used are ATM. Customers can conventionally use their machines and ATM cards to withdraw money or save according to their wishes and needs. Customers do not need to come to the bank, fill out forms and enter the queue to do this, but all they need is to come to ATM machines scattered in minimarkets, gas stations or ATM outlets on the side of the road to make transactions using their ATM cards. With this technological sophistication, it gives rise to sophistication in crime, such as card skimming.

Skimming is an act by stealing the information contained in a credit or debit card by illegally copying the information contained in the magnetic strip of a credit or debit card. Skimming perpetrators carry out their actions by using a pocket WiFi router that contains a camera that has been designed in such a way that it is similar to the PIN button cover device found on ATM machines with the aim of stealing the PIN of bank customers. With the method carried out by the thief, the required data and PIN number will be obtained and then a duplicate of the data obtained from the magnetic stripe will be made into a new (empty) ATM card.[7]

Article 5 paragraph (2) of the ITE Law states that Electronic Information and/or Electronic Documents and/or printouts are an extension of applicable legal evidence in accordance with applicable event law in Indonesia. Electronic evidence in the crime of skimming is obtained from CCTV footage installed at the ATM. However, there are still perpetrators of skimming crimes including foreign nationals who continue to

[7] Megi Mokoginta, "Perlindungan Nasabah Bank Dari Kejahatan Pembobolan Atm Menurut Uu No. 8 Tahun 1999 Tentang Perlindungan Konsumen," *Lex Privatum* 4, no. 6 (2016). p. 104.

commit their crimes despite knowing that the skimming crimes they commit are recorded on CCTV installed at ATM.

There are several studies related to this paper whose center of study is different from this paper, including research that examines legal protection against losses experienced by bank customers due to skimming in terms of information technology and banking perspectives,[8] settlement of criminal acts of fraud and theft through skimming,[9] imposing criminal sanctions on foreign nationals who break into ATM using skimming techniques,[10] and law enforcement against illegal transactions using ATM cards belonging to other people.[11] Based on this description, there are two problems examined in this paper, namely: characteristics of the crime of skimming by foreign nationals in the Bali Regional Police jurisdiction and the factors that support and hinder the law enforcement process at the level of investigation of criminal acts skimming by foreign nationals within the jurisdiction of the Bali Police.

This research is very important to do because the advancement of information and electronic technology that uses the internet network is increasingly sophisticated, so that the impact on banking services to customers is easier and more practical. It is used by irresponsible people to steal customers' money by skimming. More and more cases of skimming are harming customers, but few can be revealed and the perpetrators are being prosecuted. Therefore, this research is very important and relevant to be done.

2. Research Methods

The research method uses a type of empirical legal research, which is a type of research that observes the facts that exist in the field and then examines the provisions/regulations with the applicable laws and regulations. The approach method uses a statutory approach and an analytical approach. Sources of data come from primary data, namely the results of interviews with various relevant sources/informants in this study and secondary data obtained from primary legal materials, namely laws and regulations, secondary legal materials, namely books, literature and journals relevant to this research and material. Tertiary lega materials are in the form of dictionaries, encyclopedias. Data are collected by interview techniques with several respondents/informants relevant to this research. Data analysis using the

[8] Dian Ekawati, "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan," *UNES Law Review* 1, no. 2 (2018): 157–171, https://doi.org/https://doi.org/10.31933/law.v1i2.24.

[9] Fitrohtul Azqiyah, "Penyelesaian Tindak Pidana Penipuan Dan Pencurian Melalui Skimming Pada Sistem Elektronik (Menurut Undang-Undang Nomor 11 Tahun 2008 Jo. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik)," *Dinamika: Jurnal Ilmiah Ilmu Hukum* 27, no. 3 (2021): 350–74.

[10] Christin Dessy Natalia, A A Sagung Laksmi Dewi, and I Made Minggu Widyantara, "Sanksi Pidana Terhadap Warga Negara Asing Yang Melakukan Tindakan Pembobolan Anjungan Tunai Mandiri (ATM) Dengan Teknik Skimming," *Jurnal Preferensi Hukum* 1, no. 2 (2020): 37–41, https://doi.org/https://doi.org/10.22225/jph.1.2.2340.37-41.

