Multidisciplinary Output Research For Actual and International Issue (MORFAI Journal) ISSN (e): 2808-6635
Volume 6 No. 5 (2026)

LEGAL LIABILITY OF BANKS FOR CUSTOMER LOSSES RESULTING FROM SKIMMING FROM THE PERSPECTIVE OF ELECTRONIC TRANSACTION SECURITY

Aditya Tri Hardiyawan[1], Sanusi[2], Soesi Idayanti[3]
[1,2,3]Master of Laws Program, Universitas Pancasakti Tegal
E-mail: gazzam149@gmail.com

Received : 20 June 2026   Accepted : 11 July 2026
Revised : 29 June 2026   Published : 27 July 2026

Abstract

Banks are among the financial institutions that play a highly significant role in a country's economy. Their function as both custodians of funds and financial intermediaries is widely recognized as beneficial to society and the business sector. Today, convenience and transaction speed have become key priorities for banks in delivering services to their customers. Various banking services have adopted information technology that has become an integral part of everyday use, including online banking services, Automated Teller Machine (ATM) networks, Electronic Data Capture (EDC) networks, phone banking services, internet banking services, credit card services, installment card services, and other deferred payment facilities. This study aims to examine the legal liability of banks for customer losses resulting from skimming from the perspective of electronic transaction security. The research employs a library research method. The approach adopted in this study is a normative legal approach. The primary legal materials consist of statutory regulations with binding legal force, including: Law Number 10 of 1998 concerning Banking; Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016; Law Number 8 of 1999 concerning Consumer Protection; and Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector. In fulfilling their legal responsibility and providing services to customers to prevent skimming, banks have adopted security technologies such as two-factor authentication (2FA), data encryption, and biometric authentication (such as fingerprint and facial recognition) to enhance the protection of customer data and transactions. In addition, banks comply with policy directives issued by the Indonesian banking authorities by adhering to the applicable regulatory framework to ensure legal certainty and customer satisfaction.

Keywords: Legal Liability, Banking, Skimming, Electronic Transactions

INTRODUCTION

Banks are among the financial institutions that play a highly significant role in a country's economy. Their role as custodians of funds and financial intermediaries provides substantial benefits to both the public and the business sector. Today, convenience and speed of transactions have become key elements in the services banks provide to their customers. Modern banking services offer various conveniences that enable customers to conduct transactions anytime and anywhere, without limitations of distance, space, or time. The use of online systems supported by banking technology allows customers to perform banking transactions without having to visit a bank branch (Adam C, 2015). Several banking services currently utilise information technology that has become an integral part of everyday life, including online banking services, Automated Teller Machine (ATM) networks, Electronic Data Capture (EDC) networks, phone banking services, internet banking services, credit card services, installment card services, and other deferred payment facilities. Among these, the online banking service most frequently used by customers is the ATM. This is due to the convenience it offers, including ease of access to banking services, flexible service hours, speed and accuracy of transactions, service security, and the wide range of services available. Furthermore, customers can conveniently perform various banking activities without visiting a branch office, such as checking account balances, making payments for telephone bills, credit card bills, electricity, water, mobile phone services, and tuition fees, purchasing airline tickets, topping up mobile phone credit, transferring funds between accounts (open transfer), and changing their Personal Identification Number (PIN) (Dian Ekawati, 2018). Cases of skimming are among the most commonly encountered forms of electronic transaction fraud today. This is attributable to the widespread use of card-based electronic transaction media, including ATM/debit cards and credit cards. According to data presented on a website by Adhi Maulana at http://money.howstuffworks.com/atm-skimming.htm, in 2008, global losses resulting from crimes involving ATM cards alone reached USD 1 billion, equivalent to IDR 9 trillion (IDR 9,000 billion), based on an exchange rate of IDR 9,000 per USD. The Bank Tech website explains that the technique of compromising customers' ATM cards through skimming was first identified in 2009 at a Citibank ATM in Woodland Hills, California. The skimming technique involved attaching a device known as a skimmer to the ATM card slot. Its modus operandi was to clone data stored on the magnetic stripe of the customer's ATM card (Adhi Maulana, Liputan6.com: 2014). In 2010, various print and electronic media reported incidents of fraud involving ATM/debit cards. The majority of these fraud cases were committed using the skimming method, whereby customer data stored on the card was stolen. These incidents highlighted not only the need for issuers to strengthen the security of ATM/debit card systems but also the importance of customers exercising due diligence when conducting financial transactions using ATM/debit cards.

METHOD

This study employed normative legal research using a library research method. Normative legal research was selected because the study focuses on examining legal norms governing bank liability for customer losses resulting from skimming from the perspective of electronic transaction security. The research relied on secondary data obtained through literature studies.

The legal approach applied in this research consisted of the statutory approach and the conceptual approach. The statutory approach involved analysing relevant legislation, including Law Number 10 of 1998 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection, Law Number 11 of 2008 concerning Electronic Information and Electronic Transactions as amended by Law Number 19 of 2016, Financial Services Authority Regulation Number 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector, and other relevant legal provisions. The conceptual approach was used to examine legal doctrines and theories concerning legal liability, consumer protection, banking law, and electronic transaction security.

