Journal of Digital Law and Policy
Volume 5 Number 3, May 2026
e-ISSN 2808-3458 p-ISSN 2808-3652
https://ejournal.sidyanusa.org/index.php/jdlp/en

Bank Liability to Customers in Cases of Skimming and Account Break-Ins Civil Law Perspective

Manggasali R. Nurul[1], Wutwensa M. Bruri[2], Hattu Y. Yakoba[3]

[1,2,3]*Biak-Papua College of Law, Biak, Indonesia*

Email: [1]*rahmadiniulluk@gmail.com*

Received on	*Revised on*	*Accepted on*
26 10 2025	*31 03 2026*	*30 04 2026*

Abstract

This study aims to analyze the legal liability of banks toward customers who suffer losses caused by skimming and account breaching, and to axime the extent to wich Indonesia's positive law provides legal protection for customers. This research uses a normative legal method with statutory and conceptual approaches through library research. Data were collected from laws and regulations, legal literature, journals, and relevant court decisions. The result show that skimming and account breaching are cybercrimes that directly cause finansial losses to customers. Bank liability can be claimed through breach of contract (*wanprestasi)* and unlawful act (*perbuatan melawan hukum*) as regulated in the Indonesia Civil Code, as well as under the Banking Law and the Consumer Protection Law. Meanwhile, the ITE Law provedis criminal sanstions for perpetrators of cybercrime. However, in practice, legal protection for customers remains ineffective. The Selayar District Court Decision No.30/Pid.Sus/2019/PN.Slr shows that although perpetrators may be punished, customer compensation must still be pursued through civil proceedings or consumer protection mechanisms. This indicates a gap between legal norms and their implementation in practice.

Keywords: *Legal liability, bank, customers, skimming, account breaching, civil law.*

INTRODUCTION

The rapid advancement of digital technology has significantly transformed the banking sector, enabling customers to conduct financial transactions through automated teller machines (ATMs), internet banking, mobile banking, and other electronic platforms. While these innovations have improved efficiency and accessibility, they have also increased the vulnerability of banking systems to cybercrime[1]. Among the most common forms of cybercrime affecting banking customers are skimming and account break-ins. Skimming involves the unauthorized acquisition of customer banking information through electronic devices attached to ATMs or payment terminals, whereas account break-ins generally occur through unauthorized access to customer accounts using stolen credentials, phishing techniques, malware, or other cyber intrusion methods. These crimes frequently result in substantial financial losses for customers and may undermine public confidence in banking institutions. Considering that banking activities fundamentally rely on public trust, any failure to provide adequate protection for customer funds and personal data raises important legal questions regarding the responsibility of banks as providers of financial services[2].

In Indonesia, various legal instruments have been enacted to regulate banking activities and protect customer interests, including Law Number 10 of 1998[3] concerning Banking, Law Number 8 of 1999 concerning Consumer Protection[4], Law Number 19 of 2016 concerning Electronic Information and Transactions[5], and several regulations issued by the Financial Services Authority (OJK) and Bank Indonesia. These regulations impose obligations on banks to maintain secure systems, protect customer information, and provide legal remedies when customers suffer losses. However, practical challenges continue to arise in determining the extent of bank liability when cybercrime is committed by third parties. Banks frequently argue that losses resulting from skimming or account break-ins are caused by external criminal actors rather than institutional negligence[6]. On the other hand, customers often contend

---

[1] M. Yusuf Samad and Pratama Dahlian Persadha, "Memahami Perang Siber Rusia Dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman Siber Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats," Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi 24, no. 2 (2022): 135–46, http://dx.doi.org/10.17933/iptekkom.24.2.2022.135-146.

[2] Wahyu Avianto et al., "Determinants of Digital Bank Transformation: A Systematic Literature Review with Prisma and Bibliometrics," JPPI (Jurnal Penelitian Pendidikan Indonesia) 10, no. 4 (November 2024): 296–307, https://doi.org/10.29210/020243553.

3 Undang-Undang (UU) Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan (1998), https://peraturan.bpk.go.id/Details/45486/uu-no-10-tahun-1998?utm_source=chatgpt.com.

4 Undang-Undang (UU) Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen (1999).

5 UU Informasi Dan Transaksi Elektronik (2016).

[6] Tamás Oroszi et al., "Whole Body Vibration Ameliorates Anxiety-like Behavior and Memory Functions in 30 Months Old Senescent Male Rats," Heliyon 10, no. 4 (February 2024): e26608, https://doi.org/10.1016/j.heliyon.2024.e26608.

that banks have failed to implement adequate security measures to prevent such incidents. Consequently, disputes regarding compensation and legal accountability remain a recurring issue within Indonesia's banking sector[7].

Previous studies have generally examined cybercrime in banking, customer protection, or banking liability as separate legal issues. Nevertheless, limited attention has been devoted to a comprehensive analysis that integrates civil liability principles, consumer protection regulations, banking law, and cyber law in assessing bank responsibility for losses arising from skimming and account break-ins. This gap becomes increasingly important as digital banking services continue to expand and cyber threats become more sophisticated. Therefore, this study aims to analyze the civil legal liability of banks toward customers who suffer losses due to skimming and account break-ins, as well as to examine the adequacy of Indonesia's positive legal framework in providing legal protection and remedies for affected customers. Through a normative legal analysis of relevant legislation, legal doctrines, and judicial decisions, this study seeks to contribute to the ongoing discourse on strengthening customer protection and enhancing accountability within Indonesia's digital banking environment[8].

