Ratio Legis Journal
ISSN 2830-4624
published by
Master of Law, Faculty of Law
Universitas Islam Sultan Agung

Volume 5 No. 2, June 2026

Police Efforts in Preventing and Handling Skimming Crime in The Jurisdiction of The Riau Islands Regional Police

Laurensia Trinita Samosir

Faculty of Law, Universitas Islam Sultan Agung (UNISSULA) Semarang, Indonesia, E-mail: laurensiatrinitasamosir.std@unissula.ac.id

Abstract. *Skimming is a form of cybercrime that exploits vulnerabilities in banking security systems, particularly ATMs and debit cards, by illegally copying customers' data and subsequently using such information to gain unauthorized access to their bank accounts. The rapid advancement of information technology has contributed to the increasing complexity of this crime, creating significant challenges for law enforcement agencies in both its prevention and suppression. This study aims to analyze the effectiveness of police efforts in combating skimming crimes, identify the obstacles encountered in law enforcement practices, and formulate strategic solutions to enhance the effectiveness of legal enforcement against such offenses. This research employs a normative-empirical legal research method using statutory and conceptual approaches. The analytical framework is based on Soerjono Soekanto's Theory of Law Enforcement, which serves as the primary analytical tool in examining the effectiveness of law enforcement efforts. However, the effectiveness of these efforts remains suboptimal due to several challenges, including limited human resources with expertise in digital forensics, inadequate facilities and infrastructure, the complexity of electronic evidence-based investigations, and low levels of digital literacy among the public.*

Keywords: *Criminal Act; Cybercrime; Effectiveness Prevention; Police Efforts; Skimming.*

1. Introduction

The development of information and communication technology has had a significant impact on human life across all sectors, including the banking sector. The implementation of electronic banking systems, Automatic Teller Machines (ATMs), and digital transactions initially provided convenience and efficiency for customers in conducting financial transactions anytime, anywhere. However, on the other hand, these advances have also opened the door to the emergence of new forms of crime that exploit technological weaknesses, one of which is skimming (cybercrime).[1] Skimming is a criminal act carried out by illegally copying data information from ATM/debit cards using a skimming device installed on an ATM machine or other electronic transaction device, with the aim of unauthorized access to customer accounts and funds.

The phenomenon of skimming crime poses a serious challenge for both banking institutions and law enforcement due to its increasingly sophisticated and difficult-to-detect methods. Skimming not only harms customers financially but also has the potential to damage their financial well-being.

Public trust in electronic banking systems and the art of law enforcement in the digital age. Furthermore, these crimes often involve transnational networks that exploit weaknesses in technology and surveillance systems, requiring a systematic, coordinated, and effective response approach from various parties, including the police, banks, regulators, and other civil law institutions.

Skimming crime is the act of stealing credit/debit card information by copying all the information contained on the magnetic strip.[2] cards illegally and later the customer's information or data will be copied onto the card which is still blank. The function of the magnetic stripe is more or less the same as a cassette tape whose ferromagnetic material can be used to store data.[3] The goal of this crime is none other than to embezzle the bank's customer funds. Advances in information technology are a positive thing and have positive impacts when used properly and appropriately. However, it can also have negative consequences for individuals if misused, such as in skimming, commonly known as cybercrime.

Normatively, the crime of skimming can be viewed as a violation of the provisions on unlawful acts in national criminal law as well as electronic information and transaction law.

Referring to Article 4 Paragraph (1) of Law Number 8 of 1999 concerning Consumer Protection (UUPK), it states that every consumer has the right to security, comfort, and safety in using goods and/or services. This also applies to every banking consumer to obtain legal protection in conducting transactions to avoid the risk of losses that will arise. Then, based on a national survey conducted in 2021, from a number of banking or financial institution products,

---

[1]Laksana, Andri Winjaya. 2019. "Cybercrime Criminalization from a Positive Criminal Law Perspective." Unissula Law Journal 35, No. 1, p. 52.

[2]Enrick, Michael. 2019. "ATM Hacking Using Skimming Techniques in Relation to Restitution Applications" Jurist-Diction 2, No. 2: 557-558.

[3]Wardani, Dian Eka Kusuma and Maskun. 2019. "Skimming Crime as a Form of Cyber Crime". Jurisprudentie 6, No. 1. Pp. 168-169.

respondents considered e-wallets and bank accounts as products that were considered vulnerable to data leaks. Citing the Indonesian Cyber Security Forum 2024 report, Member of Commission III of the House of Representatives, Bambang, stated that more than 2.3 billion personal data, suspected to belong to Indonesian citizens, had circulated in various dark forums in the past three years. In 2023 alone, around 409 million data were leaked from a number of services, including BPJS Kesehatan, PLN Mobile, and a number of large e-commerce platforms.[4] On the other hand, as many as 20.5% of respondents believe that banking products do not have adequate data protection, making them highly vulnerable to data leaks through ATM skimming. can harm customers or individuals.[5]

The phenomenon of skimming crimes is not merely a theoretical issue; it has been extensively addressed by law enforcement officials in Indonesia. The ITE Law can serve as a reference for law enforcement officials in combating this crime, as the rapid development and advancement of information technology have led to changes in human activities in various fields, directly influencing the emergence of new legal forms for handling cybercrime cases. The most representative example is the Batam District Court Decision Number 569/Pid.Sus/2022/PN Btm.[6], which handled the internet skimming case. This verdict indicates that the defendants were found guilty of intentionally copying and manipulating customer data using skimming technology, thereby harming both the bank and the customer.

