



# **ANALYSIS OF PAYMENT SYSTEM SUPERVISION AND CUSTOMER PROTECTION FROM CARD SKIMMING (CASE STUDY AT THE REPRESENTATIVE OFFICE OF BANK INDONESIA OF NORTH SUMATRA)**

**Muti Audilla<sup>1</sup>, Ratna Dina Marviana<sup>2</sup>, Lukman Hakim Siregar<sup>3</sup>,  
M. Amri Nasution<sup>4</sup>,**

Dharmawangsa University<sup>1234</sup>

Email : [mutiaudilla2@gmail.com](mailto:mutiaudilla2@gmail.com)<sup>1</sup>, [ratnadinamarviana@dharmawangsa.ac.id](mailto:ratnadinamarviana@dharmawangsa.ac.id)<sup>2</sup>,  
[lukman.fe@dharmawangsa.ac.id](mailto:lukman.fe@dharmawangsa.ac.id)<sup>3</sup>, [m.amrinasution@dharmawangsa.ac.id](mailto:m.amrinasution@dharmawangsa.ac.id)<sup>4</sup>

## ABSTRACT

The development of information technology, especially in the field of online payments, has changed the way people conduct financial transactions. The advent of e-banking allows customers to conduct various banking transactions without having to go to a bank or ATM. This certainly makes the transaction process more efficient and effective, providing tremendous convenience for customers. However, despite the convenience, e-payment systems also carry great risks, especially in relation to the threat of cybercrime, such as card skimming. This crime occurs when a perpetrator steals a customer's ATM card data through a device installed on an ATM machine, which is then used to access and withdraw funds illegally. Although various related regulations have been implemented. This paper aims to find out the provisions of Bank Indonesia to keep the payment system safe and efficient, the challenges in dealing with cyber risks remain large. Therefore, it is important for every party, both banks and customers, to continue to increase awareness of the potential threat of cybercrime. In this regard, Bank Indonesia, as the payment system regulator in Indonesia, plays an important role in regulating and ensuring that the payment system operates in accordance with the principles of security, efficiency, equality of access, and consumer protection. Overall, while progress has been made in securing payment systems and electronic transactions, challenges remain. Bank Indonesia, together with banking institutions and the public, needs to continue to strengthen supervision, technology, and education efforts to ensure the security of transactions in the banking world. The protection of customers should always be the top priority, by ensuring that the payment system implemented is always safe and efficient. With more intensive measures, such as the use of advanced technology, strict supervision, and close collaboration between related parties, it is hoped that the potential for cybercrime can be minimised, and the public can enjoy safe, convenient, and reliable banking services.

Keywords: BI, Banking, ATM and EDC Machines, Card Skimming, Customers

## ABSTRAK

Perkembangan teknologi informasi, terutama di bidang pembayaran online, telah mengubah cara orang melakukan transaksi keuangan. Munculnya e-banking memungkinkan pelanggan untuk melakukan berbagai transaksi perbankan tanpa harus pergi ke bank atau ATM. Ini tentu saja membuat proses transaksi menjadi lebih efisien dan efektif, memberikan kenyamanan yang luar biasa bagi pelanggan. Namun, meskipun ada kenyamanan, sistem pembayaran elektronik juga membawa risiko besar, terutama terkait dengan ancaman kejahatan siber, seperti skimming