METHODS

This study employs a normative legal research method, focusing on the examination of legal norms governing bank liability in cases of skimming and account break-ins. Normative legal research is appropriate because the study seeks to analyze legal principles, statutory regulations, and legal doctrines that determine the responsibilities of banking institutions toward customers who suffer losses due to cybercrime. The research adopts both a statutory approach and a conceptual approach. The statutory approach examines relevant legal instruments, including the Indonesian Civil Code, Law Number 10 of 1998 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning Electronic Information and Transactions, as well as regulations issued by the Financial Services Authority (OJK) and Bank Indonesia. Meanwhile, the conceptual approach is utilized to explore theories of legal liability, consumer protection, fiduciary relationships, and risk management within the banking sector.

7 Eka Ari Endrawati, Diah Turis Kaemirawati, and Susetya Herawati, "Perlindungan Hukum Sebagai Upaya Meningkatkan Kepercayaan Masyarakat Terhadap Perbankan: Studi Kasus Kejahatan Perbankan Di Indonesia," Binamulia Hukum 13, no. 2 (December 2024): 589–602, https://doi.org/10.37893/jbh.v13i2.945.

8 Geraint Howells and Stephen Weatherill, Consumer Protection Law, 2nd ed. (Routledge, 2017), https://doi.org/10.4324/9781315259512.

The research relies exclusively on secondary legal materials obtained through library research[9]. Primary legal materials consist of legislation, regulations, and judicial decisions relevant to banking cybercrime, including the Selayar District Court Decision Number 30/Pid.Sus/2019/PN.Slr concerning a skimming case. Secondary legal materials include legal textbooks, scholarly journal articles, commentaries, and academic publications discussing banking law, consumer protection, cybercrime, and civil liability. The collected materials were analyzed qualitatively using descriptive and analytical methods to identify the legal basis of bank liability, evaluate the effectiveness of existing legal protections, and assess the consistency between statutory provisions and their implementation in practice. The findings are presented systematically to explain how Indonesian positive law addresses customer losses resulting from skimming and account break-ins and to identify potential challenges in enforcing bank accountability.

RESULTS AND DISCUSSION

The findings of this study indicate that the issue of bank liability in cases of skimming and account break-ins cannot be analyzed solely from the perspective of criminal law. Although the perpetrators of such cybercrimes may be prosecuted under the provisions of the Information and Electronic Transactions Law, the losses suffered by customers raise broader questions regarding the legal responsibilities of banks as financial service providers. As institutions entrusted with safeguarding customer funds and personal data, banks are expected to implement adequate security measures and maintain reliable electronic systems capable of preventing unauthorized access and fraudulent activities.

The analysis further reveals that Indonesian positive law provides multiple legal foundations for assessing bank liability. These foundations are not limited to contractual obligations arising from the relationship between banks and customers, but also encompass consumer protection principles, cyber law regulations, and risk management obligations imposed upon financial institutions. Consequently, determining bank liability requires a comprehensive examination of various legal frameworks that collectively regulate the rights of customers and the responsibilities of banking institutions.

Based on the legal materials examined in this study, the discussion is structured into four analytical perspectives, namely legal liability theory, consumer protection theory, cyber law regulation, and risk management theory[10]. These perspectives are subsequently used to evaluate the adequacy of Indonesia's

---

[9] Saptaning Ruju Paminto Rusdin Tahir, I Gde Pantja Astawa, Agus Widjajanto, Mompang L Panggabean, Moh Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi Kania Sugiharti, Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktek (Jambi: Sonpedia, 2023).

10 Ujang Charda S, "TYPOLOGY OF LEGAL RESEARCH METHODS IN NORMATIVE AND SOCIOLOGICAL THINKING," Fox Justi : Jurnal Ilmu Hukum 12, no. 1 (July 2021): 111–18, https://doi.org/10.58471/justi.v12i1.769.

positive legal framework in addressing customer losses resulting from skimming and account break-in incidents.

Bank Liability Based on Legal Liability Theory

The legal relationship between a bank and its customer originates primarily from a contractual agreement governing the placement and management of customer funds. Through this relationship, customers entrust their funds and personal information to the bank with the expectation that the institution will exercise a high standard of care in protecting both assets and confidential data. Consequently, the relationship extends beyond a mere commercial transaction and creates legal obligations that require banks to act prudently, professionally, and in good faith when providing banking services.

Under Indonesian civil law, contractual relationships are governed by the provisions of the Civil Code[11] concerning agreements and obligations. Article 1313 of the Civil Code defines an agreement as an act by which one or more persons bind themselves to one or more other persons. In the banking context, this provision establishes reciprocal rights and obligations between banks and customers. Customers are required to comply with the terms and conditions governing the use of banking facilities, while banks are obligated to provide secure and reliable services capable of protecting customer funds and personal information from unauthorized access or misuse.