The geographical context of the Riau Islands, particularly Batam, makes it a strategic region prone to shifts in transnational crime modes, including cybercrime such as skimming. This region is a center of economic, trade, and tourism activities that involve the mobility of foreign and domestic citizens, thus requiring a comprehensive crime prevention approach. In reality, this challenge is increasingly complex because the police must not only handle skimming crime reports but also collaborate with banks, financial services authorities, and digital forensics institutions to take effective action. This utilization has supported rapid business growth, as various information can be presented sophisticatedly and easily. obtain, and through long-distance relationships, telecommunications technology can be used for anything electronic media users desire. The parties involved do not need to meet in person; computer equipment and communication are sufficient. This situation marks the beginning of the cyber era

---

[4]Personal Data Leaks Continue to Threaten, But No Oversight Body Yet to Be Formed accessed on Saturday, January 31, 2026, at 19.30 WIB.

[5] Delphia, Risanti, and K, Harjono Maykada. Public Perception of Personal Data Protection: 2021 National Survey (Jakarta, Katadata Insight Centre, 2021), 36.

[6] Batam District Court Decision Number 569/Pid.Sus/2022/PN Btm

in business.[7] Another issue faced is the evidentiary aspect in skimming cases. Technology-based crimes like this often leave no traditional physical evidence, but rather electronic data that requires specialized skills to collect, analyze, and present in court. This raises legal questions regarding the integration of conventional and digital evidence so that law enforcement can proceed effectively in accordance with applicable criminal procedural standards related to the position of criminal law and the responsibilities of perpetrators and protectors of customer personal data.[8]

In prevention efforts, banking plays a role as the main pioneer in preventing skimming crimes. Banking operates in the business sector related to financial services, especially those related to saving money and carrying out financial transactions for Customers. Banking plays a crucial role in a country's economy by facilitating the flow of funds and providing financial access to the public. The banking sector relies heavily on customers who save and borrow from banks, as customers are one of the most important factors in banking. Winning these customers requires trust in the bank's ability to serve them. In the case of card skimming crimes, the modus operandi (data theft) used by criminals is quite complex and cannot be easily carried out by just anyone. Therefore, increased e-banking security and increased customer vigilance are necessary to ensure that e-banking transactions do not lose trust and to provide customer protection.

Considering the importance of customer protection as outlined in Pillar VI of the Indonesian Banking Architecture (API), customer protection efforts in Pillar VI of the API are outlined in four interrelated aspects that, collectively, will enhance the protection and empowerment of customer rights. Furthermore, regulations governing the implementation of card-based payment instruments are specifically regulated in Bank Indonesia Regulation No. 11/11/PBI/2009.

Banking consists of various types of financial institutions such as commercial banks, Islamic banks, foreign exchange banks, consumer banks, and others. Each type of bank has different duties and functions, such as commercial banks which tasked with facilitating economic activities, Islamic banks offering financial services based on Sharia principles, and consumer banks offering financial services to individuals and families. Banks also play a crucial role in increasing financial inclusion and expanding public access to financial services, for example by providing banking services through digital channels like mobile banking and

[7] iniek Suparni, Cyberspace Problems and Applications for Regulation, Jakarta, Sinar Grafika.2009, p. 1.

[8] Gunawan, Tri. 2023. “Reconstruction of Bank Accountability Regulations in Issuing Customer ATM Cards Against Card Skimming Crimes Based on Justice Values”. Thesis of K Law Librarian 4 Unissula.

internet banking. Therefore, banking plays a strategic role in economic development and improving public welfare.

Bank regulations in carrying out their duties are regulated in Article 25 of Law Number 23 of 1999 concerning Bank Indonesia as amended by Law Number 3 of 2004 concerning Amendments to Law Number 23 of 1999 concerning Bank Indonesia (hereinafter referred to as UUBI) which states that Bank Indonesia has the authority to determine banking provisions containing the principle of prudence. Furthermore, Article 26 of the Bank Indonesia Law states that Bank Indonesia has the authority, including:[9]

1. Issue and revoke banking business licenses;

2. Granting permission for opening, closing and moving bank offices;

nsuring transparency and security in conducting business is crucial for banks when implementing regulations and rules. Regulations and rules are implemented to maintain financial system stability and prevent actions that harm customers and the national economy.

Some of the regulations and rules that are implemented include:

1. Regulations on Banking Governance: Maintaining governance good practices within the bank, including conducting internal audits and regular inspections by supervisors.

2. Regulations on Customer Protection: Guarantee the security of funds and customer rights in transactions with banks.

From a criminal law enforcement perspective, the police, as the vanguard of crime prevention, play a crucial role. They are tasked with investigating, prosecuting, and collaborating with other agencies to uncover skimming crimes and apprehend perpetrators. However, various operational barriers, such as a lack of digital forensics training, limited early detection technology, and low public awareness of early preventive measures, represent obstacles that must be overcome to effectively prevent and combat skimming.