kartu. Kejahanan ini terjadi ketika pelaku mencuri data kartu ATM pelanggan melalui perangkat yang dipasang pada mesin ATM, yang kemudian digunakan untuk mengakses dan menarik dana secara ilegal. Meskipun berbagai peraturan terkait telah diterapkan. Makalah ini bertujuan untuk mengetahui ketentuan Bank Indonesia dalam menjaga sistem pembayaran agar tetap aman dan efisien, tantangan dalam menghadapi risiko siber tetap besar. Oleh karena itu, penting bagi setiap pihak, baik bank maupun pelanggan, untuk terus meningkatkan kesadaran akan potensi ancaman kejahanan siber. Dalam hal ini, Bank Indonesia, sebagai regulator sistem pembayaran di Indonesia, memainkan peran penting dalam mengatur dan memastikan bahwa sistem pembayaran beroperasi sesuai dengan prinsip-prinsip keamanan, efisiensi, kesetaraan akses, dan perlindungan konsumen. Secara keseluruhan, meskipun kemajuan telah dicapai dalam mengamankan sistem pembayaran dan transaksi elektronik, tantangan masih ada. Bank Indonesia, bersama dengan lembaga perbankan dan masyarakat, perlu terus memperkuat upaya pengawasan, teknologi, dan pendidikan untuk memastikan keamanan transaksi di dunia perbankan. Perlindungan pelanggan harus selalu menjadi prioritas utama, dengan memastikan bahwa sistem pembayaran yang diterapkan selalu aman dan efisien. Dengan langkah-langkah yang lebih intensif, seperti penggunaan teknologi canggih, pengawasan ketat, dan kolaborasi erat antara pihak-pihak terkait, diharapkan potensi kejahanan siber dapat diminimalkan, dan masyarakat dapat menikmati layanan perbankan yang aman, nyaman, dan andal.

*Kata Kunci: BI, Perbankan, Mesin ATM dan EDC, Skimming Kartu, Pelanggan*

## 1. INTRODUCTION

Card skimming has become a serious threat to the global banking system, including in Indonesia. Card skimming is a crime committed by using electronic devices installed on ATM machines, EDCs, or other payment terminals. The device is used to copy important data on the magnetic tape or chip of credit and debit cards without the knowledge of the card owner. Once the card data has been stolen, the perpetrator can utilise the information to make illegal transactions, such as cash withdrawals or online purchases. This crime has grown alongside the rapid use of electronic payment technology, making it an easy target for criminals who continue to innovate their skimming techniques.

In many cases, banks have focused on their own policies and actions to prevent or address card skimming. However, in this context, it is imperative to examine how Bank Indonesia, as the regulatory authority of the payment system and banking sector in Indonesia as outlined in the Bank Indonesia Law (PBI) No.22/23/PBI/2020 on Payment Systems that came into effect on 1 July 2021 plays a role in regulating policies that can help prevent and handle card skimming cases. As well as having the authority to formulate policies, Bank Indonesia plays an important role in setting security standards that banks and other financial institutions in Indonesia must adhere to. And it must implement stricter protection measures for customer data and electronic transactions.



## **2. LITERATURE REVIEW**

For literature related to this research, the author uses as a basis literature as a basis for understanding the use of modelling in the research method to be used. One of them is presented by Ahmad Fauzi (2004) [1], Linda (2024) [2], Victoria Linggoraharja (2020) [3]. The three researchers conducted a study related to the payment system and customer protection in Indonesia, with the main focus on the role of Bank Indonesia in regulating and supervising the banking sector. The results of their research can be concluded that the payment system is a series of regulations and infrastructure used to facilitate the exchange of economic value between two parties with the aim of avoiding direct payment obligations. Bank Indonesia has a very important role in regulating and supervising the payment system in Indonesia, including the infrastructure that supports it such as ATM networks, debit cards, and internet banking services. Bank Indonesia ensures that financial institutions participating in the payment system meet the set standards, as well as granting licences to institutions that meet the criteria to operate in the payment system. Thus, Bank Indonesia functions not only as a supervisor, but also as a facilitator that maintains the smoothness, security, and efficiency of the payment system in Indonesia.

### **Definition of Surveillance and Payment System**

According to Usman Effendi (2017: 138) argues that supervision is the most essential management function, no matter how good the work activities are without the supervision of the work cannot be said to be successful. Meanwhile, according to Irham Fahmi (2018: 138) says that supervision can generally be defined as a way for an organisation to achieve effective and efficient performance.

Bank Indonesia Regulations (PBI) and Laws (UU) regulate customer supervision which includes preventing and dealing with payment system problems and development in the financial sector (PPSK Law).