From the perspective of legal liability theory, customer losses resulting from skimming and account break-ins may give rise to two principal forms of civil liability: breach of contract (*wanprestasi)* and unlawful acts (*perbuatan melawan hukum*). Liability based on breach of contract arises when a bank fails to fulfill obligations that are expressly or implicitly contained within the banking agreement. Such circumstances may occur when a bank neglects to implement adequate security procedures, fails to maintain effective monitoring systems, or does not respond appropriately to indications of unauthorized transactions. If these failures contribute to customer losses, the bank may be considered to have violated its contractual obligations and therefore become liable for damages pursuant to Article 1239 of the Civil Code.

In addition to contractual liability, banks may also be held responsible under the doctrine of unlawful acts as regulated in Article 1365 of the Civil Code. This provision establishes that any person whose unlawful conduct causes harm to another party is obligated to compensate for the resulting losses. Within the banking sector, negligence in maintaining cybersecurity infrastructure, protecting customer data, updating security systems, or supervising banking operations may constitute unlawful conduct when such failures contribute to the occurrence of skimming or account break-ins. Therefore, even where a direct

[11] Kitab Undang-Undang Hukum Perdata, https://bhpjakarta.kemenkum.go.id/attachments/KUH_Perdata.pdf.

contractual violation cannot be clearly established, liability may still arise from the bank's failure to exercise the level of care reasonably expected of a financial institution.

The application of legal liability theory demonstrates that bank responsibility should not be assessed solely on the basis of whether the criminal act was committed by a third party[12]. Rather, the focus should be directed toward whether the bank fulfilled its legal obligations to provide adequate protection against foreseeable risks associated with digital banking services. Given the increasing sophistication of cybercrime, banks are expected to continuously strengthen their security systems, conduct regular risk assessments, and implement preventive measures capable of minimizing customer exposure to financial loss.

This interpretation is further supported by various regulatory instruments governing the financial sector[13]. Banking institutions are entrusted with managing public funds and therefore bear a heightened duty of care compared to ordinary business entities. As a result, when customer losses occur due to weaknesses in security systems or operational negligence, the legal consequences may extend beyond criminal liability for perpetrators and encompass civil liability on the part of the bank itself. Accordingly, legal liability theory provides a fundamental framework for understanding how responsibility may be attributed to banks in cases involving skimming and account break-ins.

Bank Liability Based on Consumer Protection Theory

Beyond the contractual relationship established between banks and customers, the legal position of customers may also be examined through the perspective of consumer protection law. In this framework, customers are recognized as consumers of banking services, while banks function as business actors providing financial products and services[14]. Consequently, the rights and obligations arising from banking transactions are not governed solely by private contractual arrangements but are also subject to the protective mechanisms established under consumer protection legislation.

Consumer protection theory is founded on the principle that consumers generally occupy a weaker position than service providers in terms of information, bargaining power, and access to resources[15]. This imbalance is particularly evident in the banking sector, where customers often possess limited knowledge

---

[12] Eka Ari Endrawati, Diah Turis Kaemirawati, and Susetya Herawati, "Perlindungan Hukum Sebagai Upaya Meningkatkan Kepercayaan Masyarakat Terhadap Perbankan: Studi Kasus Kejahatan Perbankan Di Indonesia," Binamulia Hukum 13, no. 2 (December 2024): 589–602, https://doi.org/10.37893/jbh.v13i2.945.

13 Undang-Undang (UU) Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan.

[14] Yudi Kornelis, "DIGITAL BANKING CONSUMER PROTECTION: DEVELOPMENTS & CHALLENGES," Jurnal Komunikasi Hukum (JKH) 8, no. 1 (February 2022): 378–94, https://doi.org/10.23887/jkh.v8i1.44477.

[15] Geraint Howells and Stephen Weatherill, Consumer Protection Law, 2nd ed. (Routledge, 2017), https://doi.org/10.4324/9781315259512.

regarding complex financial products, digital transaction systems, cybersecurity mechanisms, and internal operational procedures. Conversely, banks maintain exclusive control over transaction records, security infrastructures, and technical information necessary to investigate financial losses. As a result, consumer protection law seeks to restore balance by imposing additional responsibilities upon financial institutions and ensuring that customers receive adequate legal protection.

The legal basis for such protection can be found in Law Number 8 of 1999 concerning Consumer Protection[16]. Article 4 of the law recognizes several fundamental consumer rights, including the right to safety, comfort, security, and accurate information regarding goods and services. Within the context of banking services, these rights encompass the customer's expectation that financial transactions will be conducted through secure systems capable of protecting personal information and deposited funds from unauthorized access. Therefore, incidents such as skimming and account break-ins may be viewed not merely as criminal acts committed by third parties but also as events that potentially affect the fulfillment of customers' legally protected rights.

Furthermore, Article 19 of the Consumer Protection Law imposes an obligation upon business actors to provide compensation for losses suffered by consumers due to the use of goods and services they offer. This provision is particularly relevant in cases where customers experience financial losses resulting from weaknesses in banking security systems or inadequate preventive measures. From a consumer protection perspective, the central issue is not solely identifying the perpetrator of the cybercrime but determining whether the service provider has fulfilled its obligation to ensure reasonable levels of safety and security for consumers.