2. Research Methods

Based on the description in this research, this type of research uses normative-empirical legal research (Normative-Empirical Legal Research), with the support of applying empirical juridical. Soerjono Soekanto uses a benchmark in his discussion of normative legal research is from the nature and scope of legal

[9] Sentosa Sembiring, Banking Law, Revised Edition, (Bandung: Mandar Maju, 2012), p. 275.

discipline, discipline is defined as a system of teachings about reality, which usually includes analytical discipline and prescriptive discipline, and legal discipline. Usually included in the prescriptive discipline, if the law is seen to only cover its normative aspects.[10] Or in normative juridical terms, because in legal research one must also examine the juridical basis of the research.

3. Results and Discussion

3.1. Efforts to Determine the Role of the Riau Islands Regional Police in Combating Skimming Crimes

1. Philosophical Basis Regarding Efforts

The Indonesian word "upaya" (effort) means an effort, endeavor, or action taken to achieve a specific goal or solve a problem. Etymologically, the word comes from the Sanskrit word उपाय (upāya), which means a way or means to achieve something. In practice, "upaya" encompasses all forms of action that are planned, systematic, and directed towards achieving a desired outcome.

In the context of banking cybercrime, particularly skimming, the concept of "effort" must be understood as a series of strategic steps undertaken in an integrated manner by various parties to effectively prevent, detect, and address such crimes. Skimming, as a form of crime that exploits weaknesses in technological systems and user negligence, requires an approach that is not only repressive but also preventative and adaptive to technological developments. Therefore, efforts to combat skimming must encompass regulatory, institutional, and regulatory dimensions.

technology, and community participation as a mutually supportive system. This effort is often referred to as prevention without punishment, which involves technical preventive measures that implement specific guidelines such as a code of conduct, a code of ethics, and a code of practice.80Essentially, crime prevention doesn't have a standard definition. However, its essence is a plan to reduce the number and opportunities for crime to occur in society.[11] This issue was emphasized at various UN Congresses, including the 6th UN Congress in Caracas, Venezuela, in 1980, on Crime Trends and Crime Prevention Strategies. It was further emphasized at the 7th UN Congress in Milan in 1985 and the 8th UN Congress in Havana in 1990, on the issue of "Social Aspects of Crime Prevention and Criminal Justice in the Context of Development."

---

[10] Ravena, Dey and Kristian. Criminal Policy, Jakarta, Kencana, 2017, p. 3

[11]Lab, Steven P. Crime Prevention : Approaches, Practices and Evaluations, USA, Anderson Pub Co, 2010, p.26.

The efforts of the Republic of Indonesia National Police in maintaining public security and order, enforcing the law, and protecting, serving, and serving the community. In the context of skimming crimes, the role of the police is divided into two groups of activities in efforts to combat criminal acts, especially skimming; Prevention Police efforts to prevent skimming crimes are:

Public awareness raising regarding the threat of skimming and how to prevent it; Technology patrols and cooperation with banking institutions to identify vulnerable points; Collaboration with related institutions such as the OJK, Bank Indonesia, and other technical agencies to strengthen data and transaction security systems.

Based on the description above, it can be seen that efforts to combat crime can be carried out using an integrated approach, namely using penal and non-penal means. These two means are interconnected and act as a single unit in combating crime.

Crime prevention efforts through criminal law are essentially part of law enforcement efforts (particularly criminal law enforcement). This effort reflects the police's function in law enforcement, which is to prosecute criminal acts in accordance with the principles of legal rules and protection. Therefore, it is often said that criminal law policy is part of law enforcement policy. Crime prevention policies are essentially an integral part of community protection efforts and efforts to achieve public welfare.

2. Efforts to Combat Skimming Crimes by the Riau Islands Regional Police

Combating crime is inseparable from law enforcement. Law enforcement is an effort to realize the ideas of legal certainty, social benefit, and justice. The process of realizing these ideas is the essence of law.

law enforcement[12]. Based on Article 1 paragraph (1) of the Republic of Indonesia Law Number 2 of 2002 concerning the National Police Law, namely "Police are all matters relating to the functions and institutions of the police in accordance with statutory regulations". The role of the Police in dealing with criminal acts and law enforcement is clearly regulated in Article 2 of Law Number 2 of 2002, which states that "the function of the police is one of the functions of the State government in the field of maintaining public security and order, law enforcement, protection, care and service to the community". Based on the explanation of Article 2, the function of the police must pay attention to the spirit of upholding Human Rights, law and justice. However, many skimming cases that occur in the jurisdiction of the Riau Islands Regional Police, until now

[12]Barda Nawawi Arief, Mayantara Crime: Development of Cyber Crime Studies in Indonesia, Jakarta: RajaGrafindo Persada, 2019, p. 45.

there are still many that have not been able to be advanced to the investigation stage with various obstacles that make it difficult for investigators to uncover the perpetrators in the skimming cases, however until now investigators are still trying to collect evidence to uncover the criminal acts of the skimming perpetrators.