[11] Fina Agustina Suhyana, Sigid Suseno, and Tasya Safiranita Ramli, "Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain," *SIGn Jurnal Hukum* 2, no. 2 (2021): 138–56, https://doi.org/https://doi.org/10.37276/sjh.v2i2.92.

inductive method, which is a mindset based on things that are special, then from things that are special, a general conclusion is drawn.

3. Results and Discussion

3.1 Definition and Characteristics of the Crime of Skimming

Law enforcement is generally an activity carried out in the context of implementing certain legal equipment with the aim of imposing legal sanctions in ensuring compliance with established regulations.[12] Law enforcement is a mechanism in order to realize legal ideals into reality. These legal ideals will become the thoughts of the law-forming institutions that will be set forth in the laws and regulations. The formulation of thoughts forming the laws and regulations as outlined in the legal regulations which will determine how the law enforcement is carried out. In practice, the law enforcement mechanism leads to its implementation by law enforcement officials.[13]

Law enforcement of the investigation into the crime of skimming at ATM by the Bali Police, the investigation refers to the Regulation of the Head of the State Police of the Republic of Indonesia Number 6 of 2019 concerning Criminal Acts of Investigation (hereinafter referred to as Perkap No. 6 of 2019). There is an obstacle in law enforcement efforts in accordance with the applicable provisions for cybercrime, especially skimming, namely a situation that minimizes the use of paper (paperless). This clearly raises a problem, especially in the field of evidence in terms of collecting information that is collected, processed, stored, and sent using softcopy data (electronic data). Cybercrime is a crime created from the negative influence of advances in internet application technology.[14] In essence, cyber crime is an activity that optimizes computer equipment as a tool or media that is supported by a telecommunications system, either using a telephone or a wireless system using a special wireless antenna. This is what is called telematics, namely the convergence of telecommunications, media and information technology, which originally each developed separately.[15]

Cyber crime is seen as a world of computer-based communication, which is known daily by the general public as the internet. The internet is a computer network system that can connect between countries, between continents based on the transmission control protocol / internet protocol. The presence of Cyber space (internet) breaks the barriers that are limited by distance and time to become unlimited.[16] There are several forms of cyber crime that have close ties to the use of computer-based technology and telecommunications networks, including:

---

[12] S Harefa, "Penegakan Hukum Terhadap Tindak Pidana Di Indonesia Melaui Hukum Pidana Positif Dan Hukum Pidana Islam. University Of Bengkulu Law Journal, 4 (1), 35–58," 2019.

[13] Satjipto Rahardjo, "Penegakan Hukum: Suatu Tinjauan Sosiologis," 2009. p. 24.

[14] Ari Jualiano Gema, "Cybercrime: Sebuah Fenomena Di Dunia Maya," n.d.

[15] Rini Retno Winarni, "Efektivitas Penerapan Undang–Undang ITE Dalam Tindak Pidana Cyber Crime," *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat* 14, no. 1 (2016), https://doi.org/http://dx.doi.org/10.36356/hdm.v14i1.440.

[16] Alfath Ridho Illahi, "Tinjauan Yuridis Tentang Penanggulangan Kejahatan Dunia Maya (Cyber Crime) Yang Berkonten Dengan Pornografi= The Juridical Review of Cyber Crime Prevention in Pornography" (Universitas Pelita Harapan, 2017).

