Journal Equity of Law and Governance
Volume 8, Nomor 1, Page: 89-96
https://ejournal.warmadewa.ac.id/index.php/elg/index

Online ISSN 2776-5121
Print ISSN 2775-9512

https://doi.org/10.22225/elg.8.1.2026.89-96

Legal Regulations on Criminal Acts of Theft Using Skimming Systems in The Banking World Today

I Kadek Ari Putra[1], Ni Luh Made Mahendrawati[1], I Ketut Rai Setiabudhi[2], I Nyoman Gede Sugiartha[1]

1. Universitas Warmadewa, Denpasar, Bali, Indonesia
2. Universitas Udayana, Denpasar, Bali, Indonesia

Coressponding author;
I Kadek Ari Putra, Universitas Warmadewa, Denpasar, Bali, Indonesia
Email: kadekariputra31@gmail.com

Abstract. Indonesia is a country based on the rule of law that adheres to Pancasila and the 1945 Constitution, guaranteeing equality before the law for all citizens. However, advances in information technology, particularly in the banking sector, have given rise to serious challenges, including digital crime, particularly the theft of personal data through skimming methods. Skimming is a cybercrime and information technology crime in which a customer's ATM card data is illegally duplicated using specialised tools. Perpetrators then use this stolen data to access and drain customer funds. This banking crime is closely related to the Electronic Information and Transactions Law (EIT Law), specifically Articles 30 and 31, which regulate illegal access and interception of electronic systems. This study adopts a normative juridical method with a literature review approach, examining various legal materials. The focus of the study is on the legal regulations governing criminal skimming technology in the national banking system. The study's results show that, although the ITE Law has become the legal basis for prosecuting skimming, there remain structural weaknesses. These weaknesses stem from a lack of clarity in the definition and scope of the offence, which ultimately creates difficulties in consistently and fairly enforcing the law. The protection of customers' personal data is emphasised in ITE Law, which makes it part of the right to privacy that banks must guarantee. Skimming perpetrators can be prosecuted under the criminal provisions of ITE Law or under Articles 362 and 363 of the Criminal Code (KUHP) on theft.

Keywords: skimming; banking; cyber crime; electronic information and transactions law; criminal law

INTRODUCTION

Advances in information technology are currently occurring at a rapid pace and have become a fundamental part of modern life. The rapid increase in the use of information technology services has reinforced the crucial role of technology across various aspects of daily life, from the simple to the complex. (Pang et al., 2023). In fact, the advancement of information technology within a society is often used as a benchmark for the progress of civilisation. Information technology has penetrated various sectors, including tourism, where systems enable online storage, processing, and financial transactions, bringing significant changes across many areas of life. (Deputat et al., 2024).

The development of information technology services has dramatically influenced the banking sector, a vital business that collects and distributes public funds, including through the issuance of non-cash payment instruments. Banks continue to innovate to facilitate customer access to services, now driven by the public's preference for digital or online transactions. (Kumari & Devi, 2022). The adoption of this advanced technology has led to e-banking and

systems such as automated teller machines (ATMs), which now replace traditional tellers, transforming banking services into something more accessible, driven by the increase in internet users and the pandemic. (Burkul & Patil, 2024).

Information technology has now entered various sectors, including tourism. This system can store, retrieve, modify, process, and conduct financial transactions online, and advances in information technology can bring significant changes across various fields. The tourism sector has great potential to develop as a source of income for a region, as it not only benefits the tourist destination itself but also the local community involved, including the management of tourist attractions, crafts, and culinary arts. (Bakalo et al., 2025). It is undeniable that people nowadays prefer online payment methods, thereby creating opportunities for irresponsible individuals to commit crimes. Although E-Banking offers convenience, this innovation also carries significant risks in the form of cybercrime, which is growing alongside it. Technological sophistication. These banking crimes aim to steal account and credit card information, and even hack into bank database systems. (Patil & Shekokar, 2023). One specific form of increasingly sophisticated cybercrime is skimming, which involves stealing debit/credit card data using secretly installed devices. (Sujatha et al., 2025). This crime not only harms individual customers but also disrupts public safety and risks damaging the image of a tourist destination.

