ALGEBRA : JURNAL PENDIDIKAN, SOSIAL DAN SAINS

ISSN : 2807-663X e-ISSN : 2807-629X
Journal Homepage : https://algebra.yana.or.id/index.php/ejournal/index
Volume 5 Number 4 (2025)

JURIDICAL ANALYSIS OF BANKING INSTITUTIONS' LIABILITY FOR CARDING CRIMES

Arina Novitasari[1*], Dika Anggara Putra[2], Dian Rosita[3]
[123]Program Studi Hukum, Fakultas Pendidikan, Ekonomi dan Hukum, Universitas Muhammadiyah Kudus, Kudus, Indonesia
[*]Correspondence Email: arinanovitasari@umkudus.ac.id

ABSTRACT

The rapid development of technology has brought humanity into a wave of modernization characterized by digitalization, leading to significant changes in all aspects of human life. The role of technology today offers various conveniences. The transformation of payment systems from cash-based to cashless transactions provides ease for customers and helps reduce the risk of crimes such as robbery, theft, and counterfeiting. One of the most widely used cashless payment methods that is frequently misused by irresponsible individuals for criminal purposes today is the credit card. The focus of this study is to examine the legal accountability of banking institutions in relation to a specific type of cybercrime, namely carding, which causes financial losses to customers. This research employs a normative juridical method. The findings indicate that the bank's liability from a civil law perspective refers to Article 1338 paragraph (1) of the Indonesian Civil Code and Article 19 paragraph (1) of Law No. 8 of 1999 concerning Consumer Protection. Customer losses resulting from carding crimes are viewed as a consequence of inadequate protection by the issuing bank in maintaining network security. Errors or negligence by bank employees can be construed as the bank's responsibility; however, if it can be proven that the carding crime did not occur due to the issuing bank's negligence, then the bank is not obliged to compensate for the losses suffered by the customer.

Keywords: Carding; Accountability; Banking; Civil Law.

INTRODUCTION

The rapid advancement of technology has brought humanity into a wave of modernization characterized by extensive digitalization. It is undeniable that the digital world has brought significant changes to all aspects of human life. These major transformations have also altered the way people conduct their daily activities across various sectors, including government, business, banking, education, healthcare, and even personal life.

The role of technology has become increasingly vital in overcoming the limitations of human interaction. With the presence of technology, distance and time are no longer barriers to communication and interaction. One of the sectors profoundly influenced by technological advancement is banking. The shift from cash-based to cashless payment systems has benefited society by providing greater convenience and efficiency. Among the most widely used cashless payment methods today are credit cards and debit cards.

Credit and debit cards offer a variety of conveniences transactions become faster and easier. There is no longer a need to carry large amounts of cash when shopping. Simply by carrying a card containing personal and account data, individuals can withdraw money anytime and anywhere. This cashless payment method not only simplifies transactions for customers but also reduces the risk of crimes such as robbery, theft, and counterfeiting.

Article 1 point 6 of Bank Indonesia Regulation No. 14/02/PBI/2012 on the Implementation of Activities Using Card-Based Payment Instruments states that:

> *"A Debit Card is a payment instrument using a card that can be used to make payments for obligations arising from economic activities, including shopping transactions, by directly debiting the cardholder's savings account at a bank or other authorized financial institution in accordance with applicable laws and regulations."*

In addition to debit cards, banks also issue another alternative form of cashless payment, namely credit cards. Article 1 paragraph (4) of the same regulation defines a credit card as:

> *"A payment card representing a payment obligation by the customer arising from an economic activity, including shopping transactions and/or cash withdrawals, where the obligation is first fulfilled by the acquirer or issuer."*

In recent years, the use of credit cards has become a global lifestyle that reaches almost all social groups. Credit cards, which offer various conveniences in transactions, allow individuals to make large purchases without carrying substantial cash. It is undeniable that credit cards have become one of the most favored payment instruments after checks and giro. Consequently, the use of cash as a means of payment has gradually declined, replaced by credit card usage.

However, the widespread use of credit cards also opens opportunities for criminal acts. Individuals with computer skills and malicious intent can exploit computer and internet technology to commit crimes or fraud that harm others. These individuals take advantage of technological progress to engage in cyber-based banking crimes commonly referred to as *cybercrime*.

Cybercrime refers to criminal acts involving computers, generally defined as the illegal use of computer systems (Hamzah, 2013). Credit card data theft, or carding, is one form of cybercrime that occurs in online banking transactions. The most common form of carding crime is identity theft.

In *carding* crimes, perpetrators use another person's credit card number and identity, often obtained through the internet. Although *carding* is non-violent, its impact is substantial. For example, offenders may use another person's account for online shopping to enrich themselves unlawfully.