1. *Unauthorized Access to Computer System and Service,* is a crime with a modus operandi by entering a computer network system secretly without the permission or knowledge of the owner in an illegal manner. Usually, criminals called hackers carry out these actions aimed at tapping or hijacking data or taking important and confidential information from the owner without permission. There is also a hacker who acts with the intention of testing his ability to break into the security that is owned or embedded in an internet network. The higher the level of security possessed by an internet network system that was successfully breached, the higher the level of satisfaction of the hacker.
2. *Illegal Contents*, is a crime committed by uploading content or data and information to the internet regarding hoaxes, unethical and classified as an act that is against the law and can cause a commotion in the general public.
3. *Data Forgery,* is a crime committed by making as if the original data in important documents stored as scriptless documents via the internet. The target of this crime is usually aimed at e-commerce documents with the mode as if there was a technical error in typing so that the goal of the perpetrator to seek profit can be achieved.
4. *Cyber Espionage,* is a crime to spy or spy on circumstances/conditions/profits and certain other things from other parties who are desired by seeking to break through the internet network system (computer network system) of the targeted parties. This crime is generally carried out by targeting business competitors who are already using a computerized system to store important data.
5. *Cyber Sabotage and Extortion,* is a crime committed by disrupting, damaging and even destroying data from a computer program or a computer network system connected to the internet. This crime in the general public is often encountered in the form of a virus or a certain program that accidentally enters the internet network which causes the performance of computer programs to be disrupted, slow, and often error-free, does not work according to its function, and even causes certain damages according to its function, with what the perpetrator wants. To seek profit, the criminal will come to offer himself as a service for repairing internet networks, computers and damaged data or rediscovering lost data that has been infected with an embedded virus, with high fees according to the wishes of the perpetrators of the crime.
6. *Offence Againts Intellectual Property,* is a crime specifically aimed at the intellectual property rights that a person owns on the internet. For example, plagiarizing the web site design/web page of a site belonging to someone else in a way that is contrary to the law.
7. *Infringements of Privacy,* is a crime that is directed at very personal and confidential data and information from other people, such as biodata/curriculum vitae, email address, email password, ATM PIN number, credit card number, medical information (medical record), and so on that stored in the application of personal data contained in a computerized network, and if it leaks to irresponsible parties it can cause a loss that is both material and immaterial.[17]

The crime of skimming is carried out by the perpetrator by taking data from banking customers which is carried out without knowledge of the customer concerned in the

[17] Ibid.

ATM machine of a bank that is the target, which has a device called a magnetic strip installed. From this magnetic strip, customer data that has been successfully copied is then sent wirelessly to the perpetrator. Customer data that has been illegally retrieved stored in a magnetic strip is then copied using a tool in the form of electronic data capture called a skimmer. This skimmer will then function as a means of copying customers' personal data that has been stored in magnetic strips/magnetic tape used in banking transactions to identify customers who will make transactions through ATM.

The skimming process on ATM machines can be done by various methods including:

1. Glancing at the customer who is entering the pin combination number on the ATM or Debit machine;
2. Installing a mini camera on an ATM machine in an invisible place with the aim of seeing the movement of the customer's fingers when entering the pin combination number; or
3. By installing a fake keyboard key that is useful for viewing and storing the pin combination number entered by the customer.[18]

After the customer data and ATM pin number are owned by the perpetrator, the perpetrator will carry out the next process, namely by filling in a new empty electronic card with customer data that has been previously obtained in the skimmer. In the process of making a new fake ATM card, this can be done in three ways, namely:

1. How to Altered Card
   Is a method that is done by changing and entering data according to the wishes of the perpetrator in the original electronic card. This method is done by heating the relief on the electronic card (reembossed) and then filled in with the customer's personal data (re-encoded).[19]
2. How to *Totally Counterfeit*
   This is a method that is done by using an entirely fake electronic card. This method requires the perpetrator to print a new card that is similar to the original electronic card containing images, logos, and numbers so that it looks as if the electronic card made is genuine. It is made through an embossing and encoding process.[20]
3. How to *White Plastic Card*
   This is the way to make electronic cards using plain white plastic cards. This method only goes through the encoding process because the manufacture of fake cards is only done by entering customer data without printing something that resembles the original physical card.[21]

This ATM card, which is a fake electronic card, will be able to be used on ATM machines and debit machines as well as genuine ATM cards in general. So it can be concluded that the skimming perpetrator will be able to freely use the fake ATM card he has made to carry out banking transactions according to his wishes without being

[18] R Toto Sugiharto, "Tips ATM Anti Bobol: Mengenal Modus-Modus Kejahatan Lewat ATM Dan Tips Cerdik Menghindarinya," *Media Pressindo, Jakarta*, 2010. p. 126-127.
[19] Ibid.
[20] Lexy Fatharany Kurniawan, "Penegakan Hukum Tindak Pidana Kartu Kredit" (Universitas Airlangga, 2006). p. 30-31.
[21] Ibid.

noticed by the customer who has the original ATM card. Of course, this skimming act is very detrimental to customers, so there needs a law enforcement process in order arresting the perpeprators.