Advances in banking technology have given rise to various forms of cybercrime, one of which is skimming, which steals customer data through electronic devices. This challenge is primarily rooted in the definition and legal limitations of the Electronic Information and Transactions Law, which create inconsistencies in distinguishing specific cybercrimes (such as skimming and hacking) from ordinary theft and raise philosophical dilemmas about justice and the protection of individual rights in the digital age. (Ngcece & Mkhize, 2023).

This situation underscores the urgency of conducting an in-depth analysis of banks' responsibilities and the role of the law in protecting and providing justice for victims of skimming. (Nola et al., 2021). The theft of customers' personal information poses a major threat and can result in significant losses; the confidentiality of this data must be protected in accordance with banking principles and the Electronic Information and Transactions Law. (Garg & Gupta, 2025). Therefore, it is necessary to formulate more detailed and targeted legal norms to accommodate technological advances and enhance the security of digital transactions, thereby protecting tourists, maintaining the tourism sector's reputation, and ensuring the sustainability of the banking system.

This study takes as its starting point the crucial issue of regulatory inconsistency, particularly between criminal law and financial sector regulations (Menz, 2024). The lack of synergy between these regulations is a significant obstacle that hinders the consistency and effectiveness of officials in enforcing the law, making an in-depth analysis urgent. Furthermore, there are no clear legal guidelines for banks to follow when investigating skimming cases.

METHOD

Crimes in the banking sector that utilise information technology are highly varied. Still, in this study, the author will focus on analysing the legal regulations governing theft involving skimming systems in the current banking context. In normative legal research or literature studies, data collection methods are carried out through literature studies of various legal sources, including primary, secondary, and tertiary legal sources, as well as non-legal sources. The data collected is then processed and analysed to answer the questions at hand.

DISCUSSION

Legal Regulations on Information Technology Criminal Theft Using Skimming Systems in the Banking World Today

To explain what is meant by banking crime, various terms are used in theory. These terms include banking crime, crime in the banking sector, crime against banking, banking criminal acts, criminal acts in the banking sector, criminal acts against banking, and various other terms.(Thalib et al., 2025).

According to Kristian, these terms are grouped into two categories. The first category consists of criminal acts in the banking sector, defined as crimes against banks or criminal acts against banks. (de Souza & de Souza, 2024). The second group consists of banking offences, which encompass the meaning of the term banking crime explained earlier. The term banking crime needs to be distinguished from the term crime related to the banking sector. Banking crime is a violation of banking regulations that is punishable by criminal sanctions under the Banking Law, Law No. 7 of 1992, as amended by Law No. 10 of 1998 on Banking. (Sulistyandari et al., 2024).

Crimes in the banking sector refer to acts related to basic banking operations, which are punishable under criminal law outside the Banking Act or relevant legislation. According to Sutherland, white-collar crime is generally defined as criminal acts committed by individuals with good reputations and high social positions in their fields of work. (Evans, 2023). Criminal offences in the banking sector are a type of economic crime, namely conventional offences that seek to gain profit through economic motives such as theft, embezzlement, robbery, fraud, and other offences related to banks. The crime of skimming customer money is a type of cybercrime. Cybercrime is a crime committed in cyberspace, using information and communication technology as a tool. (Lee et al., 2023).