The efforts of the Riau Islands Regional Police in dealing with skimming crimes in the Riau Islands jurisdiction, especially by the Riau Islands Regional Police, are carried out through a comprehensive and integrated approach, including preemptive, preventive and repressive efforts.

This approach is part of a crime prevention strategy that focuses not only on enforcement but also on prevention and community development to minimize the occurrence of technology-based crimes. The efforts undertaken are as follows:

a. Law Enforcement Efforts (Repressive)

Repressive measures are steps taken to take action against perpetrators of skimming crimes through law enforcement. In this case, the Special Criminal Investigation Directorate (Ditreskrimsus) of the Riau Islands Regional Police plays a primary role in conducting inquiries and investigations into skimming cases. This process includes gathering evidence, examining witnesses and experts, conducting digital forensic analysis, and arresting and detaining the perpetrators. In practice, handling skimming cases requires specialized expertise in information technology, given that most of the evidence used is electronic data. Therefore, increasing the capacity of investigators in the field of digital forensics is crucial. Legally, skimming perpetrators can be charged under the provisions of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016, specifically regarding illegal access to electronic systems, as well as provisions in the Criminal Code regarding theft and fraud.

b. Technical and Systematic Prevention Efforts (Preventive)

Preventive efforts are focused on strengthening security systems and preventing crimes before they occur. In this regard, the police are collaborating with banks, the Financial Services Authority (OJK), and Bank Indonesia to improve banking system security, particularly at ATMs and electronic transaction systems. These preventive measures include routine patrols at ATM locations, monitoring suspicious activity in banking areas, and coordinating with banks to install CCTV cameras and fraud detection systems. Furthermore, the police are promoting the use of chip-based card technology, which is more secure than magnetic stripe technology, as part of an effort to close the gap for skimming crimes. In the context of the Riau Islands region, which directly borders other countries, preventive efforts also include monitoring the potential entry of transnational criminals, who are often involved in international skimming networks.

In its development, crime prevention efforts can be carried out using several approaches:

1. Social approach (social crime prevention), which emphasizes how the roots of crime can be eradicated so that the social life patterns of society change;

2. Situational crime prevention approach, which emphasizes how to reduce opportunities for the perpetrator committed a crime;

This prevention effort is seen as the most strategic crime prevention effort, playing a crucial role, and is considered more likely to be successful than implementing penal measures through the criminal justice system. In line with this, criminal policies implemented through the criminal justice system have failed to reduce or even eliminate the skimming crime that remains rampant in Indonesia.

Directly through outreach, social media, and digital campaigns. This step is crucial given that low digital literacy often creates loopholes for criminals to carry out their activities. By increasing public awareness, it is hoped that the potential for crime can be reduced early.

Based on the above description, it can be concluded that police efforts in the Riau Islands jurisdiction to combat skimming crimes have been carried out comprehensively through preemptive, preventive, and repressive approaches. However, in practice, various obstacles remain, such as limited human resources with technological expertise, limited facilities and infrastructure, and low public awareness of the risks of cybercrime. Therefore, strengthening institutional capacity, increasing cross-sectoral cooperation, and ongoing public education are needed to ensure more effective efforts to combat skimming crimes.

In practice, skimming involves installing a device on an ATM or electronic payment device to obtain data stored on the magnetic stripe of a customer's ATM or debit card. The obtained data is then transferred to another card (cloned card) and used to conduct unauthorized transactions or withdrawals. This act essentially constitutes illegal access to an electronic system aimed at gaining economic advantage at the expense of others. Therefore, skimming is not only a crime against property but also a crime against information security and electronic systems.[13]

---

[13] Law Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024, Article 30 paragraph (3).

Normatively, the construction of the crime of skimming can be found in the provisions of Article 30 paragraph (3) of Law Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024. This article states that any person who intentionally and without rights or unlawfully accesses a computer and/or electronic system with Any means by violating, breaking through, exceeding, or breaching the security system. This provision serves as the primary legal basis for prosecuting skimming perpetrators because the act of obtaining customer data is carried out through unauthorized access to legally protected electronic systems. In addition, the crime of skimming can also be linked to Article 32 paragraph (1) of the Electronic Information and Transactions Law which regulates the prohibition of changing, adding, reducing, transmitting, damaging, removing, moving, or hiding electronic information and/or electronic documents belonging to other people or the public without rights. In the context of skimming, customer data obtained illegally is electronic information that is protected by law so that any act of taking and using such data without permission is a form of violation of these provisions.[14]

Viewed from a general criminal law perspective, skimming is also related to the crime of theft as stipulated in Article 362 of the Criminal Code. Although the object taken is not a physical movable object, but rather electronic data that is then used to control the victim's funds, the substance of the act still contains elements of unlawful appropriation of another person's property. Technological developments have

This means that the objects of crime are no longer limited to tangible objects, but also include data and information of high economic value. Therefore, the modern criminal law approach recognizes that data theft resulting in financial loss can be viewed as a crime against property.[15]

The legal framework for skimming crimes has been further strengthened by the issuance of various regulations in the banking sector that mandate customer data protection and the security of electronic payment systems. Bank Indonesia and the Financial Services Authority (OJK) have issued various provisions concerning the implementation of information technology risk management, electronic transaction security, and consumer protection in the financial services sector. These regulations demonstrate that the state views skimming crimes as a serious threat to the stability of the financial system and public trust in the banking industry. In law enforcement practice, the criminal framework for

[14]Ibid., Article 32 paragraph (1).