The principles underlying consumer protection theory also emphasize transparency, accountability, fairness, and access to remedies[17]. Banks are expected to provide clear information regarding transaction risks, available security features, complaint mechanisms, and procedures for resolving disputes. In addition, banks must respond promptly and transparently when customers report suspicious transactions or unauthorized account activities. Delays in handling complaints or failures to provide adequate explanations may further undermine consumer rights and weaken public confidence in banking institutions.

The application of consumer protection theory becomes particularly important in digital banking environments where technological complexity often creates significant evidentiary challenges for customers. Victims of skimming and account break-ins frequently encounter difficulties in proving whether losses resulted from personal negligence, third-party criminal conduct, or weaknesses within

[16] Undang-Undang Perlindungan Konsumen (1999).

[17] Trisadini Prasastinah Usanti and Anindya Prastiwi Setiawati, Customer Protection of Digital Services by Commercial Banks Concerning Consumer and Community Protection in the Financial Services Sector, no. 04 (n.d.).

banking systems. In such situations, a strict reliance on contractual principles may place customers at a disadvantage. Consumer protection law therefore serves as a corrective mechanism designed to ensure that customers are not unfairly burdened by informational asymmetries and institutional inequalities.

This approach is further reinforced by the Financial Services Authority Regulation (POJK) No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector[18]. The regulation requires financial service providers to maintain consumer confidentiality, establish complaint-handling mechanisms, and assume responsibility for losses arising from errors or negligence in business operations. These obligations demonstrate that customer protection constitutes an integral component of financial sector governance rather than merely a contractual commitment between private parties.

Accordingly, consumer protection theory provides a broader framework for evaluating bank liability in cases of skimming and account break-ins. While contractual liability focuses primarily on obligations arising from agreements, consumer protection theory emphasizes the duty of banks to safeguard customer interests, maintain service reliability, and ensure effective remedies when losses occur. This perspective strengthens the legal position of customers and reinforces the responsibility of banking institutions to uphold trust and security within the digital financial ecosystem.

Bank Liability Based on Cyber Regulation: ITE Law

The increasing adoption of digital banking services has transformed conventional banking risks into cybersecurity challenges[19]. Transactions that were previously conducted through face-to-face interactions are now performed through automated teller machines (ATMs), internet banking platforms, mobile banking applications, and other electronic systems. While these technologies provide efficiency and convenience, they also create opportunities for cybercriminals to exploit technological vulnerabilities through methods such as skimming, phishing, malware attacks, credential theft, and unauthorized account access. Consequently, incidents involving skimming and account break-ins are no longer merely banking disputes but have become issues closely connected to cyber law and electronic system governance.

In Indonesia, the primary legal framework governing cyber activities is Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 (ITE Law)[20]. The law establishes various prohibitions against unauthorized access to electronic systems, unlawful acquisition of electronic information, and manipulation of electronic data. Articles 30 through 32 of the

[18] Peraturan Otoritas Jasa Keuangan Tentang Perlindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan (2022), https://peraturan.bpk.go.id/Home/Details/227355/peraturan-ojk-no-6pojk072022-tahun-2022.

[19] Tamás Oroszi et al., "Whole Body Vibration Ameliorates Anxiety-like Behavior and Memory Functions in 30 Months Old Senescent Male Rats," *Heliyon* 10, no. 4 (February 2024): e26608, https://doi.org/10.1016/j.heliyon.2024.e26608.

[20] UU Informasi Dan Transaksi Elektronik.

ITE Law specifically criminalize unauthorized access, interception, duplication, transfer, alteration, or destruction of electronic information and electronic systems. These provisions provide the legal basis for prosecuting perpetrators involved in skimming operations and account break-ins, as such activities generally involve the unlawful acquisition and misuse of customer banking data.

A notable example can be found in the Selayar District Court Decision Number 30/Pid.Sus/2019/PN.Slr, in which the defendant was found guilty of conducting skimming activities by illegally copying customer ATM card data and subsequently using the duplicated information to withdraw funds from customer accounts. The court concluded that the defendant's actions fulfilled the elements of unauthorized access to electronic systems as regulated under the ITE Law. This case demonstrates that skimming constitutes a form of cybercrime that can be prosecuted through criminal law mechanisms[21]. However, while criminal sanctions may punish offenders, they do not automatically resolve questions concerning compensation for customer losses or the extent of bank liability.

From a cyber law perspective, responsibility is not limited to perpetrators alone. The ITE Law also imposes obligations upon electronic system operators to ensure the reliability, security, and proper functioning of electronic systems under their control. As providers of digital banking services, banks operate electronic systems that process, store, and transmit sensitive customer information. Therefore, banks are expected to implement adequate cybersecurity measures capable of preventing unauthorized access, protecting customer data, and ensuring the integrity of electronic transactions.

This obligation is reflected in Article 15 of the ITE Law, which requires electronic system operators to maintain secure and reliable systems and to ensure that such systems function properly. In the context of banking operations, compliance with this obligation includes the implementation of encryption technologies, authentication mechanisms, fraud detection systems, transaction monitoring procedures, and regular security audits. Failure to adopt reasonable cybersecurity measures may indicate negligence on the part of the bank and potentially establish a basis for civil liability when customers suffer losses as a result of security breaches.