The start of a process of investigation and investigation by the police if there have been reports and complaints from the public that a criminal event has occurred. Investigators have an obligation to carry out investigative activities that aim to find out whether an incident that has been reported has indeed occurred and to ascertain whether it is a legal event or not, because it is not uncommon that reports or complaints submitted by the public do not clearly indicate a legal events. The initial process of investigating the crime of skimming generally uses tools in the form of a set of computers, other electronic devices such as cellphones, androids, tablets, and systems that are connected to a network and the internet. The evidence obtained in a skimming crime is generally stored in the electronic device system or in a computer system. So in essence, a process of investigative action is to find and then confiscate the suspect's electronic or computer equipment or goods as evidence and at the same time find out who the suspect is. From the computer, the investigation can determine whether there is evidence that a skimming crime has occurred.[22]

The modus operandi of skimming crimes that use the internet and multi-media technologies such as CCTV, will affect the law enforcement process especially at the investigation and investigation stage. Law enforcement officials collect evidence and evidence related to this legal event by observing the CCTV installed in every ATM machine, so that legally it can be used as evidence in the next examination process. The issuance of the Decree of the Constitutional Court (MK) No. 20/PUU-XIV/2016 provides a legal umbrella to expand the types of evidence contained in the Criminal Procedure Code (*KUHAP*) so that it has legal force in the trial process. There are formal and material requirements that must be met in the ITE Law. Article 5 paragraph (4) basically states that the information and electronic documents referred to by law do not have to be in written form. While the material requirements are in Article 6, Article 15, and Article 16 of the ITE Law, which basically states that Information and Electronic Documents that have been collected must be guaranteed to be authentic, intact, and their availability. To ensure the achievement of these material requirements, it is necessary to check using experts in the field of digital forensics. So the point is, prior to the Constitutional Court's decision, the regulation on the validity of CCTV acquisition as legal evidence was not regulated.

After the issuance of the decision of the Constitutional Court No. 20/PUU-XIV/2016 immediately changed the standard for evidence using digital evidence, which includes CCTV as one of the legal digital evidence. The Constitutional Court's ruling states that Article 5 paragraph (1) and paragraph (2) of the ITE Law is contrary to the 1945 Constitution of the Republic of Indonesia as long as it is not interpreted differently, in particular the phrase "Electronic Information and/or Electronic Documents" as evidence obtained in the context of law enforcement at the official request of the police, prosecutors, and/or other law enforcement institutions as determined based on Article 31 paragraph (3) of the ITE Law.

[22] Indra Safitri, "Tindak Pidana Di Dunia Cyber," *Legal Journal From Indonesian Capital & Investmen Market* 2, no. 1 (1999).

Cyber crime when compared to other common crimes contained in the Criminal Code, has different characteristics. In carrying out its modus operandi, this form of skimming crime has its own uniqueness when compared to other cyber crimes. This is what causes the law enforcement process that begins with the investigation and investigation process requiring specialist arrangements outside of the generalist provisions stipulated in the Criminal Procedure Code. The special arrangements for skimming crimes contained in the ITE Law are as follows:

a. The validity of electronic evidence in the form of electronic information and electronic documents which are not required to be in written form can be used as legal evidence in the process of proving in the crime of skimming. (Article 5)
b. There is a special authority granted by law to certain Civil Servant Officials within the Government whose scope of duties and responsibilities is in the field of information technology and electronic transactions as investigators. (Article 43)
c. In the process of examining the crime of skimming, law enforcement officers such as investigators, public prosecutors, and judges have the authority to request expert information from service providers or electronic system operators regarding data related to the cases being handled, while maintaining privacy, confidentiality, and smoothness, public services, data integrity and data integrity. (Article 16)
d. In the process of investigating the crime of skimming, investigators will coordinate and ask for permission from the chairman of the local district court so that they can be given the authority to conduct searches, confiscate electronic systems related to the alleged crime of skimming, to prevent the electronic system from being deleted by the perpetrators or to avoid tracking the perpetrators quickly, so that the traces of the perpetrators are easy to find. (Article 43)

The crime of skimming is one of the crimes that are oriented towards utilizing the sophistication of information technology and internet networks so that along with the development of increasingly sophisticated technology, the modus operandi variation of skimming crimes will increase also. Therefore, law enforcement officers in carrying out their duties in addition to being guided by the applicable laws and regulations, must also be equipped with knowledge and skills in the field of information and technology (IT) to eradicate skimming crimes so that the perpetrators are not rampant and arbitrary so that people use ATM or internet-connected technologies get legal protection.