[15]Adami Chazawi and Ardi Ferdian, Information Crime and Electronic Transactions Malang: Media Nusa Creative, 2015, p. 98.

skimming has been applied by the courts through various decisions, including Batam District Court Decision No. 569/Pid.Sus/2022/PN Btm. In this case, the defendant was found guilty of committing acts related to the acquisition and misuse of customer electronic data to obtain unlawful profits. The judge's reasoning indicated that these actions met the elements of a crime stipulated in the Electronic Information and Transactions Law because Unauthorized access to an electronic system that results in harm to another party. The ruling also confirms that Indonesian positive law has a sufficient normative basis for prosecuting skimming perpetrators, even though there are no specific regulations that explicitly use the term "skimming."

Based on this explanation, the criminal offense of skimming in Indonesian law is constructed through a combination of general criminal law norms and specific criminal law in the field of information technology. This construction shows that skimming is viewed as a form of cybercrime that contains elements of illegal access to electronic systems, misuse of electronic data, and unlawful control of another person's property. Therefore, law enforcement against the crime of skimming requires an approach that is oriented not only toward the protection of property but also toward the protection of electronic systems and data security as part of the legal interests that must be upheld by the state.

3.2. Effectiveness of Prevention and Handling of Skimming Crimes in the Jurisdiction of the Riau Islands Regional Police

1. Theory of Punishment Effectiveness

The effectiveness of prevention and mitigation can be measured by the extent to which the process is able to provide a real effect of reducing a skimming crime and no cases arising afterward, and the implementation of repressive measures reduces the number of cases through a deterrent effect. From the perspective of the legal system theory proposed by Lawrence M. Friedman, the effectiveness of law enforcement is influenced by three main elements: legal structure, legal substance, and legal culture. In the context of combating skimming in the Riau Islands region, these three elements have not been fully implemented optimally. The legal substance is actually quite adequate, but from the legal structure side there are still limitations in the capacity of law enforcement officers, while from the legal culture side, public awareness of data security is still relatively low. This imbalance causes skimming prevention efforts to not reach an optimal level of effectiveness.

In the theory of legal effectiveness, Lawrence M. Friedman previously argued that the legal system consisted of three main components, namely:

a. Substance (legal content), namely the applicable rules;

b. Structure (legal structure), namely law enforcement institutions;

c. Legal culture, namely the attitudes and behavior of society towards the law.[16]

The effectiveness of the law is determined by the extent to which these three components work harmoniously. In the context of this research, Law No. 19 of 2016 concerning Electronic Information and Transactions, as amended by Law No. 1 of 2024 concerning the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions, substantially regulates the legal mechanisms and consequences for committing skimming crimes. The effectiveness of preventing and overcoming skimming crimes in the jurisdiction of the Riau Islands Regional Police can essentially be seen from the extent to which efforts made by law enforcement officers are able to achieve legal objectives, namely providing protection to the community, creating a deterrent effect for perpetrators, and preventing similar crimes from occurring in the future. From the perspective of the theory of legal effectiveness, law enforcement is said to be effective if the applicable legal norms are able to be implemented optimally and complied with by the community.[17] In this context, the crime of skimming is part of the crime

Normatively, efforts to prevent and overcome skimming have a strong legal basis through Law Number 11 of 2008 concerning Electronic Information and Transactions as amended by Law Number 19 of 2016, which regulates illegal access to electronic systems and the protection of personal data of electronic system users.[18] Furthermore, provisions in the Criminal Code can also be used to prosecute skimming perpetrators through articles related to theft and fraud. With this legal basis, the police have strong legal legitimacy to enforce the law against skimming perpetrators. However, the effectiveness of law enforcement is determined not only by the existence of regulations, but also by other factors such as the legal structure and legal culture of the community.

The effectiveness of preventing and responding to skimming is a critical issue in the Indonesian criminal justice system. This is due to the lack of specific regulations governing skimming, which, in reality, is a crime with massive consequences.

2. Factors Influencing the Effectiveness of Prevention and Handling of Skimming Crimes.

---

[16]Lawrence M. Friedman, The Legal System: A Social Science Perspective, Russell Sage Foundation, New York, 1975, p. 15–16

[17]Soerjono Soekanto, Factors Influencing Law Enforcement, Jakarta: RajaGrafindo Persada, 2008.

[18]Law Number 11 of 2008 concerning Electronic Information and Transactions in conjunction with. Law Number 19 of 2016.