Previously, the terms "hacker" and "cracker" referred to individuals with specialised skills who could gain access to computer systems for various purposes. Now, however, many tools and systems have been created that can operate independently to carry out different forms of intrusion and system destruction. Essentially, attacks on information system security within organisations are now considered criminal acts in both criminal and civil contexts. Although most of these criminal acts are related to financial issues, such attacks often also result in loss of life, especially when they target systems that are critical to human life. In general, four types of activities can be classified as crimes in the field of information technology. The first is wiretapping, which is the act of listening to or intercepting communications between two parties. In accordance with Indonesian regulations, only certain state institutions or other parties authorised by law, such as the Indonesian National Police, the State Intelligence Agency, and the Corruption Eradication Commission, are permitted to conduct wiretapping. The second is interruption, which is the act of causing communication between two parties that should be established to be interrupted. One example of an attack that disrupts a computer system is Denial-of-Service (DoS) or Distributed Denial-of-Service (DDoS). The third is modification, which is the act of changing data or information (Mishra & Dharmavaram, 2025). or information that moves through an information technology system without the permission of the sender or recipient. Web defacement is one form of attack that can be categorised as a type of crime. The fourth is fabrication, the act of deceiving someone into believing that a request for interaction is coming from an individual, now better known as phishing. When considering how it works, skimming refers to the activity of illegally copying data from the magnetic strip of credit cards or ATM/debit cards. This indicates that skimming is an act in which the perpetrator attempts to steal information from the magnetic strip of ATM/debit cards by illegal means, enabling the perpetrator to gain control of the victim's account.

The above skimming behaviour constitutes illegal access to another party's computer or information system with the intent to steal personal data contained therein. This act is classified as a criminal offence in the field of information and electronic transactions, which prohibits any individual from deliberately and without authorisation or unlawfully accessing a computer or electronic system in any way, in order to obtain electronic information or documents, as stipulated in Article 30(2) of Law No. 19 of 2016 amending Law No. 11 of 2008 on Information and Electronic Transactions, commonly referred to as the ITE Law. (Shubham et al., 2023).

More specifically, Article 30 paragraph 2 of the ITE Law states that "Any individual who deliberately and without permission or illegally enters a computer and/or electronic system by any means to obtain electronic information and/or electronic documents."

Any action is punishable if it meets the criminal requirements listed in the alleged article. In Article 30, paragraph 2 of the ITE Law above, it can be seen that the criminal elements include:

1. The element of fault is intent.

2. The element of unlawfulness is without authorisation or contrary to legal provisions.

3. The element of action is accessed by various means.

4. The element of the object is a computer and/or electronic system.

5. The objective is with the intent to obtain electronic information and/or electronic documents. (Setyaningrum et al., 2022).

Skimming is a method used by criminals in the banking sector to steal customer data stored on ATM cards. The modus operandi involves attaching a skimming device to the ATM card slot. ATMs are electronic devices or electronic systems used in banking activities. (Sujatha et al., 2025).

Skimmer is not a tool used by skimming perpetrators. Perpetrators often also use spy cameras to observe customers' finger movements as they enter their ATM card PIN. However, spy cameras are now rarely used as skimming devices become increasingly sophisticated. The website How Stuff Works reports that there are now types of skimmers capable of reading ATM card PIN codes. Moreover, these skimmers can directly send the obtained data to the perpetrators via SMS. Here is a systematic overview of how skimming perpetrators operate: Criminals look for ATM machines that are targets for skimming devices. What they want are ATM machines that are unguarded, quiet, and without CCTV surveillance.

Criminals began stealing customer information by attaching skimming devices to ATM card slots.

Using skimming devices, criminals can duplicate the magnetic strip data on ATM cards and then transfer this information to blank ATM cards. This process can be done manually, in which the perpetrator returns to the ATM to retrieve the prepared data chip. However, if the perpetrator uses a more sophisticated skimming device, the collected data can be accessed from any location. In general, this data is sent via text message.

Crimes involving the theft of customer funds through skimming are also classified as violations in the banking sector. In this context, skimming refers to the copying of ATM cards. As explained earlier, ATM cards are copied by installing a skimming device in the card slot and a hidden camera above the trusted buttons. The purpose of installing a skimmer is to capture the electronic information stored on the magnetic strip of the customer's ATM card. Meanwhile, the hidden camera serves to capture each customer's PIN number. After successfully collecting this data, a new card is made by duplicating the information obtained, so the perpetrator can immediately use the fake ATM card without the customer's knowledge.