#### **Types of Supervision**

1. Preventive Control
2. Corrective Control
3. Direct and Indirect Supervision

#### **Monitoring Function**

According to Julina (2018: 72), the supervisory function is the identification of various factors that hinder activities, and taking the necessary corrective actions so that goals can be achieved. This function is needed to ensure that what has been planned and organised can run well. In more detail, the supervisory function is defined as a systematic effort in setting performance standards and various predetermined goals.

#### **Payment System**

According to Booth, in "Financial Markets, Institutions, and Money" (2018), states that a payment system is a set of mechanisms used to move money and settle financial obligations. The system includes various payment instruments and institutions that enable transactions between individuals and organisations. According to Bank Indonesia (BI), the payment system is the entire mechanism used to transfer funds or payment instruments from one party to another in order to conduct transactions, whether in the form of money transfers, bill payments, or other transactions. Bank Indonesia as the payment system authority in Indonesia has a role in regulating, supervising, and facilitating the smooth



running of the payment system. Bank Indonesia plays a role in monitoring the policies of the payment system, namely security, efficiency, equal access and consumer protection:

### **Definition, Techniques, How Skimming Works**

Skimming is the act of stealing customer data by installing data recording devices, generally carried out on Automated Teller Machines (ATMs) and Electronic Data Capture (EDC) machines whose function is to duplicate or copy customer personal data, and then the personal data is misused by irresponsible people. In running the skimming method, there are skimmers, hidden cameras and keypads. The skimmer tool functions to record customer activity in using an ATM machine, this tool is able to record electromagnetic strips and record customer finger movements when entering the pin on the victim's card when the card is inserted into the ATM machine. The hidden camera is used to record the victim's activity when inputting the PIN on the ATM machine. or even more sophisticated is the replacement of the keypad on the ATM machine and EDC machine by the perpetrator so that the customer's pin will be recorded automatically when the customer presses the keypad.

#### **A. Skimming Technique**

The perpetrator installs a small device called a skimmer in the ATM or POS card reader slot. These devices look similar to the real thing and often go unnoticed by users. When the card is inserted, the skimmer reads the data on the card's magnetic tape, such as the card number and card owner information. or Installing a fake keypad that functions to record the pin combination entered by the customer. after obtaining customer data and customer pin, the next process in the number of the perpetrator makes a fake electronic card that is made by himself by entering customer data that has previously been obtained.

#### **B. How Skimming Works**

1. Card Alteration Method, which is to use the original electronic card that has been the data is changed. This process is done by heating the relief on the electronic card, then filling the card with the customer's personal data (re-encoded). (reembossed), then filling the card with the customer's personal data (re-encoded).
2. The Total Counterfeiting Method is the creation of a completely fake electronic card. This process involves printing a card that closely resembles the original e-card, complete with images, logos, and numbers, making it look like the real thing. This process includes embossing and encoding.
3. The White Plastic Card Method is the manufacture of electronic cards using a plain white plastic card. This process only involves encoding, because the counterfeit card is only processed based on data without falsifying the physical form. is only processed based on data without falsifying the physical form of the card.

### **Definition of Bank Products ATM and EDC Machine**

Automatic Teller Machine or Automatic Teller Machine (ATM) is a Self Service Terminal specially made to serve customers in conducting banking transactions that can be done at any time, is one of the bank's services.

which is based on electronic channels with the aim that customers can transact like in a branch office using a machine.



Electronic Data Capture (EDC) is a device used by merchants to accept payments from customers using credit cards, debit cards, prepaid cards, and QRIS. This EDC machine is equipped with a scanner that reads the magnetic stripe or chip on the card and sends the payment information to the card issuing bank. Your payment transaction can be done in real time with the linked account. These EDCs are usually used by shops, restaurants, and other businesses that accept card payments.

### **Protection of Customers from Card Skimming**

Customer protection is all efforts that ensure legal certainty to provide protection to consumers. This is in accordance with Bank Indonesia Regulation number 22/20/PBI/2020 concerning Consumer Protection Bank Indonesia needs to adjust to the development of consumer protection principles. which refers to the principles of equality and fair treatment, openness, education and literacy, and protection of consumer information data.