To measure the effectiveness of the law, it is necessary to first understand the theory of punishment. The role of punishment is a fundamental basis in criminal law, explaining the reasons and objectives of the state in imposing punishment on perpetrators of crimes. In criminal law literature, theories of punishment are generally divided into three: absolute theory, relative theory, and combined theory.[19]

a. Absolute Theory (Retaliation Theory)

Absolute theory views punishment as a form of retribution for the wrongdoing committed by the perpetrator. According to this theory, punishment is imposed solely because of the crime, without consideration for future social benefits.

b. Relative Theory (Objective Theory)

In contrast to absolute theory, relative theory views punishment as a means to achieve specific goals, such as crime prevention and offender rehabilitation. This theory encompasses general deterrence and special deterrence.

Speaking of prevention and mitigation, in practice, the police in the Riau Islands have demonstrated quite progressive measures, such as public awareness campaigns on skimming methods, increased ATM monitoring, and collaboration with banks to improve transaction security systems. These measures are part of a preventative effort aimed at eliminating opportunities for crime before it occurs. However, the effectiveness of these preventive measures still faces challenges, particularly related to the low level of digital literacy and a lack of awareness of the importance of maintaining personal data security. This situation leaves the public vulnerable to becoming victims of skimming crimes, despite various preventative measures being implemented.

Viewed from another perspective, police officers have also implemented repressive law enforcement efforts, particularly through the Special Criminal Investigation Directorate, which handles cybercrime. Handling skimming cases requires a different approach than conventional crimes, as it involves electronic evidence and digital analysis techniques. In several cases, police in the Riau Islands have successfully uncovered skimming networks, including those involving foreign actors.

This demonstrates that the police have the operational capability to handle these crimes. However, effective enforcement still faces challenges such as limited

[19] Andi Hamzah, Theory and System of Criminal Justice, Jakarta: RajaGrafindo Persada, 2014, p.19.

human resources with expertise in digital forensics, limited technological equipment, and the complexity of proving in the judicial process.[20]

The effectiveness of combating skimming is also greatly influenced by inter-agency coordination. Skimming crimes are not solely the responsibility of the police, but also involve the role of banks, financial services authorities, and other institutions related to financial systems and information technology. In this regard, cooperation between the police, banks, and regulators is key to creating an integrated security system. Despite this coordination, in practice, obstacles remain, such as slow information exchange, differing procedures between agencies, and a suboptimal integrated reporting and case handling system. In carrying out its function of maintaining public security and order, the Indonesian National Police (Polri) plays a vanguard role in creating a safe, orderly, and conducive social environment. This role is realized through patrols, securing vital objects, crowd control, and early detection of potential security disturbances. Through a preventive and preemptive approach, the Polri strives to prevent criminal acts before they occur.

Furthermore, the Riau Islands' geographical location, which is an archipelago and borders other countries, also poses challenges in combating skimming. This situation opens up opportunities for transnational criminals to enter and complicates monitoring and law enforcement. Therefore, a more comprehensive approach is needed, including increased international cooperation and strengthening surveillance systems in border areas. Therefore, it can be concluded that the effectiveness of skimming prevention and control within the jurisdiction of the Riau Islands Regional Police remains suboptimal, despite various normative and operational efforts. To increase this effectiveness, it is necessary to strengthen the capacity of law enforcement officers, improve public digital literacy, optimize inter-agency cooperation, and utilize more sophisticated technology to detect and prevent skimming. A holistic and sustainable approach is key to addressing the ever-evolving dynamics of cybercrime.

3.3. Obstacles Faced in Law Enforcement Against Perpetrators of Skimming Crimes and Strategic Solutions in Improving Prevention and Mitigation.

1. General Overview

Law enforcement against skimming crimes within the jurisdiction of the Riau Islands Regional Police faces various structural, substantial, and cultural obstacles. These obstacles relate not only to the technical aspects of law enforcement, but also to the rapid development of information technology and the complex and cross-border nature of cybercrime. From a law enforcement

[20] M. Yahya Harahap, Discussion of Problems and Application of the Criminal Procedure Code, Jakarta: Sinar Grafika, 2012.

theory perspective, these obstacles can be analyzed through factors influencing legal effectiveness, as proposed by Soerjono Soekanto: the law itself, law enforcement officers, facilities and infrastructure, society, and legal culture. Legal substance is the rules, norms, and patterns of human behavior that exist within the system. Substance also means the product in the form of regulatory decisions (statutory regulations) produced by the people within the system.[21] Legal substance or statutory restrictions can make it more difficult to combat ATM skimming crimes.

2. Obstacles to Law Enforcement Against Perpetrators of Skimming Crimes

Aggravated theft is a form of conventional crime that not only causes material harm to victims but also impacts the public's sense of security. To understand the causes of this crime, a criminological approach is crucial because it can explain the motives and factors underlying the perpetrator's deviant behavior. Based on this rationale, the solution formulated in this study is aimed at creating a law enforcement system that is not only effective in prosecuting perpetrators but also capable of providing protection, guidance, and guaranteeing a better future for children as the nation's next generation.

a. Limited Human Resources (HR)