Before installing skimming devices, criminals observe behaviour in the area around ATMs. They hope that the skimming devices they install will collect a lot of customer information, so they choose ATMs that are frequently used for transactions but have low surveillance or where people around them appear busy and indifferent. Skimmers often target ATMs in tourist areas because of the high activity and the indifference of those around them. Shopping centres are also very attractive to criminals for installing skimming devices, given the high frequency of transactions. In fact, ATMs targeted by skimming criminals can even be located in quiet places. Skimming attacks occur in a short period of time, generally around one or two hours. Although the time is short, the losses customers can incur can amount to hundreds of millions or even billions of rupiah if many transactions occur at the ATM where the device is installed. For banks with advanced technology and regular monitoring of ATM machines, skimming incidents can be identified immediately. Banks in this category can detect skimming within 3 to 4 hours. Although detected quickly, the losses can be enormous.

Crime through skimming techniques has long been prevalent in the banking world. The method of hacking ATM cards using skimming techniques was first uncovered in 2009 at a Citibank ATM in Woodland Hills, California. At that time, skimming was carried out using a device installed in the ATM machine slot where the ATM card is inserted, known as a skimmer. It works by exploiting data from the magnetic stripe on the customer's ATM card. However, with the advancement of modern information technology, skimming methods have also become more sophisticated, using GSM or WIFI technology. This allows perpetrators to operate and access customer data from locations far from the ATM, even from other countries.

Banking crimes involving skimming have caused significant losses to the banking sector. The victims are not only customers who have lost money from their savings accounts due to skimming, but also the banks themselves. Skimming crimes have eroded customer trust in banks. Of course, this cannot be ignored; a comprehensive solution from all stakeholders is needed to address cybercrime in the banking sector.

Because skimming falls under the category of cybercrime, which is multi-dimensional and not bound by space or time, it must be handled with a comprehensive and sustainable approach, in line with ongoing advances in information and communication technology.

Since skimming is a multidimensional cybercrime that is not bound by space or time, it must be addressed with a comprehensive, sustainable approach, in line with ongoing advances in global information and communication technology.

- Changes to national criminal law and procedures in line with international agreements relevant to such crimes.
- Improving the quality of computer network security at the national level in line with international standards.
- Strengthening the knowledge and capabilities of law enforcement officials regarding the prevention, investigation and prosecution of cases related to cybercrime.
- Raising public awareness about the dangers of cybercrime and the importance of preventing such incidents.
- Deepening collaboration between countries in the field of technology-related cybercrime offences.

The Law on Electronic Information and Transactions regulates various aspects of the application of information technology and electronic transactions, including the protection of personal data and criminal acts related to information technology. This is controlled in Law Number 1 of 2024, articles 30 and 32 concerning Electronic Information and Transactions. Legal Aspects: Perpetrators may be subject to sanctions in accordance with the provisions of the Electronic Information and Transactions Law, particularly the articles governing illegal

acts in the use of electronic information. For example, Article 30 governs illegal access to electronic systems. Evidence Aspect: In a legal context, electronic information obtained through skimming can be used as evidence. The Electronic Information and Transactions Law stipulate that electronic documents have the same legal force as physical documents, as long as they meet specific requirements. Responsibility: According to the Electronic Information and Transaction Law, perpetrators of criminal acts are responsible for all legal consequences of their actions. If data theft causes losses to customers or banks, perpetrators may be subject to criminal and civil penalties. Criminal sanctions are punishments imposed by the government on individuals found to have committed a criminal offence (crime or violation of the law). The main objectives of criminal sanctions are to punish the perpetrator, prevent future criminal offences, reform the perpetrator's behaviour, and deter the community. In criminal acts involving the theft of customer personal data, the customer's personal data is certainly the object. In Indonesia, regulations concerning personal data are implicitly set out in Law Number 19 of 2016, which amends Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law).