From a juridical perspective, banking institutions function as intermediaries that collect and distribute public funds. The relationship between banks and their customers can be both contractual and non-contractual. Contractual relationships are based on written agreements, while non-contractual relationships rely on trust, confidentiality, and prudence.

Maintaining the confidentiality of customer data is a core obligation of banking institutions. Protecting customer information is crucial to building trust and confidence in conducting various banking transactions. However, as technology continues to evolve, so do the risks of banking-related crimes. Data breaches have become a serious concern in the digital era, as the misuse of financial information can erode public trust in banking institutions.

Based on the background above, the focus of this research is to analyze the legal liability of banking institutions in cases of cybercrime, specifically carding, which results in financial losses for customers. The urgency of this study has increased due to the rapid development of digital technologies that enable increasingly sophisticated methods of credit card data theft, including attacks that exploit data breaches and security gaps in online transaction systems. Although banks have implemented security technologies such as multi-layer authentication and AI-based fraud

detection systems, modern carding techniques continue to evolve, creating security gaps that have not been fully anticipated by existing regulations. Legal uncertainties related to data protection and the scope of a bank's liability within the digital transaction ecosystem constitute a contemporary issue that requires further examination.

The research question in this study is how banking institutions can be held legally responsible when carding crimes cause customer losses, and whether the current digital security systems and regulatory frameworks are adequate to prevent data theft and unauthorized transactions in modern banking services. Therefore, this research aims to identify, analyze, and provide recommendations regarding the issue of carding crimes in Indonesia.

RESEARCH METHODS

The research method used in this study is normative juridical, namely a method that focuses on examining legislation, legal principles, and legal doctrines relevant to addressing the issue of banking liability in carding crimes (Marzuki, 2011). The data for this research were obtained through literature study consisting of primary legal materials such as the Banking Law, Bank Indonesia Regulations, OJK Regulations, and court decisions related to cybercrime. Secondary legal materials are also used, including books, scholarly journals, research reports, institutional publications, and academic opinions discussing the development of digital banking crimes. To strengthen the conceptual understanding, tertiary legal materials such as legal dictionaries and encyclopedias are employed.

The approaches applied are the statute approach and the conceptual approach. In analyzing legal provisions, the study utilizes various methods of legal interpretation, including grammatical, systematic, and teleological interpretations, to ensure that the norms are interpreted accurately within the context of current developments in banking security technology and emerging legal gaps in digital transactions. Thus, this research method does not only examine norms textually but also positions them within the framework of customer protection needs in the digital era.

RESULTS AND DISCUSSION

In accordance with Law No. 10 of 1998 concerning Banking, banking institutions are financial entities that function to collect public funds in the form of deposits such as current accounts, savings, or time deposits and to redistribute those funds in the form of credit. In addition, banks are considered institutions of integrity because one of the key principles in their management is the principle of trust.

In general terms, banking can be defined as a type of enterprise that provides services in the financial sector. Technology plays a vital role in the banking industry. The more advanced and diverse the facilities provided by banks to serve their customers, the greater the reliance on technology. Technology acts as a catalyst for innovation that enhances the quality of customer service.

The use of technology in banking has become a new competitive standard in the digital era. The transformation from cash-based to cashless payment systems indicates that technological advancements bring substantial benefits to society. From the perspective of efficiency, technology offers speed and convenience in transactions; however, it also gives rise to various legal challenges that may disadvantage bank customers.

One of the most widely used cashless payment methods that is also frequently misused by irresponsible individuals for criminal purposes is the credit card. The typical modus operandi in credit card-related crimes involves the use of another person's data or identity to make purchases at merchants that accept non-cash payments. The duplication of credit cards is carried out by reading the data stored on the card's magnetic stripe using a *Magnetic Stripe Card Reader* (MSR), after which the data is transferred to a blank or counterfeit card using a Magnetic Stripe Card Writer (Herman et al., 2023). These counterfeit cards are then used by perpetrators for fraudulent purchases.

This type of credit card data theft is known as carding or cyber fraud, which constitutes a form of cybercrime. A credit card is issued by an issuing bank that extends a certain amount of credit to the customer without requiring the customer to maintain deposits with that bank (Ali Arifin, 2002). According to Bank Indonesia Regulation No. 11/11/PBI/2009, an issuing bank is a bank or non-bank institution authorized to issue credit and/or debit cards.