One of the main obstacles to law enforcement against skimming is the limited human resources (HR) of police officers, particularly in the fields of digital forensics and information technology. Skimming crimes require specialized expertise in identifying skimming devices, analyzing electronic data, and tracing the perpetrator's digital footprint. However, not all law enforcement officers possess these competencies, resulting in technical difficulties in the investigation and prosecution process. Furthermore, limited facilities and infrastructure, such as digital forensics devices, are also a major obstacle.

digital forensics, data analysis software, and other supporting systems are also inhibiting factors in effectively uncovering skimming cases. Law enforcement is one of the most important pillars in the law enforcement process. If a regulation has been created very well but the quality of law enforcement is below standard, then it can still cause problems. Based on an interview conducted by the author with IPDA Esi Aryanto, SH (Panit I Unit I Subdit V Ditreskrimsus) member of the Riau Islands Police Chief, in the case of skimming crimes that also require the police to cooperate with banks, so they must go through a fairly challenging process due to legal limitations on bank secrecy. In this case, the bank may provide the police with access to customer information to assist the

[21] Hakim, Lukman. 2020. Principles of Criminal Law. Budi Utama, Yogyakarta

investigation.[22] However, the bank will only release the data after verifying that the customer is a victim of skimming and only after receiving an official request from the Chief of the Indonesian National Police.

b. The Complexity of Proof in Skimming Crimes

Different with crime conventional Which generally leaving physical evidence, skimming crimes are more common involving electronic evidence that requires special methods in collecting, securing, and presenting it in court. In this case, although the Criminal Procedure Code has provided a legal basis for evidence, regulations related to electronic evidence still need strengthening, as stipulated in Law Number 11 of 2008 concerning Electronic Information and Transactions, which has been amended by Law Number 19 of 2016. Often there is also the involvement of more than one perpetrator, thus complicating the investigation and inquiry process. In practice, this evidence process often requires expert testimony and coordination with other institutions, which can slow down the law enforcement process.

4. Conclusion

Based on the results of the discussion regarding "Police Efforts in Preventing and Handling Skimming Crimes in the Riau Islands Regional Police Jurisdiction" the following conclusions can be drawn: 1. That the implementation of law enforcement in the prevention and handling of skimming crimes carried out by the police has been carried out through a comprehensive approach, including preemptive, preventive, and repressive efforts. Preemptive efforts are carried out through education and socialization to the public regarding the modus operandi of skimming crimes, while preventive efforts are realized through cooperation with banking parties in improving transaction security systems and monitoring ATM machines. Repressive efforts are carried out through the process of investigation and inquiry against perpetrators of skimming crimes by referring to the provisions of Law Number 11 of 2008 concerning Information and Electronic Transactions as amended by Law Number 19 of 2016 and the provisions of the Criminal Code. 2. The effectiveness of combating skimming crimes in the Riau Islands region is generally still less than optimal. This is due to various factors affecting law enforcement, including limited human resources with expertise in digital forensics, limited supporting facilities and infrastructure, the complexity of electronic data-based evidence, and low levels of digital literacy. Furthermore, the transnational nature of skimming crimes also presents a barrier to law enforcement, necessitating more intensive cross-border cooperation.

---

[22] Interview with IPDA Esi Aryanto, SH (Head of Unit I, Sub-Directorate V, Directorate of Special Criminal Investigation) on April 7, 2026, at 10:00 WIB at the Riau Islands Regional Police Headquarters

5. References

Journals:

Amsari Damanik, Rini, D R. Sari, 2024. “Penegakan Hukum Pidana Terhadap Tindak Pidana Skimming” Journal of Law and Nation, Vol. 3 No. 1, hal. 89-97

Ardiko G.M. Sitompil, Haryadi, Tri Iman Munandar, 2020. “Penahanan Terhadap Anak Pelaku Tindak Pidana”, PAMPAS: Journal Of Criminal, Vol. 1. No. 3, hlm. 36.

Delphia, Risanti dan K, Harjono Maykada. 2021. Persepsi Masyarakat atas Perlindungan Data Pribadi. Survei Nasional Tahun 2021 Jakarta, Katadata Insight Centre, 36.

Depri Liber Sonata, 2014. “Metode Penelitian Hukum Normatif Dan Empiris: Karakteristik Khas Dari Metode Meneliti Hukum”, Fiat Justisia Jurnal Ilmu Hukum, Fakultas Hukum Universitas Lampung,Vol. 8, Nomor 1 Januari-Maret.

Enrick, Michael. 2019. “Pembobolan ATM Menggunakan Teknik Skimming Kaitannya Dengan Pengajuan Restitusi”. Jurist-Diction 2, No. 2 2019. 557-558.

Gunawan, Tri. 2023. “Rekonstruksi Regulasi Pertanggung Jawaban Bank Dalam Penerbitan Kartu Atm Nasabah Terhadap Kejahatan Card Skimming Berbasis Nilai Keadilan”. Tesis K Law Pustakawan 4 Unissula.

Laksana, Andri Winjaya. 2019. “Pemidanaan Cybercrime dalam Perspektif Hukum Pidana Positif”. Jurnal Hukum Unissula 35, No. 1, hlm 52.

Linggoraharjo, Victoria. 2020. Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming. Argumentum. Volume 7. Nomor 1. hlm. 40.