In Indonesia, regulations concerning Personal Data are implicitly set out in Law Number 19 of 2016, which amends Law Number 11 of 2008 regarding Electronic Information and Transactions (ITE Law). Crimes that violate privacy or personal data are regulated in the Electronic Information and Transactions Law (EIT Law), and the following is an explanation of the penalties for theft: "Any illegal act of accessing an electronic system with the intention of obtaining Electronic Information or Documents through means that violate the security system is considered a criminal act under Article 31 of the EIT Law. Perpetrators can be charged under the Criminal Code (KUH Pidana) and the Electronic Information and Transactions Law. Several judges presiding over skimming cases have sentenced perpetrators under Articles 362 and 363(1)(4). They have also applied Article 31 of Law No. 19 of 2016, which amends Law No. 11 of 2008 on Electronic Information and Transactions.

CONCLUSION

This study offers in-depth insights into the challenges and opportunities the banking sector faces in addressing cybercrime threats, with a particular focus on skimming. Rapid growth in information technology has created an environment rich in innovation and progress in the banking sector, enabling financial institutions to offer more efficient and convenient services to customers. However, behind these advances lie significant risks, with cybercriminals exploiting loopholes and weaknesses in existing security systems. By understanding these dynamics, this study aims to identify strategic measures that banking institutions can take to strengthen customer data protection and prevent skimming practices, thereby maintaining public trust in the banking sector in this digital age.

The current legal system is often out of step with technological developments, creating legal uncertainty that can be exploited by criminals. This study shows that the legal definitions and boundaries in ITE Law need to be clarified in order to distinguish specific cybercrimes from conventional offences. In addition, synergy between laws governing financial and criminal matters must be improved to create a comprehensive, responsive framework for emerging threats. The handling of skimming cases, which is a form of cybercrime that harms many customers, still faces significant normative obstacles. One of the main issues is the lack of specific, comprehensive regulations to address this problem. Although the Electronic Information and Transactions Law (ITE) and the Banking Law already exist, neither provides clear regulations on the technical mechanisms needed to prevent and combat skimming. In addition, the protection of customers' personal data has not been comprehensively regulated, leaving loopholes for criminals to misuse sensitive information. In this context, it is crucial to

develop more detailed regulations to protect customers and provide legal certainty in addressing the ever-evolving practice of skimming.

In addition to regulatory considerations, customer education and awareness also play a crucial role in creating a secure transaction environment. The public needs adequate knowledge of the potential risks associated with digital transactions, as well as guidance on steps to protect their personal data. In this case, financial institutions have a responsibility to convey information and provide relevant training to customers actively. They must educate customers about safe and effective transaction practices in this ever-evolving digital era. With a proactive approach, it is hoped that customers will be better prepared to face potential threats and more confident in conducting online transactions.

ACKNOWLEDGMENT

Praise and thanks be to God Almighty for His mercy and grace, so that this research entitled "Legal Regulations on Criminal Acts of Theft Using Skimming Systems in the Banking World Today" can be completed correctly and on time.

REFERENCES

Bakalo, N., Makhovka, V., Krekoten, I., Glebova, A., & Kulakova, S. (2025). Local tourism as financial and economic development driver of the community: Management aspect. *World Development Perspectives*, *38*, 100693. https://doi.org/10.1016/j.wdp.2025.100693

Burkul, T. S., & Patil, S. (2024). A Comprehensive Examination of Biometric ATM Operations Involving Fingerprint and Face Recognition Using Deep Learning. *2024 Second International Conference on Advances in Information Technology (ICAIT)*, 1–8. https://doi.org/10.1109/ICAIT61638.2024.10690458

de Souza, M. C. S., & de Souza, R. S. (2024). Law enforcement, social demands and reputation risks as drivers of compliance functions: a comparative analysis of the largest banks' disclosures in the UK and Brazil. *Crime, Law and Social Change*, *81*(3), 255–280. https://doi.org/10.1007/s10611-023-10116-8

Deputat, M., Podolian, M., Zhupnyk, V., Terletska, K., & Gorishevskyy, P. (2024). Evolution of information systems and technologies in the hospitality and tourism sector: a historical perspective. *Multidisciplinary Science Journal*, *6*, 2024ss0729. https://doi.org/10.31893/multiscience.2024ss0729

Evans, L. (2023). Representations of white collar crime in the Caribbean. *Organised Crime, Financial Crime, and Criminal Justice*, 160–176. https://doi.org/10.4324/9781003020813-10