The legal materials used in this research consisted of primary, secondary, and tertiary legal materials. Primary legal materials comprised statutory regulations related to banking, consumer protection, and electronic transactions. Secondary legal materials included books, scientific journals, legal commentaries, and previous research relevant to the subject matter. Tertiary legal materials consisted of legal dictionaries, encyclopaedias, and other supporting references that facilitated the interpretation of legal concepts.

Data collection was conducted through a literature review by systematically identifying, collecting, and examining relevant legal materials. The collected legal materials were subsequently analysed using a qualitative juridical analysis through descriptive-analytical methods. The analysis was carried out by interpreting applicable legal provisions and legal doctrines to evaluate the extent of banks' legal liability in protecting customers against losses caused by skimming and to formulate legal conclusions consistent with the applicable regulatory framework.

RESULTS AND DISCUSSION

Legal Liability of Banks for Customer Losses Resulting from Skimming from the Perspective of Electronic Transaction Security

The development of the digital era has progressed rapidly, and this transformation has also occurred within the banking sector. Financial services in Indonesia have become increasingly accessible, with the digitalisation of transaction systems becoming an inseparable component of modern banking operations. The use of mobile banking, internet banking, and Automated Teller Machines (ATMs) has enabled customers to access banking services conveniently at any time and from any location (Nur Rofi, 2026).

Skimming crimes frequently occur without the knowledge of the customers themselves. Customers generally become aware of skimming only after the funds in their accounts have been depleted, demonstrating the vulnerability of both legal and technological data protection within the banking sector. Banks, as financial institutions, have a legal obligation and responsibility to safeguard customers' personal data. Furthermore, as financial intermediaries, banks play a crucial role in supporting national development. Banks collect funds from the public and redistribute them in the form of loans or financing to stimulate economic growth. Therefore, the stability of and public confidence in the banking system must always be maintained. If skimming crimes continue to occur without adequate legal protection and a clear mechanism of liability, public trust in the national banking system may decline, which could ultimately disrupt broader economic stability.

From a juridical perspective, the protection of customers as consumers of financial services has been regulated under various statutory provisions, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998 concerning Banking, and Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016. In addition, the supervision of financial service institutions is carried out by the Financial Services Authority (Otoritas Jasa Keuangan/OJK), which is authorised to ensure the security and consumer protection of the financial services sector. In practice, disputes frequently arise regarding banks' liability for losses suffered by victims of skimming. Victims are often required to undergo lengthy procedures to obtain reimbursement of their lost funds, and there are cases in which the allocation of responsibility between the bank and the customer becomes a matter of dispute. This raises questions concerning the effectiveness of the existing legal protection and the appropriate mechanism of legal liability that should be implemented.

According to Philipus M. Hadjon, legal protection fundamentally constitutes an effort to preserve and respect human dignity while recognising the fundamental rights possessed by every legal subject under statutory regulations, thereby protecting them from arbitrary actions. Furthermore, legal protection may also be understood as a set of legal norms designed to safeguard particular interests against potential violations by other parties. In the context of consumer protection, legal protection therefore refers to the legal guarantees provided to protect the rights of customers or consumers from suffering losses and to ensure that those rights are properly fulfilled.

Within the modern banking system, banks are obligated to provide protection for customers' funds and personal data in every banking transaction, including ATM transactions and electronic banking (e-banking) services. This obligation arises from the legal relationship between the bank as a financial service provider and the customer as a consumer of banking services. In this context, the security of transaction systems constitutes a fundamental responsibility of banks in maintaining public confidence in the banking system. The legal basis for banks' liability for customer losses resulting from skimming offences can be found in several statutory regulations. First, Law Number 10 of 1998 concerning Banking stipulates that banks are required to conduct their business activities in accordance with the prudential principle and are responsible for maintaining public confidence in the banking system (Law Number 10 of 1998 concerning Banking, 1998, Article 29 paragraph (2)). This prudential principle includes the obligation of banks to ensure the security of their operational systems, including electronic transaction systems such as ATMs and e-banking.

With respect to legal liability, banks fundamentally have an obligation to protect customers' funds and personal data as a consequence of the legal relationship between the bank and its customers. Where customer losses are proven to have resulted from skimming crimes attributable to weaknesses in the bank's security system or deficiencies in its supervisory mechanisms, the bank may be held liable to provide compensation. Dispute resolution mechanisms may include submitting a complaint to the bank, mediation facilitated by the Financial Services Authority (OJK), settlement through alternative dispute resolution institutions, or litigation before the courts. Accordingly, legal protection for customers who become victims of skimming is, in principle, already available within the Indonesian legal system. Nevertheless, its effectiveness still requires further strengthening in terms of implementation, regulatory oversight, and public awareness regarding the security of digital transactions.