Modus dan karakteristik tindak pidana skimming; definisi dalam riset kriminal dan teknologi perbankan. Jurnal Ilmiah Mahasiswa, 2021. “Analisis Perilaku Skimming pada ATM”, Journal Unibos, Vol. 3 No. 2.

Moh Rosul, 2019. “Peranan Polri Dalam Penanggulangan Tindak Pidana Pencurian dengan Pemberatan” Dinamika Jurnal Ilmiah Ilmu Hukum. Vol. 25. No. 9.

Pamuji, Reza Aditya. 2018. "Perlindungan Hukum Bagi Nasabah dan Tanggung Jawab Bank Dalam Kasus Card skimming." Lex Renaissance 3.1, hlm. 12-12.

Wardani, Dian Eka Kusuma dan Maskun. 2019. “Kejahatan Skimming sebagai Salah Satu Bentuk Cyber Crime”. Jurisprudentie 6, No. 1, hlm. 168-169.

Widjojo,Hadi Widyopramono. 2005. Cybercrimes dan Pencegahannya, Jurnal HukumTeknologi, Fakultas Hukum Universitas Indonesia.

Books:

Abdul kadir Muhammad, Hukum dan Penelitian Hukum, Bandung : Citra Aditya Bakti, 2004.

Asafri Jaya Bakri, Konsep Maqashid Syariah Menurut Al-Syatibi, Jakarta: RajaGrafindo Persada, 1996.

Barda Nawawi Arief, Kebijakan Hukum Pidana, Bandung, Citra Aditya Bakti, 1996.

Chazawi Adami dan Ferdian Ardi, Tindak Pidana Informasi dan Transaksi Elektronik, Malang: Media Nusa Creative, 2015.

Chazawi Adami, Pelajaran Hukum Pidana, Bagian 1;Stelsel Pidana, Teori- Teori Pemidanaan dan Batas Berlakunya Hukum Pidana, PT. Raja Grafindo, Jakarta, 2002.

Didik M. Arief Mansur dan Elisatris Gultom, Cyber Law: Aspek Hukum Teknologi Informasi, Bandung: Refika Aditama, 2009.

Hakim, Lukman. Asas-asas Hukum Pidana. Budi Utama, Yogyakarta, 2020. Hermansyah, Hukum Perbankan Nasional Indonesia, Jakarta: Kencana, 2014.

Jasser Auda, Maqasid Al-Shariah as Philosophy of Islamic Law, London: The International Institute of Islamic Thought, 2008.

Jimly Asshiddiqie, Pengantar Ilmu Hukum Tata Negara, Jakarta: Rajawali Pers, 2010.

John Rawls, A Theory of Justice, Harvard University Press, Cambridge, 1971. Johnny Ibrahim, Teori & Metodologi Penelitian Hukum Normatif, Bayumedia, Malang, 2018.

Lawrence M. Friedman, Sistem Hukum Dalam Perspektif Ilmu Sosial, “The Legal System: A Sosial Science Perspektive”, Nusa Media, Bandung, 2019.

Lawrence M. Friedman, The Legal System: A Social Science Perspective, Russell Sage Foundation, New York, 1975.

M. Yahya Harahap, Pembahasan Permasalahan dan Penerapan KUHAP, Jakarta: Sinar Grafika, 2012.

Maskun. Kejahatan Siber Cyber Crime, Kencana Media, Jakarta. 2013.

Peter Mahmud Marzuki, Penelitian Hukum, Kencana, Jakarta, 2017. Ravena, Dey dan Kristian. Kebijakan Kriminal (Criminal Policy), Jakarta, Kencana, 2017.

Romli Atmasasmita, Sistem Peradilan Pidana Kontemporer, Jakarta: Prenadamedia Group, 2013.

Ronny Hanitijo Soemitro, Metodologi Penelitian dan Jur imetri, Jakarta: Ghalia Indonesia 1990.

Sadjijono, Hukum Kepolisian di Indonesia, Yogyakarta: LaksBang PRESSindo, 2008.

Satjipto Rahardjo, Ilmu Hukum, Citra Aditya Bakti, Bandung, 2020.

Wahbah Az-Zuhaili, Al-Fiqh al-Islami wa Adillatuhu, Jilid IV (Damaskus: Dar al-Fikr, 2004.

Wirdjono Prodjodikoro, Tindak Pidana Tertentu Di Indonesia, Rafika Aditama, Bandung, 2008.

Regulation:

Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions

Law Number 19 of 2016 concerning Electronic Information and Transactions.

Law Number 3 of 2004 concerning Amendments to Law Number 23 of 1999 concerning Bank Indonesia

Law Number 8 of 1999 concerning Consumer Protection Law Number 2 of 2002 concerning the National Police Republic of Indonesia

Law Number: 8 of 1981 concerning Criminal Procedure Law.

Regulation of the Chief of Police Number 22 of 2010 concerning Organizational Structure and Work Procedures at the Regional Police and Criminal Code Level, Directorate of Criminal Investigation

Regulation of the Chief of the Republic of Indonesia National Police Number 14 of 2018 concerning Organizational Structure and Work Procedures at the Regional Police Level.