3.2 Supporting and Inhibiting Factors in the Investigation of the Crime of Skimming at Automated Teller Machines (ATM)

Friedman said that there are three elements that imply the process of law enforcement which includes substance, structure and culture. The substance component requires that the rules be clear and do not lead to multiple interpretations. So, in making laws, it is obligatory to pay attention to 3 (three) aspects, namely philosophical, juridical and

sociological. The substance here means an integrity of reality in people's lives who can live in the midst of society which can also be called living law.[23]

The process of Law Enforcement more fully stated by Soerjono Soekanto in the theory of Law Enforcement, including: (1) the legal factor itself (law factor); (2) law enforcement factors; (3) factors of facilities and facilities that support law enforcement; (4) community factors; and (5) cultural factors. These five factors can be an obstacle to the law enforcement process at the level of investigation of the crime of skimming at ATM using skimming techniques by Foreign Citizens in the Bali Police Legal Area.

Related to the legal factors themselves (law factors) and community factors, they can be supporting factors, but these two factors can also have the potential to be an inhibiting factor in the law enforcement process at the investigation level against skimming crimes at ATM using skimming techniques by Foreign Citizens in the Bali Police Legal Area. Therefore, the inhibiting factors in the law enforcement process at the investigation level against skimming crimes at ATM using skimming techniques by foreign citizens in the Bali Police Legal Area include:

a. Legal Factors Own (Legal Factors)
   Skimming is a crime of stealing from an ATM using high technology or electronic system technology. The provisions in the ITE Law and the Amended ITE Law do not regulate criminal acts using computer facilities and/or electronic system facilities that can harm other parties. Meanwhile, using Article 362 of the Criminal Code is also not possible, because the crime of skimming is not ordinary theft, but theft using electronic system technology.
b. Law Enforcement Factor
   Most of the investigators of the Bali Police are still not familiar with information technology and there is no internet socialization at the Bali Police. Considering the very importance of supporting human resources to support the smooth running of an investigation, investigation, and arrest process. According to the results of interviews with A.A. Wirahhatiningsih, Head of the Division Bin OPS The general criminal director of the Bali Police said that only a few personnel and not many investigators at the Bali Police understand the field of information technology, this is not balanced with the existing cases, along with the rampant crime of skimming through ATM which can still happen at any time in the country. There are still many skimming crimes that have not been revealed or the investigation has stopped due to a lack of experts at the Bali Police Police Office. Therefore, it is necessary for the Bali Police to think about providing IT training to police officers at each Poltabes, Polda, Polres and Polsek specifically regarding the crime of skimming. The limited number of personnel who handle not only skimming crimes, of course, requires an adequate number of personnel. Because the lack of investigators will hinder the investigation process, the process will be slow. The limited number of investigators greatly affects the effectiveness of the investigator's performance in conducting investigations. With the current number of investigators, it is

[23] I Nengah Suantra and Made Nurmawati, "Penegakan Hukum Terhadap Pelanggaran Atas Ketentuan Perizinan Toko Swalayan Di Wilayah Provinsi Bali," *Jurnal Magister Hukum Udayana(Udayana Master Law Journal)* 8, no. 2 (2019): 188–206, https://doi.org/https://doi.org/10.24843/JMHU.2019.v08.i02.p04.

clear that it is difficult to deal with the increasing crime rate. With the number of existing investigators, it is very disproportionate to the number of reports that must be completed, so the performance of the Bali Police Satreskrim is not effective.

c. Factors of facilities and infrastructure
   The factor of facilities and facilities that support law enforcement is still considered to be one of the weak factors in law enforcement against the crime of skimming. For example, the currently available computer facilities only function as administrative activities, while e-commerce-based crimes as well as skimming crimes are carried out using networked computers and high and complex technological capacities so that law enforcement officials are still difficult to track, detect or balance activities. the perpetrators of these crimes. The same thing can also be seen in the lack of ability and skills of law enforcement officers in the computer field which results in tactical, technical investigations, prosecutions and examinations in court because they involve the system in the computer.
d. Community Factor
   People in the Bali Police jurisdiction who have been victims of the crime of skimming are not willing to report to law enforcement officers, because according to information from I Nengah Ariasa, a BNI Bank employee in Denpasar City, he said that people are bothered by long-winded and procedural reports. They also assume that by reporting to law enforcement officials their lost money will not be returned. Another consideration is that the amount of money lost is relatively small. The results of this interview show that the legal awareness of this community is still low. Reporting to law enforcement officials for the skimming crime that happened to him, is actually not for his own sake, but for the benefit of the wider community. If there are people who report the occurrence of this skimming crime, law enforcement officers become aware to eradicate skimming crimes that may occur in the future, it can also be useful for other people to be careful in every transaction with an ATM card.
e. Cultural Factor
   Cultural factors are considered to be one of the causes of weak law enforcement on skimming crimes. Culture is a tradition or habit that is passed down from generation to generation and is recognized and maintained. People who are victims of the crime of skimming are usually reluctant to report and deal with the police, especially since the losses suffered are not so great that they prefer to classify them. This culture makes it difficult for the criminal act of skimming to be revealed and processed by investigators up to the trial process in court.