The issuance of credit cards is based on a special agreement governed by Book III of the Indonesian Civil Code (KUHPerdata). The credit card issuance agreement between the issuing bank and the cardholder falls under the category of a loan-for-consumption agreement (*perjanjian pinjam pakai habis*) as regulated in Articles 1754–1773 of the Civil Code. Article 1754 defines such an

agreement as *"a contract in which one party delivers to another a certain quantity of consumable goods, with the condition that the latter shall return an equal quantity of goods of the same kind and quality."*

The characteristics of a loan-for-consumption agreement are that once the loan is granted, the object of the loan becomes the property of the borrower, and if the goods are destroyed for any reason, the borrower bears the loss. Another characteristic is that the lender cannot demand the return of the loaned goods before the term specified in the agreement expires. Disputes related to defaulted credit card payments, incorrect billing, unauthorized deductions, or interest rates inconsistent with the agreement can be resolved through mutual consent between the cardholder and the issuing bank.

The agreement governing the use of a credit card is accessory to the principal credit card issuance agreement, as it involves three parties: the cardholder as the buyer, the merchant as the seller, and the issuing bank as the payer. This agreement falls within the scope of sales contracts as regulated in Articles 1457–1518 of the Civil Code, although its execution depends on the terms outlined in the primary credit card issuance agreement.

From a contractual perspective, the legal relationship between the issuing bank and the credit cardholder constitutes an obligation arising from mutual consent, where the content of the agreement binds both parties. This is stipulated in Article 1338 paragraph (1) of the Civil Code, which forms the foundation of freedom of contract, stating that *"all legally executed agreements shall bind the parties as law."* In essence, the contractual clauses mutually bind both parties, and the content of the credit card issuance agreement must adhere to applicable legal provisions.

According to the author's analysis, referring to Johanes Gunawan's theory of bank accountability toward customers as consumers (Gunawan, 1999), the responsibility of banks can be divided into three stages:

1. **Pre-Transaction Stage**
   At this stage, the issuing bank introduces and offers its products to potential customers by providing information about requirements, types of credit cards offered, the rights and obligations of cardholders, and potential risks associated with credit card usage. Meanwhile, prospective customers seek information about the product they intend to apply for.
2. **Transaction Stage**
   In this stage, the consumer, as a credit card user, enters into a binding agreement with the issuing bank. This marks the formal issuance of the credit card.
3. **Post-Transaction Stage**
   This stage involves the resolution of disputes, complaints, or problems that may arise between the bank and the credit cardholder.

Referring to Article 19 paragraph (1) of Law No. 8 of 1999 concerning Consumer Protection, it is stated that *"business actors are responsible for compensating for damages, contamination, and/or losses suffered by consumers as a result of consuming goods and/or services produced or traded."* Customer losses due to *carding* crimes can thus be regarded as a consequence of the issuing bank's inadequate protection of its network security, allowing unauthorized parties to breach it. Therefore, credit cardholders as consumers are entitled to legal protection.

The provision of legal protection for bank customers as consumers is guaranteed by both the Consumer Protection Law and the Banking Law. Liability for customer losses is imposed on the bank if negligence can be established. According to Article 1467 of the Civil Code, *"a person is not only responsible for the losses caused by himself but also for those caused by persons under his responsibility."* In this context, the civil liability of the bank arises from the fault or negligence of its employees, which can be interpreted as the bank's own responsibility. However, if it can be proven that the *carding* incident did not result from the issuing bank's negligence, then the bank is not obligated to compensate the customer for the loss incurred.

As the use of credit cards increases within the digital payment ecosystem, numerous carding cases in Indonesia show that this crime continues to evolve by exploiting new vulnerabilities in banking technology and procedures. In practice, a common pattern involves high-value card-not-present (CNP) transactions conducted by unknown parties while the physical card remains with the customer. One of the most widespread schemes in the past two years is the SIM-swap method, in which perpetrators take over the victim's mobile number so that the bank's OTP is redirected to the perpetrator's device. When customers file disputes, banks often argue that the transaction was "legitimate" because it was authenticated using an OTP, even though it is later found that the OTP was diverted through a security gap that should have been monitored by the bank.

This trend aligns with reports from various institutions showing that CNP fraud accounts for the largest proportion of card-related crime—reaching more than 50% of total card fraud in many

jurisdictions—and with the increasing volume of consumer complaints in the digital banking sector. In courts, such disputes test a bank's ability to demonstrate that its authentication systems meet the required standards of due diligence, including providing technical logs such as OTP delivery history, device fingerprints, IP addresses, mobile number change records, and anomaly-detection flags. If the bank is unable to provide such evidence, courts tend to view the incident as systemic negligence on the bank's part. Conversely, if it is proven that the customer actively disclosed the OTP, accessed phishing links, or engaged in other negligent conduct, liability shifts toward the consumer. Thus, the allocation of risk in carding cases largely depends on proving negligence (fault-based liability) and examining the robustness of the bank's technical controls.