The relevance of cyber law in assessing bank liability becomes increasingly apparent because modern cybercrime often exploits weaknesses within digital infrastructures rather than relying solely on physical access to banking facilities. As cyber threats continue to evolve, banks are expected to continuously strengthen their technological safeguards and adapt their security frameworks to emerging risks. A failure to do so may not only expose customers to financial harm but also undermine public confidence in digital banking services.

---

[21] D. A. P. Apsari, N. P. S. Meinarni, and W. G. S. Parwita, "Pengaruh Penggunaan Internet Banking Dan Perlindungan Data Nasabah Terhadap Cybercrime Di Kota Denpasar," *Ganaya: Jurnal Ilmu Sosial Dan Humaniora* 4, no. 1 (2021): 142–49, https://jayapanguspress.penerbit.org/index.php/ganaya/article/view/1254.

Accordingly, the ITE Law serves a dual function in cases involving skimming and account break-ins. First, it provides criminal sanctions against individuals who unlawfully access or misuse electronic information and systems. Second, it establishes normative obligations for electronic system operators, including banks, to maintain secure digital environments. Therefore, the legal analysis of bank liability cannot focus exclusively on the actions of cybercriminals but must also consider whether banking institutions have fulfilled their obligations as operators of electronic systems entrusted with safeguarding customer data and financial assets[22].

Bank Liability Based on Risk Management Theory

In addition to contractual obligations, consumer protection principles, and cyber law requirements, bank liability in cases of skimming and account break-ins may also be analyzed through the perspective of risk management theory. Within the banking industry, risk management constitutes a fundamental component of governance and operational sustainability[23]. Banks are entrusted with managing public funds and therefore bear a heightened responsibility to identify, assess, mitigate, and monitor risks that may threaten the security of customer assets and the stability of financial operations. Consequently, cyber threats such as skimming and account break-ins should not be viewed as unforeseeable incidents but rather as operational risks that require proactive management and continuous mitigation.

Risk management theory emphasizes that organizations must anticipate potential threats before losses occur[24]. In the context of digital banking, this principle requires banks to implement preventive measures capable of reducing vulnerabilities within their information systems. Such measures include regular cybersecurity assessments, fraud detection mechanisms, real-time transaction monitoring, multi-factor authentication systems, customer awareness programs, data encryption technologies, and periodic security audits. The objective is not only to respond to incidents after they occur but also to minimize the likelihood of cybercrime through effective risk prevention strategies.

---

[22] Budi Raharjo, "FINTECH TEKNOLOGI FINANSIAL PERBANKAN DIGITAL," *Penerbit Yayasan Prima Agus Teknik*, May 2021, 1–299.

[23] Douw Gerbrand Breed et al., "A Forward-Looking IFRS 9 Methodology, Focussing on the Incorporation of Macroeconomic and Macroprudential Information into Expected Credit Loss Calculation," *Risks* 11, no. 3 (March 2023): 59, https://doi.org/10.3390/risks11030059.

[24] Giovanni Borraccia, "Financial Conditions in Europe: Dynamics, Drivers, and Macroeconomic Implications," *IMF Working Papers* 2023, no. 209 (September 2023): 1, https://doi.org/10.5089/9798400254789.001.

The importance of risk management in banking operations is reflected in various regulatory frameworks issued by Bank Indonesia[25] and the Financial Services Authority (OJK)[26]. These regulations require banks to apply prudential principles and comprehensive risk management practices across all aspects of their business activities. Compliance obligations extend beyond financial management and encompass operational risks, information technology risks, cybersecurity threats, and customer data protection. Accordingly, banks are expected to continuously evaluate their security infrastructures and adapt to evolving technological threats that may affect customers and financial services.

From a legal perspective, inadequate risk management may constitute evidence of negligence when customer losses result from foreseeable and preventable cybersecurity incidents. For example, a bank that fails to update outdated security systems, neglects to install anti-skimming technology on ATM networks, ignores suspicious transaction patterns, or delays responding to customer complaints may be regarded as having failed to exercise the level of care expected of a professional financial institution. In such circumstances, the resulting losses cannot be attributed solely to external criminal actors because the bank's failure to implement reasonable preventive measures may have contributed to the occurrence or severity of the incident.

Risk management theory also highlights the close relationship between accountability and public trust. The banking sector operates primarily on the basis of confidence, meaning that customers deposit funds with the expectation that financial institutions possess the expertise and capacity necessary to protect those assets. When cyber incidents repeatedly occur despite available preventive technologies and regulatory requirements, public confidence in the banking system may be significantly weakened. Therefore, effective risk management serves not only as a regulatory obligation but also as a strategic mechanism for maintaining institutional credibility and long-term sustainability.

Furthermore, modern banking risk management extends beyond technical safeguards and incorporates organizational governance, employee supervision, and internal compliance mechanisms. Several cases of account break-ins have revealed that cybersecurity risks may originate not only from external attackers but also from internal weaknesses, including employee negligence, inadequate oversight, unauthorized disclosure of customer information, or failures in internal control systems. As a result, banks must ensure that risk management policies are integrated throughout the organization rather than limited to information technology departments alone.