Based on several inhibitory and supporting factors in law enforcement efforts above, it can be known that in addition to being a supporting factor can also be an inhibitory factor in law enforcement. This happens because if the factor is not able to function optimally it will be an inhibitory factor in law enforcement. For example, the human resources factor and the infrastructure factor. If human resources cannot use the facilities and infrastructure properly, even though the facilities and infrastructure available are sophisticated then this will be a factor inhibiting law enforcement. Similarly, if human resources are skilled, but facilities and infrastructure do not support it will be an inhibitory factor in law enforcement as well. So there needs to be

good synergy to create a law enforcement system consisting of qualified supporting factors.

Factors supporting the law enforcement process at the stage of investigating skimming crimes at ATM using skimming techniques by Foreign Citizens in the Bali Police Legal Area in terms of the perspective of law enforcement theory put forward by Soerjono Soekanto include the legal factors themselves (law factors and community factors) which is stated as follows:[24]

a. The Legal Factor
   According to the law enforcement theory from Soerjono Soekanto, one of the factors that influence the law enforcement process is the law itself (law factor). In law enforcement efforts, there is a need for harmonization between various laws and regulations of different degrees. This discrepancy can occur, for example, between written and unwritten regulations, between higher-level regulations or lower-level regulations, between specific and general laws, and between the laws that apply later and those that were in force earlier. All of these can affect law enforcement problems because the purpose of establishing a regulation is to provide legal certainty, benefit and justice. For this reason, in order to avoid that a regulation does not apply effectively in the community, it is necessary to pay attention to the principles and objectives of the law itself.
   Related to the crime of skimming at ATM with skimming techniques by Foreign Citizens in the Bali Regional Police Legal Area. Considering the crime of skimming through ATM, including banking crimes, the perpetrators can be charged with Law Number 7 of 1992 concerning Banking (Banking Law 1992) and Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking (Banking Law 1998). In addition, Law No. 36/1999 on Telecommunications (Telecommunication Law) can also be used.
b. Community Factor
   According to the law enforcement theory from Soerjono Soekanto, other factors that influence the law enforcement process are community factors. The community is the primary factor that contributes greatly to law enforcement efforts in Indonesia because it is closely related to public awareness of their rights and obligations before the law. A legal substance contained in legislation and legal structures (law enforcement officers) that are already good and optimal, will be meaningless if it is not supported by people who have legal awareness which includes knowledge of the law, appreciation of legal functions and obedience to the law. Law enforcement will not run smoothly in accordance with the ideals of the law if public awareness of the law is still low.

   People in the case of skimming through ATM are people from banking circles and people who have banking ATM or what are referred to as bank customers. Efforts made by the banking sector towards law enforcement of the crime of skimming are immediately resolving complaints from customers if there are customers who are victims of skimming crimes, educating customers to be careful when making transactions at ATM or EDC merchant machines anywhere, so that there is no opportunity for perpetrators to remember or record customer debit/credit card serial numbers and improve security around

[24] Soekanto Soejono, "Pengantar Penelitian Hukum," *Universitas Indonesia, Jakarta*, 1986.

ATM machines through security and CCTV to minimize similar crimes, as well as improve systems and infrastructure of machines and banking systems to become more sophisticated and vulnerable to customer crime.

Efforts made by the banking community towards law enforcement of the crime of skimming are immediately resolving complaints from customers if there are customers who are victims of skimming crimes, educating customers to be careful when making transactions at ATM or EDC merchant machines anywhere. , so that there is no opportunity for perpetrators to remember or record customer debit/credit card serial numbers as well as improve security around ATM machines through security and CCTV to minimize similar crimes, as well as improve systems and infrastructure of machines and the banking system to be more efficient, sophisticated and vulnerable to customer crime.