## **3. DATA ANALYSIS AND RESEARCH TECHNIQUES**

This research is Descriptive Qualitative, which is research that describes, analyses events more thoroughly and in detail.

### **Data Analysis**

The analysis process begins with reviewing all available data from various sources, namely interviews, observations, official documentation, drawings, photos, then summarising the core, process, and statements that need to be maintained (Rasimin, 2018).

#### **1. Pre-Field Analysis**

Qualitative research has conducted data analysis before entering the field. Analysis is carried out on data from preliminary studies, or secondary data. However, the focus of this research is still temporary, and continues to develop after the researcher enters and during the field.

#### **2. Data Analysis While in the Field**

The qualitative research process after entering the field, begins with determining a key informant "key informant" who is the right informant and in accordance with the research we are researching. After that the researcher can conduct interviews with these informants, and take notes, and record the results of the interview. after that the researcher asks several questions that are appropriate to the object of research, continued by analysing the results of the interviews that had been conducted with the results of the informants' answers. So the research process starts from something broad, then scaled down. In this study, researchers will interview the right informants, informants who know exactly about the payment system in the banking world, so that it will make it easier to question and examine a problem that has been identified. relating to the crime of skimming.

### **Research Techniques**

#### **1. Observation**

According to Sugiyono (2018: 229) observation is a data collection technique that has specific characteristics when compared to other techniques. Observation is also not limited to people, but also other natural objects. Through observation, researchers can learn about behaviour and the meaning of that behaviour. Observation in this study is by observing an object under study either directly or indirectly by involving all the senses to.

#### **2. Interview**



According to Bungi (2018, 133) interviews are a technique of obtaining information for research purposes by means of question and answer while meeting face to face between the interviewer and the interviewee, through dialogue both orally and in writing. Interviews will be conducted with the fields concerned with the problems that occur. occurred. In this case the researcher uses a structured interview method, namely an interview in which the form of questions is registered which has been compiled beforehand.

### 3. Documentation

According to Sugiyono (2015) Documentation is a data collection technique that is carried out by searching and collecting documents related to research problems. These documents can be in the form of notes, reports, books, photographs or recordings that already exist and can be used to explore research topics.

## 4. RESULTS AND DISCUSSION

a. Supervision of the payment system from card skimming by Bank Indonesia North Sumatra has gone well?

## Indonesia North Sumatra has been running well?

Bank Indonesia again urges the public to continue to maintain prudence in the use of non-cash transactions and urges Banks to continue to educate customers. For the convenience of the community, non-cash transaction facilities continue to be expanded to cover various transaction activities, including to help the community's homecoming activities. Bank Indonesia continues to educate the public on the dangers that threaten the payment system. "One of the obstacles faced by Bank Indonesia is the limited scope of its coverage, because Bank Indonesia only has one branch in each province, while the number of banks is quite large. Therefore, Bank Indonesia conducts education by involving banks to help socialise information to customers. As institutions that are directly responsible for customers, banks have an obligation to educate customers about the products and services they offer. Bank Indonesia can provide socialisation, but since Bank Indonesia branches are limited and cannot reach all customers in each province, the main responsibility for education remains with the banks themselves.

With reference to reports that some customers at certain banks have experienced unauthorised withdrawals from their accounts, Bank Indonesia offers the following information:

1. Bank Indonesia is currently co-ordinating with the banks involved and Police Department to put an immediate end to this criminal activity.
2. Preliminary investigation results show that ATM card data theft occurs through skimming and PIN monitoring by unauthorised parties. In response, the relevant banks have taken the necessary security measures.
3. Bank Indonesia has requested that all banks re-evaluate and examine their ATMs, including EDC (Electronic Data Capture) devices, across all locations and traders to ensure no more abuse occurs
4. Bank Indonesia also urged bank customers to pay attention to their surroundings when using ATMs and EDC machines and checking carefully that there are no additional equipment attached to the machine in question.