CONCLUSION

In fulfilling their legal responsibility and providing services to customers to prevent skimming, banks have adopted security technologies such as two-factor authentication (2FA), data encryption, and biometric authentication (such as fingerprint and facial recognition) to enhance the protection of customer data and transactions. In addition, banks comply with policy directives issued by the Indonesian banking authorities by adhering to the applicable regulatory framework to ensure legal certainty and customer satisfaction. From a juridical perspective, the protection of customers as consumers of financial services has been regulated under various statutory provisions, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998 concerning Banking, and Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016.

REFERENCES

Adam Chazawi. Tindak Pidana Informasi dan Transaksi Elektronik. Malang: Media Nusa Creative, 2015.

Adhi Maulana. "Begini Cara Kerja Pembobolan Kartu ATM dengan Metode Skimming." https://www.liputan6.com/tekno/read/2049670/begini-cara-kerja-iskimmingi-kartu-atm.

———. "Mengenal Modus Pembobolan ATM Melalui Teknik Skimming." https://www.liputan6.com/tekno/read/2302264/mengenal-modus-pembobolan-atm-melalui-teknik-skimming.

Budi Suhariyanto. Tindak Pidana Teknologi Informasi (Cybercrime): Urgensi Pengaturan dan Celah Hukumnya. Jakarta: Rajawali Press, 2013.

Cahyadi, Ketut Partha, and A.A.A. Ngr. Sri Rahayu Gorda. "Perlindungan Hukum Terhadap Nasabah dari Ancaman Kejahatan Perbankan Skimming Melalui Layanan Electronic Banking (Studi Kasus di Bank Rakyat Indonesia)." Jurnal Analisis Hukum 2, no. 1 (2019): 173.

Dian Alan Setiawan. "Perkembangan Modus Operandi Kejahatan Skimming dalam Pembobolan Mesin ATM Bank sebagai Bentuk Kejahatan Dunia Maya (Cybercrime)." Vol. 16, No. 2, 2018.

Dian Ekawati. "Perlindungan Hukum Terhadap Nasabah Bank yang Dirugikan Akibat Kejahatan Skimming Ditinjau dari Perspektif Teknologi Informasi dan Perbankan." Unnes Law Review 1, no. 2 (2018): 159. https://review-unes.com/index.php/law/article/view/24/15.

Hermansyah. Hukum Perbankan Indonesia. Revised Edition. Jakarta: Kencana, 2009.

Indrajit, Eko Richardus. Keamanan Teknologi Informasi dan Internet. Jakarta: EKOJI Preinexus, 2013.

J. Robberl. Teori Kriminologi: Konteks dan Konsekuensi. Jakarta: Kencana, 2015.

Jovin Ganda Ramdhan, and Sumiyati. "Perlindungan Hukum Nasabah Korban Skimming Ditinjau dari Undang-Undang Nomor 8 Tahun 1999." Mimbar Keadilan 12 (2019): 85.

Kansil, C.S.T. Pengantar Ilmu Hukum dan Tata Hukum Indonesia. Jakarta: Balai Pustaka, 1989.

Kelsen, Hans. Teori Hukum Murni. Translated by Rasul Mutaqien. Bandung: Nuansa & Nusa Media, 2006.

Kusuma, Mahesa Jati. Hukum Perlindungan Nasabah Bank: Upaya Hukum Melindungi Nasabah Bank terhadap Tindak Kejahatan ITE di Bidang Perbankan. Bandung: Nusa Media, 2012.

———. "Perlindungan Hukum Terhadap Nasabah Bank yang Menjadi Korban Kejahatan ITE di Bidang Perbankan." Al' Adl 5, no. 9 (2013): 38. https://ojs.uniska-bjm.ac.id/index.php/aldli/article/view/188/181.

Linggoharjo, Victoria. "Tanggung Jawab Kejahatan Perbankan Melalui Modus Operandi Skimming." Magister Hukum Argumentum 7, no. 1 (2020): 34. https://media.neliti.com/media/publications/339486-tanggung-jawab-kejahatan-perbankan-melal-557e7cc7.pdf.

Mansur, M. Arief, and Elisatris Gultom. Urgensi Perlindungan Korban Kejahatan (Antara Norma dan Realita). Jakarta: PT RajaGrafindo Persada, 2006.

Muchsin. Perlindungan dan Kepastian Hukum bagi Investor di Indonesia. Surakarta: Universitas Sebelas Maret, 2003.

Rahardjo, Satjipto. Ilmu Hukum. Bandung: Citra Aditya Bakti, 2012.

Ridwan HR. Hukum Administrasi Negara. Jakarta: Rajawali Pers, 2016.

Salim HS, and Erlies Septiana Nurbani. Penerapan Teori Hukum pada Penelitian Disertasi dan Tesis. Buku Kedua. Jakarta: Rajawali Pers, 2009.

Setiono. Rule of Law (Supremasi Hukum). Surakarta: Program Pascasarjana Magister Ilmu Hukum Universitas Sebelas Maret, 2004.

Youky Surinda. "Konsep Tanggung Jawab Menurut Teori Tanggung Jawab dalam Hukum." http://id.linkedin.com (accessed March 21, 2022).

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen.

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016.

Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Kitab Undang-Undang Hukum Perdata (KUHPerdata).