The public as bank customers should be careful when making transactions at ATM or EDC merchant machines anywhere. The call for caution and awareness is needed from customers so as not to carelessly throw away credit/debit card transaction receipts that have been used, because from credit/debit card transaction receipts there are data that can be traced to be used in criminal acts of theft of funds and development knowledge for the general public regarding the types of banking crimes and the modus operandi of the perpetrators of the skimming crime. This attitude to always be careful is intended so that there is no opportunity for perpetrators to remember or record customer debit/credit card serial numbers and improve security around ATM machines through security and CCTV to minimize similar crimes, as well as improve machine systems and infrastructure.

4. Conclusion

Based on the description of the discussion above, the law enforcement process at the investigation stage of the crime of skimming by foreign nationals in the Bali Police jurisdiction is carried out based on the National Police Chief Regulation No. 6 of 2019 includes receiving police reports, making administrative investigations, examining victims and witnesses, collecting evidence and conducting cases that end in the examination process in court. The process of investigating the crime of skimming on an ATM machine is not the same as the mechanism for investigating other ordinary (conventional) crimes. This difference can be seen in the process of catching criminals and requires coordination with related parties such as the head of the local court. Factors supporting the law enforcement process at the level of investigation of the crime of skimming by foreign nationals in the Bali Police jurisdiction include: (a) Legal factors; and (b) Community factors. In an effort to enforce the law on the crime of skimming, namely the bank immediately processes reports from customers if there are customers who are indicated to be victims of skimming. People who are bank customers have been careful in every transaction through ATM machines or EDC machines merchants. While the factors that hinder the law enforcement process at the investigation level against skimming crimes by foreign nationals in the Bali Regional Police jurisdiction include: (a) The legal factors themselves (Legal Factors), although the existence of cybercrime regulations is not only in the Information and Technology Law, but also includes: Information and technology law, but there are also other special laws outside the Criminal Code, but there are still unregulated forms of cybercrime, especially those involving the misuse of advanced technology such as

skimming through ATM; (b) The factor of law enforcement officers, because most of the Bali Police investigators have not mastered information technology well so that this is not balanced with the existing cases; (c) Facilities and facilities that do not support law enforcement, such as uneven internet facilities, weak wifi networks and limited computers/laptops; (d) Community factors in the Bali Police jurisdiction who have been victims of skimming crimes, are not willing to report to law enforcement officials, because they think it will trouble them with procedural reports. This fact proves that the legal awareness of the community is quite low; and (e) the legal culture factor that feels reluctant to deal with the police, especially since the losses suffered are not so great that they prefer to classify.

Acknowledgments

In this article, the authors would like to thank the resource person Mr. Adhiguna at the General Crime Director Unit of the Bali Police who has provided a lot of information related to the writing of this article and also other colleagues who cannot be mentioned, all of whom have motivated and become brain storming in developing the author's ideas.

References

Anwari, Imron. "Penerapan Hukum Pidana Kini Dan Masa Mendatang." Genta Publishing, Yogyakarta, 2014.

Arthesa, Ade, and Edia Handiman. "Bank Dan Lembaga Keuangan Bukan Bank." *Jakarta, PT Indeks Kelompok Gramedia*, 2006.

Azqiyah, Fitrohtul. "Penyelesaian Tindak Pidana Penipuan Dan Pencurian Melalui Skimming Pada Sistem Elektronik (Menurut Undang-Undang Nomor 11 Tahun 2008 Jo. Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik)." *Dinamika: Jurnal Ilmiah Ilmu Hukum* 27, no. 3 (2021): 350–74.

Ekawati, Dian. "Perlindungan Hukum Terhadap Nasabah Bank Yang Dirugikan Akibat Kejahatan Skimming Ditinjau Dari Perspektif Teknologi Informasi Dan Perbankan." *UNES Law Review* 1, no. 2 (2018): 157–71. https://doi.org/https://doi.org/10.31933/law.v1i2.24.

Gema, Ari Jualiano. "Cybercrime: Sebuah Fenomena Di Dunia Maya," n.d.

Harefa, S. "Penegakan Hukum Terhadap Tindak Pidana Di Indonesia Melaui Hukum Pidana Positif Dan Hukum Pidana Islam. University Of Bengkulu Law Journal, 4 (1), 35–58," 2019.