Garg, N., & Gupta, K. (2025). Data privacy in online banking using blowfish algorithm: A review. In *Progressive Computational Intelligence, Information Technology and Networking* (pp. 888–891). CRC Press. https://doi.org/10.1201/9781003650010-145

Kumari, A., & Devi, N. C. (2022). The Impact of FinTech and Blockchain Technologies on Banking and Financial Services. *Technology Innovation Management Review*, *12*(1/2). https://doi.org/10.22215/timreview/1481

Lee, S.-H., Kang, I., & Kim, H.-W. (2023). Understanding cybercrime from a criminal's perspective: Why and how suspects commit cybercrimes? *Technology in Society*, *75*, 102361. https://doi.org/10.1016/j.techsoc.2023.102361

Menz, M. (2024). Evidencing source of wealth–challenges, questions, solutions and recommendations. *Journal of Money Laundering Control*, *27*(1), 171–180. https://doi.org/10.1108/JMLC-02-2023-0041

Mishra, O., & Dharmavaram, V. G. (2025). Toward an Intelligent Cybersecurity System. In *The Techno-Legal Dynamics of Cyber Crimes in Industry 5.0* (pp. 43–54). Wiley. https://doi.org/10.1002/9781394242177.ch3

Ngcece, S., & Mkhize, S. M. (2023). An Exploratory Study of the South African Police Services (SAPS) Systems in Combating Cybercrime. In *Cybercrime and Challenges in South Africa* (pp. 159–175). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-3057-9_7

Nola, S., Basri, S. Z., & Nur Hafiza, S. (2021). Legal Protection For Customer Of Bankrupt Rural Bank (BPR) In Indonesia. *Jurnal Hukum Bisnis Bonum Commune*, 109–118. https://doi.org/10.30996/jhbbc.v4i1.4485

Pang, B., Chen, T., & Dai, M. (2023). *Analysis on the Development of Visual Communication Design Under the Innovation of Information Technology* (pp. 535–543). https://doi.org/10.1007/978-3-031-29097-8_63

Patil, S., & Shekokar, N. M. (2023). A Study of Recent Techniques to Detect Zero-Day Phishing Attacks. In *Intelligent Approaches to Cyber Security* (pp. 71–83). Chapman and Hall/CRC. https://doi.org/10.1201/9781003408307-7

Setyaningrum, W., Morana, A. C., Vaizi, K. N., Damarina, R., Akbar, S. A., & Oktasari, S. (2022). Anticipation of the ITE Law and Reconciliation of Its Forms Freedom of Expression through the E-Hights Website. *Jurnal Hukum Novelty*, *13*(2), 266. https://doi.org/10.26555/novelty.v13i2.a23799

Shubham, Kumar, R., Aditya, A., & Shivahare, B. D. (2023). Cyber Crime Prevention and Techniques: A Comprehensive Survey. *2023 3rd International Conference on Innovative Sustainable Computational Technologies (CISCT)*, 1–4. https://doi.org/10.1109/CISCT57197.2023.10351225

Sujatha, G. M., Rahman, F. A., Dhanalaskhmi, J. G. S., Chandru, S. K., & Srinivasan, V. (2025). *ATM skimming device detection using IOT*. 030001. https://doi.org/10.1063/5.0254592

Sulistyandari, S., Afwa, U., Sutrisno, P. A., & Nordin, R. (2024). Implementation of Prudential Banking Principles: State Responsibility in Combating Banking Crimes in Indonesia. *Volksgeist: Jurnal Ilmu Hukum Dan Konstitusi*, 341–359. https://doi.org/10.24090/volksgeist.v7i2.12132

Thalib, P., Kurniawan, F., Maghfirah Salsabila, S., & Kholiq, M. N. (2025). Legal Framework and Employee Liability in Banking Compliance and Crime Prevention: The Case Analysis of Indonesia. *Yustisia Jurnal Hukum*, *13*(3), 298. https://doi.org/10.20961/yustisia.v13i3.93370