Within the framework of positive law, Article 19 of the Consumer Protection Law places banks—as business actors—responsible for compensating losses arising from their services unless they can prove that the losses did not result from their fault or negligence. In practice, this creates a form of limited reverse burden of proof, meaning banks cannot simply claim that customers were "careless"; they must demonstrate that their security systems complied with industry standards, including strong customer authentication (SCA), data encryption, strict verification procedures for phone number changes, and real-time transaction monitoring. If a bank fails to present complete and auditable technical evidence, the risk is automatically shifted to the bank as the service provider. Meanwhile, customers bear the risk if it is proven that they acted contrary to security principles, such as sharing OTPs, entering personal data on fraudulent websites, or using devices compromised by malware.

Furthermore, the digital payment ecosystem—which involves merchants, payment gateways, and telecommunications providers—creates the possibility of shared liability, particularly when data leaks originate from non-bank systems, where banks remain obligated to facilitate chargebacks according to international network standards.

This analysis shows that carding can no longer be viewed solely as the consumer's individual fault, but rather as a phenomenon that requires a comprehensive assessment of systemic negligence, the bank's readiness to implement advanced security technologies, and the accuracy of its risk-based supervision. By incorporating recent case trends, legal gaps, and the challenges of proving negligence in modern digital transactions, this study gains contemporary relevance, revealing how technological developments create new opportunities for crime while the legal protection framework must continually adapt to maintain the balance between consumer rights and banking obligations.

CONCLUSION

Carding is a form of cybercrime. The credit card usage agreement constitutes an accessory agreement to the primary credit card issuance agreement, involving three parties: the credit card holder as the buyer, the merchant as the seller, and the issuing bank as the payer. From the perspective of contract law, the legal relationship between the issuing bank and the cardholder is a consensual obligation, in which the terms agreed upon bind both parties, as stipulated in Article 1338(1) of the Indonesian Civil Code, which forms the basis of the freedom of contract principle. Referring to Article 19(1) of Law No. 8 of 1999 on Consumer Protection, losses suffered by customers due to carding constitute a form of inadequate protection by the issuing bank in safeguarding its network security, allowing unauthorized parties to breach the system. Therefore, customers or credit card users—as consumers—are entitled to legal protection. This complexity illustrates that carding is no longer a simple crime but a systemic issue involving the bank, merchant, payment gateway, and even telecommunications providers, which legally creates the potential for shared liability when the point of data leakage originates from systems outside the bank. To address these challenges, this study highlights the need for adaptive and responsive policy recommendations aligned with technological developments and the escalating scale of digital crime. First, banks must strengthen their digital security compliance, including mandatory continuous security audits, the implementation of strong customer authentication, and the enhancement of anomaly-detection systems based on machine learning. Second, OJK and Bank Indonesia should tighten minimum security standards for payment service providers, including regulations for online merchants, payment gateways, and telecommunication operators involved in the credit card transaction chain. Third, a clear liability framework must be established so that carding disputes are no longer dependent on the bank's narrow interpretation but instead follow a standardized risk-allocation scheme. Fourth, consumer education must be improved through digital security literacy campaigns, particularly regarding the risks of phishing, OTP protection, public-network usage, and device security. Through stronger regulation, consistent technological security standards, and heightened user awareness, it is

expected that carding incidents can be reduced and legal protection for banking consumers can be strengthened in the era of financial digitalization.

BIBLIOGRAPHY

Gentur Cahyo dkk. 2022. Tanggung Jawab Bank Sebagai Wujud Perlindungan Hukum Bagi Nasabah Kontrak Perbankan. Jurnal Transparasi Hukum Vol. 5 No 1, Januari 2022

Hamzah, Andi. 1996. Hukum Acara Pidana Indonesia. Jakarta: Sapta Arta Jaya.

Herman dkk, 2023. Kejahatan Carding Sebagai Bentuk Cyber Crime dalam Hukum Pidana Indonesia. Halu Oleo Legal Research Volume 5, Issue 2, August 2023

Hermansyah. 2013. Hukum Perbankan Nasional. Edisi Kedua Jakarta: Kencana

Johanes Gunawan. 1999 Hukum Perlindungan Konsumen. Bandung: Universitas Katolik Parahyangan

KUH Perdata

Marzuki, Peter Mahmud. 2011, Legal Research, Jakarta: Kencana

Peraturan Bank Indonesia (PBI) Nomor 16/1/2014 tentang Perlindungan Konsumen Jasa Sistem Pembayaran

Peraturan Bank Indonesia Nomor 14/02/PBI/2012 tentang Penyelenggaraan Kegiatan Alat Pembayaran Dengan Menggunakan Kartu

Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan

Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen

Wiguna, Kadek Doni dkk. 2022. Pertanggungjawaban Bank Atas Kerugian Nasabah Yang Menggunakan Electronic Banking. Jurnal Kertha Desa Vol. 9 No. 12, Oktober 2022