**INTERNASIONAL CONFERENCE & CALL FOR PAPER**

**ECONOMICS, BUSINESS, INNOVATION AND CREATIVITY (EBIC), 30<sup>th</sup> April 2025**

Vol: 2

No.: 1

No. E-ISSN: 3025-4086

Figure 1. Bank Indonesia's Policy on the Implementation of the Latest Chip

Based on the above statement, it can be concluded that prior to the implementation of chip technology from magnetic stripe, the bank had taken various precautions to protect customer data, such as installing keypad protectors, anti-skimmer devices, and optimising surveillance through CCTV at ATM machines.

b. The role of Bank Indonesia in providing protection for customers from card skimming in North Sumatra Province is effective?

card skimming in North Sumatra Province is it effective?

The various facilities and diversity of payment system services followed by an increase in transactions in payment system services certainly have consequences not only for consumers but also for organisers and authorities in the payment system sector. Consumers want accurate and clear information about the benefits and risks of payment system services. This is necessary to reduce the risks that may arise in using payment system services. "Some of the problems faced by customers are:

1. Privacy
2. Copying Data
3. Smart Customer

Bank Indonesia established a division that specifically handles Consumer Protection of Payment System Services, namely the Payment System Consumer Protection Division which was established on 1 August 2013. The establishment of this division was motivated by the increasing transactions in the payment system and as a form of concern for all payment system consumers and Bank Indonesia also has PBI No.16/1/PBI 2014 concerning Consumer Protection / Payment System customer service division. The functions of this division are education, consultation and facilitation.

Bank Indonesia is also accelerating the implementation of chip card usage to avoid skimming cases in the future. The use of chip technology and 6-digit PIN is intended to improve transaction security, mitigate the risk of fraud, and align the implementation of debit and credit cards with international best practices. The use of chip technology will allow customers to make safer and more convenient transactions without fear of data duplication. Previously, ATM cards were vulnerable to counterfeiting and data duplication, known as skimming, where data stored on the magnetic stripe is copied by a skimmer installed at the EDC. The data stored on the skimmer can then be used to create another card that can be used in the same way as the original. If we do not act quickly to eradicate this criminal behaviour, it could erode public confidence in the ATM card industry.

Bank Indonesia has taken comprehensive measures to address and prevent skimming cases. They utilise Machine Learning technology to analyse transaction data and detect suspicious activity, and monitor ATM devices and EDC machines to identify illegal skimming devices. In addition, regulation and supervision of financial institutions were strengthened, with an emphasis on implementing stricter security procedures and the use of encryption technology to protect transaction data. Bank Indonesia is also actively educating the public on the potential dangers of skimming and how to protect personal information. Cooperation with the police and the Financial Services Authority (OJK) is also conducted to follow up on skimming cases and ensure the security of the payment system is maintained.

Follow-up of Complaint Handling Bank Indonesia follows up on complaints by Education Consultation and Facilitation, in the following manner:

1. Any consumer complaint that is submitted via email or telephone to Bank Indonesia's contact centre.



2. Consumer complaints that are submitted by mail or have fulfilled the requirements to be followed up

## 5. CONCLUSION

Based on the description of several chapters on "Supervision conducted by Bank Indonesia in the Payment System and Customer Protection from Card Skimming Actions", several conclusions can be stated as follows:

1. Payment system supervision against card skimming at Bank Indonesia North Sumatra, although supervision has been running well, there are still some aspects that need to be improved. Supervision of the payment system, including cooperation with banks and the police, has been effective in responding to skimming. However, customer education and equitable application of security technology need to be improved. Bank Indonesia has also implemented Machine Learning technology to detect suspicious transactions and skimming devices in real-time. While this technology is effective, the protection of customers' personal data remains a top priority. Overall, despite the progress, strengthening education, technology, and more intensive supervision are still needed to prevent skimming in the future.

2. The protection of customers from card skimming in North Sumatra has been effective, however, there are still challenges that need to be overcome. Bank Indonesia has implemented preventive measures, such as public education, provision of complaint channels, and establishment of Payment System Consumer Protection Division. However, the main obstacle is the limited reach of education through only one branch per province, and the need for increased collaboration with banks to educate customers more fully. Although security measures and policies, such as the use of chip cards and anti-skimming devices, have been implemented, more even-handed supervision and higher public awareness are still needed. Therefore, further collaboration between Bank Indonesia, banks, and the public is key to reducing the risk of future skimming crimes and improving customer protection.