---

[25] Peraturan Bank Indonesia Nomor 17/20/PBI/2015 Tahun 2015 Tentang Perubahan Ketiga Atas Peraturan Bank Indonesia Nomor 12/11/PBI/2010 Tentang Operasi Moneter, 17/20/PBI/2015 (2015), https://peraturan.bpk.go.id/Details/135540/peraturan-bi-no-1323pbi2011?utm_source=chatgpt.com.

26 Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum, 38/POJK.03/2016, https://peraturan.bpk.go.id/Details/128349/peraturan-ojk-no-38pojk032016-tahun-2016.

The findings suggest that risk management theory provides an important framework for evaluating bank liability because it focuses on prevention rather than merely post-incident accountability. Under this perspective, the central legal question is not only whether a cybercrime occurred, but also whether the bank had implemented adequate measures to identify and mitigate foreseeable risks. If reasonable precautions were not taken despite the availability of technological and regulatory safeguards, the bank may bear responsibility for the resulting losses. Therefore, effective risk management functions as both a legal obligation and a practical instrument for protecting customers, preserving public trust, and ensuring the resilience of digital banking systems.

Analysis of Indonesia's Positive Legal Framework on Skimming and Account Break-ins

The analysis of Indonesia's positive legal framework demonstrates that legal protection for customers affected by skimming and account break-ins is regulated through multiple legal instruments operating across civil, criminal, administrative, and consumer protection regimes[27]. These include the Indonesian Civil Code, Law Number 10 of 1998 concerning Banking, Law Number 8 of 1999 concerning Consumer Protection, Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law), as well as regulations issued by the Financial Services Authority (OJK) and Bank Indonesia. Collectively, these instruments establish legal obligations for banks to safeguard customer funds, maintain secure electronic systems, and provide remedies when losses occur. However, despite the existence of these regulatory frameworks, practical challenges continue to arise in determining liability and ensuring effective compensation for affected customers.

From a civil law perspective, Articles 1239 and 1365 of the Civil Code provide the primary legal basis for holding banks accountable. Customers may pursue claims based on breach of contract when banks fail to fulfill obligations arising from banking agreements, or based on unlawful acts when negligence in maintaining security systems results in financial losses. These provisions theoretically provide sufficient legal mechanisms to seek compensation. Nevertheless, their practical application often encounters evidentiary difficulties, particularly in proving whether customer losses resulted directly from bank negligence or from the independent actions of third-party cybercriminals. Consequently, customers frequently face challenges in establishing the causal relationship necessary to support civil claims.

Consumer protection regulations strengthen the legal position of customers by recognizing them as consumers of financial services. Law Number 8 of 1999[28] concerning Consumer Protection and POJK No. 1/POJK.07/2013 impose obligations upon financial institutions to provide secure services, maintain

[27] Hassanain Haykal, "Toward a Responsive Legal Framework: Addressing Transaction Security Risks in Indonesia's Digital Banking Services," *International Journal of Law and Society (IJLS)* 4, no. 2 (August 2025): 234–49, https://doi.org/10.59683/ijls.v4i2.290.

[28] Undang-Undang Perlindungan Konsumen.

confidentiality, and address consumer complaints effectively. These regulations reflect a broader policy objective of balancing the relationship between financial institutions and customers. However, in practice, customers often encounter procedural obstacles when seeking compensation because technical information regarding transactions, cybersecurity systems, and internal investigations remains largely under the control of banking institutions. This informational imbalance may place customers in a relatively weaker position during dispute resolution processes[29].

The ITE Law further complements the legal framework by criminalizing unauthorized access to electronic systems, theft of electronic information, and other forms of cybercrime commonly associated with skimming and account break-ins. Through this framework, perpetrators may be subjected to criminal sanctions for unlawful activities involving banking data and electronic systems. Nevertheless, the ITE Law primarily focuses on punishing offenders rather than regulating compensation mechanisms for victims. As a result, customers who suffer financial losses must generally pursue separate civil or consumer protection remedies to obtain restitution, creating additional legal complexity and potentially prolonging the resolution process.

A practical illustration of this issue can be observed in the Selayar District Court Decision Number 30/Pid.Sus/2019/PN.Slr involving a skimming operation conducted by a foreign national. While the court successfully imposed criminal sanctions against the perpetrator, the decision did not automatically resolve questions concerning compensation for affected customers. This situation highlights a significant distinction between criminal accountability and civil liability. The punishment of offenders may satisfy the objectives of criminal justice, but it does not necessarily restore customer losses unless additional legal mechanisms are pursued. Consequently, legal protection remains fragmented across multiple regulatory frameworks and enforcement processes.

The findings further reveal that one of the principal weaknesses within the current legal framework is the absence of specific regulations comprehensively addressing bank liability in cases of cyber-enabled financial losses. Existing regulations provide general obligations relating to prudential banking, consumer protection, and electronic system security, yet they do not establish clear standards for determining liability when losses result from sophisticated cybercrime. Banks frequently argue that skimming and account break-ins are caused by external criminal actors beyond their control, whereas customers contend that such incidents often indicate weaknesses in banking security systems. This divergence creates uncertainty regarding the allocation of responsibility and may hinder effective dispute resolution.