Illahi, Alfath Ridho. "Tinjauan Yuridis Tentang Penanggulangan Kejahatan Dunia Maya (Cyber Crime) Yang Berkonten Dengan Pornografi= The Juridical Review of Cyber Crime Prevention in Pornography." Universitas Pelita Harapan, 2017.

Kasmir, Dr. "Dasar-Dasar Perbankan Edisi Revisi 2014." *Jakarta: Rajawaloi Pers*, 2015.

Kurniawan, Lexy Fatharany. "Penegakan Hukum Tindak Pidana Kartu Kredit." Universitas Airlangga, 2006.

Mokoginta, Megi. "Perlindungan Nasabah Bank Dari Kejahatan Pembobolan Atm Menurut Uu No. 8 Tahun 1999 Tentang Perlindungan Konsumen." *Lex Privatum* 4, no. 6 (2016).

Natalia, Christin Dessy, A A Sagung Laksmi Dewi, and I Made Minggu Widyantara. "Sanksi Pidana Terhadap Warga Negara Asing Yang Melakukan Tindakan Pembobolan Anjungan Tunai Mandiri (ATM) Dengan Teknik Skimming."

Jurnal Preferensi Hukum 1, no. 2 (2020): 37–41. https://doi.org/https://doi.org/10.22225/jph.1.2.2340.37-41.

Rahardjo, Satjipto. "Penegakan Hukum: Suatu Tinjauan Sosiologis," 2009.

Safitri, Indra. "Tindak Pidana Di Dunia Cyber." *Legal Journal From Indonesian Capital & Investmen Market* 2, no. 1 (1999).

Sambiangga, Roni. "Sistem Keamanan ATM (Automated Teller Machine/Anjungan Tunai Mandiri)." *Teknik Informatika Sekolah Teknik Elektro Dan Informatika Institut Teknologi Bandung*, 2014, 1–10.

Soejono, Soekanto. "Pengantar Penelitian Hukum." *Universitas Indonesia, Jakarta*, 1986.

Suantra, I Nengah, and Made Nurmawati. "Penegakan Hukum Terhadap Pelanggaran Atas Ketentuan Perizinan Toko Swalayan Di Wilayah Provinsi Bali." *Jurnal Magister Hukum Udayana(Udayana Master Law Journal)* 8, no. 2 (2019): 188–206. https://doi.org/https://doi.org/10.24843/JMHU.2019.v08.i02.p04.

Sugiharto, R Toto. "Tips ATM Anti Bobol: Mengenal Modus-Modus Kejahatan Lewat ATM Dan Tips Cerdik Menghindarinya." *Media Pressindo, Jakarta*, 2010.

Suhyana, Fina Agustina, Sigid Suseno, and Tasya Safiranita Ramli. "Transaksi Ilegal Menggunakan Kartu ATM Milik Orang Lain." *SIGn Jurnal Hukum* 2, no. 2 (2021): 138–56. https://doi.org/https://doi.org/10.37276/sjh.v2i2.92.

Tianotak, Nazarudin. "Urgensi Cyberlaw Di Indonesia Dalam Rangka Penangan Cybercrime Disektor Perbanka." *Jurnal Sasi* 17, no. 4 (2011).

Wahid, Abdul. "Kejahatan Mayantara (Cyber Crime)," 2005.

Winarni, Rini Retno. "Efektivitas Penerapan Undang–Undang ITE Dalam Tindak Pidana Cyber Crime." *Jurnal Ilmiah Hukum Dan Dinamika Masyarakat* 14, no. 1 (2016). https://doi.org/http://dx.doi.org/10.36356/hdm.v14i1.440.

Laws and Regulations

Law Number 8 of 1981 concerning the Criminal Procedure Law.

Law Number 10 of 1998 on Amendments to Law No. 7 of 1992 on Banking.

Law Number 36 of 1999 on Telecommunications.

Law Number 11 of 2008 on Information and Electronic Transactions.

Law Number 48 of 2009 on Judicial Power.

Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Information and Electronic Transactions.

Regulation Of The State Police Of The Republic Of Indonesia Number 6 Of 2019 About Repeal Of Police Chief Regulations The Republic Of Indonesia Number 14 Of 2012 Concerning Management Of Criminal Investigations