## REFERENCES

Abdussamad, Z. (2022). Qualitative Research Methods Book.

Andi Prastowo, Qualitative Research Methods in Research Design Perspective, Bandung: Alfabeta, 2018.

Arief Budiono, Application of Sharia Principles in Islamic Financial Institutions. *Journal of Law and Justice* Vol.2 No.1, 2017

Asmaaysi, Alifian. (2022). Tasks, Objectives and Roles of Bank Indonesia. Jakarta 2023.

Christiani, T. A. (2016). Bank Indonesia and the Financial Services Authority in Legal Perspective.

Ghalib, v. P. (2018). Implementation of bank indonesia regulation number 16/1/pbi/2014 concerning consumer protection of payment system services at pt bank bca tbk padang (doctoral dissertation, andalas university).

Atmaja, Y. S., & Paulus, D. H. (2022). Participation of Bank Indonesia in Regulating the Digitalisation of the Indonesian Payment System. *Legal Issues*, 51(3), 271-286.

Damayanti, A. D., Irgeuazzahra, A., Fitria, A., & Tarina, D. D. Y. (2024). The role of bank indonesia in banking fraud cases. *Journal de Facto*, 10(2), 228-247.

Faridi, M. K. (2019). Cyber Crime in the Banking Sector. *Cyber Security and Digital Forensics*, 1(2), 57-61.

Fauzi, A., Widayati, E., Sasmita, M., Maulana, R., Aulia, T., & Herdinov, A. (2023). The



role of Bank Indonesia in regulating and maintaining a smooth payment system. *Journal of Accounting and Business Management*, 3(1), 80-89.

Febrinda, R. R., & Ningsih, R. (2023). Readiness of Digitalisation of Non-Cash Payment System in People's Market. *Journal of Economics and Public Policy*, 13(2), 87-100.

Kusuma, M. J., & SH, M. (2019). Bank customer protection law: Legal efforts to protect bank customers against ITE crimes in the banking sector. Nusamedia.

Nasution, A. M., & Suprayitno, E. (2022). The effect of e-banking usage and customer protection on customer trust with financial literacy as a moderating variable. *Scientific Journal of Islamic Economics*, 8(2), 1205-1213.

Ningsih, L. W., Astuti, R. P., Holisah, S. N., Amin, M. S., & Yunus, M. (2024). Development of Payment System in Indonesia: Policy and Role of Bank Indonesia. *Journal of Digital Economics and Business*, 1(4), 697-702.

Financial Services Authority (OJK), Wise eBanking, Jakarta, 2015.

Setiawan, D. A. (2018). The Development of the Modus Operandi of Skimming Crimes in Bank ATM Machine Break-ins as a Form of Cybercrime. *Era Hukum - Scientific Journal of Legal Sciences*, 16(2).

Sumbodo, M., & Fernal, J. O. (2019). Skimming, how it works and prevention at ATMs. *IKRA-ITH Technology Journal of Science and Technology*, 3(2), 11-16.

Surach Winarni, S. H. (2017). Legal Protection for Customers and Bank Responsibility for Customers who Experience Losses (Case Study of Theft of Customer Deposit Funds with Card Skimming Mode).

Tarigan, H. A. A. B., & Paulus, D. H. (2019). Legal Protection of Customers on the Implementation of Digital Banking Services. *Journal of Indonesian Legal Development*, 1(3), 294-307.

Utomo, R. P., Idayanti, S., & Widyastuti, T. V. (2023). Banking Efforts in Resolving Card Skimming. NEM Publisher.

Indonesia, B. (2011). Bank Indonesia Regulation. Retrieved September, 15, 2017.

Indonesia, B. (2004). Regulation of Bank Indonesia number: 6/10/PBI/2004 on the health rating system of commercial banks. Bank Indonesia Regulation.