[29] Dicky Malik Ibrahim, Yusuf Hidayat, and Fokky Fuad Wasitaatmadja, "Legal Protection of Banking Customers Who Are Victims Of Information And Electronic Transaction Crimes," *Jurnal Ilmiah Penegakan Hukum* 11, no. 1 (June 2024): 102–20, https://doi.org/10.31289/jiph.v11i1.11099.

Therefore, although Indonesia's positive legal system has established a relatively comprehensive normative framework for addressing skimming and account break-ins, the effectiveness of customer protection remains dependent upon implementation and enforcement. The challenge is not merely the availability of legal rules but also the consistency of their application, the transparency of banking institutions, and the ability of regulatory authorities to ensure accountability. Strengthening legal certainty may require clearer regulatory standards regarding bank liability, enhanced consumer protection mechanisms, and more effective integration between civil, administrative, and cybercrime enforcement frameworks. Such measures would contribute to greater legal protection for customers while simultaneously reinforcing public trust in Indonesia's increasingly digital banking sector.

CONCLUSION

This study concludes that banks may be held legally liable for customer losses arising from skimming and account break-ins through multiple legal frameworks. From the perspective of civil liability, banks may be responsible based on breach of contract (wanprestasi) under Article 1239 of the Indonesian Civil Code when they fail to fulfill obligations arising from banking agreements, as well as on the basis of unlawful acts (perbuatan melawan hukum) under Article 1365 when negligence in maintaining security systems results in customer losses. Furthermore, consumer protection principles recognize customers as consumers of financial services and impose obligations on banks to provide secure, reliable, and accountable services. The analysis of cyber law regulations also demonstrates that banks, as electronic system operators, are required to maintain secure and reliable electronic systems, while risk management principles emphasize the duty of banks to identify, mitigate, and control cybersecurity risks. Accordingly, bank liability should not be assessed solely by reference to the actions of cybercriminals, but also by evaluating whether the bank has fulfilled its legal, operational, and security obligations in protecting customer funds and personal data.

The study further finds that Indonesia's positive legal framework provides a relatively comprehensive basis for addressing skimming and account break-ins through the Civil Code, the Banking Law, the Consumer Protection Law, the ITE Law, and regulations issued by the Financial Services Authority and Bank Indonesia. Nevertheless, the effectiveness of customer protection remains constrained by several practical challenges, including difficulties in proving bank negligence, the fragmented nature of compensation mechanisms, and the absence of specific regulations comprehensively governing bank liability in cyber-enabled banking losses. While criminal sanctions may be imposed on perpetrators, customers often remain required to pursue separate civil or consumer protection remedies to recover their losses. Therefore, strengthening legal certainty requires clearer standards regarding bank liability, enhanced consumer protection mechanisms, greater transparency in dispute resolution processes, and

stronger regulatory oversight to ensure that legal protections available in theory can be effectively implemented in practice.

REFERENCES

Apsari, D. A. P., N. P. S. Meinarni, and W. G. S. Parwita. "Pengaruh Penggunaan Internet Banking Dan Perlindungan Data Nasabah Terhadap Cybercrime Di Kota Denpasar." *Ganaya: Jurnal Ilmu Sosial Dan Humaniora* 4, no. 1 (2021): 142–49. https://jayapanguspress.penerbit.org/index.php/ganaya/article/view/1254.

Avianto, Wahyu, Hermanto Siregar, Anny Ratnawati, and Mulya E. Siregar. "Determinants of Digital Bank Transformation: A Systematic Literature Review with Prisma and Bibliometrics." *JPPI (Jurnal Penelitian Pendidikan Indonesia)* 10, no. 4 (November 2024): 296–307. https://doi.org/10.29210/020243553.

Borraccia, Giovanni. "Financial Conditions in Europe: Dynamics, Drivers, and Macroeconomic Implications." *IMF Working Papers* 2023, no. 209 (September 2023): 1. https://doi.org/10.5089/9798400254789.001.

Breed, Douw Gerbrand, Jacques Hurter, Mercy Marimo, Matheba Raletjene, Helgard Raubenheimer, Vibhu Tomar, and Tanja Verster. "A Forward-Looking IFRS 9 Methodology, Focussing on the Incorporation of Macroeconomic and Macroprudential Information into Expected Credit Loss Calculation." *Risks* 11, no. 3 (March 2023): 59. https://doi.org/10.3390/risks11030059.

Endrawati, Eka Ari, Diah Turis Kaemirawati, and Susetya Herawati. "Perlindungan Hukum Sebagai Upaya Meningkatkan Kepercayaan Masyarakat Terhadap Perbankan: Studi Kasus Kejahatan Perbankan Di Indonesia." *Binamulia Hukum* 13, no. 2 (December 2024): 589–602. https://doi.org/10.37893/jbh.v13i2.945.

———. "Perlindungan Hukum Sebagai Upaya Meningkatkan Kepercayaan Masyarakat Terhadap Perbankan: Studi Kasus Kejahatan Perbankan Di Indonesia." *Binamulia Hukum* 13, no. 2 (December 2024): 589–602. https://doi.org/10.37893/jbh.v13i2.945.

Haykal, Hassanain. "Toward a Responsive Legal Framework: Addressing Transaction Security Risks in Indonesia's Digital Banking Services." *International Journal of Law and Society (IJLS)* 4, no. 2 (August 2025): 234–49. https://doi.org/10.59683/ijls.v4i2.290.

Howells, Geraint, and Stephen Weatherill. *Consumer Protection Law*. 2nd ed. Routledge, 2017. https://doi.org/10.4324/9781315259512.

———. *Consumer Protection Law*. 2nd ed. Routledge, 2017. https://doi.org/10.4324/9781315259512.

Ibrahim, Dicky Malik, Yusuf Hidayat, and Fokky Fuad Wasitaatmadja. "Legal Protection of Banking Customers Who Are Victims Of Information And Electronic Transaction Crimes." *Jurnal Ilmiah Penegakan Hukum* 11, no. 1 (June 2024): 102–20. https://doi.org/10.31289/jiph.v11i1.11099.

Kitab Undang-Undang Hukum Perdata. https://bhpjakarta.kemenkum.go.id/attachments/KUH_Perdata.pdf.

Kornelis, Yudi. "DIGITAL BANKING CONSUMER PROTECTION: DEVELOPMENTS & CHALLENGES." *Jurnal Komunikasi Hukum (JKH)* 8, no. 1 (February 2022): 378–94. https://doi.org/10.23887/jkh.v8i1.44477.

Oroszi, Tamás, Klára Felszeghy, Paul G. M. Luiten, Regien G. Schoemaker, Eddy A. Van Der Zee, and Csaba Nyakas. "Whole Body Vibration Ameliorates Anxiety-like Behavior and Memory

Functions in 30 Months Old Senescent Male Rats." *Heliyon* 10, no. 4 (February 2024): e26608. https://doi.org/10.1016/j.heliyon.2024.e26608.

———. "Whole Body Vibration Ameliorates Anxiety-like Behavior and Memory Functions in 30 Months Old Senescent Male Rats." *Heliyon* 10, no. 4 (February 2024): e26608. https://doi.org/10.1016/j.heliyon.2024.e26608.

Peraturan Bank Indonesia Nomor 17/20/PBI/2015 Tahun 2015 Tentang Perubahan Ketiga Atas Peraturan Bank Indonesia Nomor 12/11/PBI/2010 Tentang Operasi Moneter, 17/20/PBI/2015 (2015). https://peraturan.bpk.go.id/Details/135540/peraturan-bi-no-1323pbi2011?utm_source=chatgpt.com.

Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 Tahun 2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum, 38/POJK.03/2016. https://peraturan.bpk.go.id/Details/128349/peraturan-ojk-no-38pojk032016-tahun-2016.

Peraturan Otoritas Jasa Keuangan Tentang Perlindungan Konsumen Dan Masyarakat Di Sektor Jasa Keuangan (2022). https://peraturan.bpk.go.id/Home/Details/227355/peraturan-ojk-no-6pojk072022-tahun-2022.

Raharjo, Budi. "FINTECH TEKNOLOGI FINANSIAL PERBANKAN DIGITAL." *Penerbit Yayasan Prima Agus Teknik*, May 2021, 1–299.

Rusdin Tahir, I Gde Pantja Astawa, Agus Widjajanto, Mompang L Panggabean, Moh Mujibur Rohman, Ni Putu Paramita Dewi, Nandang Alamsah Deliarnoor, Muhamad Abas, Rizqa Febry Ayu, Ni Putu Suci Meinarni, Fatimah Hs, Ni Wayan Eka Sumartini, Dewi Kania Sugiharti, Saptaning Ruju Paminto. *Metodologi Penelitian Bidang Hukum: Suatu Pendekatan Teori Dan Praktek*. Jambi: Sonpedia, 2023.

Samad, M. Yusuf, and Pratama Dahlian Persadha. "Memahami Perang Siber Rusia Dan Peran Badan Intelijen Negara Dalam Menangkal Ancaman Siber Understanding Russian Cyber Warfare and the Role of the State Intelligence Agency in Countering Cyber Threats." *Jurnal Ilmu Pengetahuan Dan Teknologi Komunikasi* 24, no. 2 (2022): 135–46. http://dx.doi.org/10.17933/iptekkom.24.2.2022.135-146.

Ujang Charda S. "TYPOLOGY OF LEGAL RESEARCH METHODS IN NORMATIVE AND SOCIOLOGICAL THINKING." *Fox Justi : Jurnal Ilmu Hukum* 12, no. 1 (July 2021): 111–18. https://doi.org/10.58471/justi.v12i1.769.

Undang-Undang Perlindungan Konsumen (1999).

Undang-Undang (UU) Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen (1999).

Undang-Undang (UU) Nomor 10 Tahun 1998 Tentang Perubahan Atas Undang-Undang Nomor 7 Tahun 1992 Tentang Perbankan (1998). https://peraturan.bpk.go.id/Details/45486/uu-no-10-tahun-1998?utm_source=chatgpt.com.

Usanti, Trisadini Prasastinah, and Anindya Prastiwi Setiawati. *Customer Protection of Digital Services by Commercial Banks Concerning Consumer and Community Protection in the Financial Services Sector*. no. 04 (n.d.).

UU Informasi Dan Transaksi Elektronik (2016).