JHSS (Journal of Humanities and Social Studies)
https://journal.unpak.ac.id/index.php/jhss
Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

CONSUMER PROTECTION FOR CREDIT CARD HOLDERS AGAINST TRANSACTION BILLS NOT MADE BY CUSTOMERS PERSPECTIVE FATWA DSN MUI NUMBER 54/DSN/MUI/X/2006

Nadiyah Roihanah Ritonga [a*)], Fatimah Zahara [b)]

[a)] *State Islamic University of North Sumatra, Medan, Indonesia*

[*)]*Corresponding Author: nadiyah0204212154@uinsu.ac.id*

Article history: *received 21 June 2025; revised 02 July 2025; accepted 15 August 2025* *DOI: https://doi.org/10.33751/jhss.v9i2.12655*

Abstract. The development of digital financial technology has brought ease of transactions, but also increased the risk of credit card misuse, especially illegal transactions that are not carried out by customers. This study aims to find out the normative review of consumer protection regulations in the financial services sector (banks), to analyze the DSN-MUI fatwa on unauthorized transactions and forms of customer protection, to find out the form of protection provided by banks to credit card users, and, to find out the form of responsibility of banks for illegal transactions experienced by customers. This type of research is juridical-normative with a *conceptual approach* and *a statute approach*. Data is collected through document studies and then data is processed qualitatively and analyzed using deductive logic. The results of the study show that banks have an absolute responsibility in ensuring the security of the transaction system and are obliged to provide protection to customers. The DSN-MUI fatwa emphasizes the importance of a valid contract and the principle of justice, which prohibits the imposition of losses on customers for transactions without consent. Real cases such as credit card break-ins by third parties show the weakness of banks' verification systems and digital security. Therefore, customer protection needs to be carried out through preventive (such as improving consumer security and education systems) and repressive approaches (such as compensation and administrative sanctions). This study emphasizes the importance of collaboration between positive law and sharia principles in protecting consumers for transactions made from credit card holders so that transactions do not occur without customer consent.

Keywords: Consumer Protection, Customers, Credit Cards, DSN MUI Fatwa

I. INTRODUCTION

The development of information technology and the digitalization of the financial sector have changed people's behavior patterns in transactions. One of the leading products in the modern payment system is the credit card, which provides convenience and flexibility in transactions without the need to carry cash. Credit cards are considered a practical solution in fulfilling consumptive and urgent needs, as well as being part of the financial system that encourages the acceleration of the digital economy.

However, these technological advancements also carry considerable risks, especially in terms of transaction security and consumer protection. As the use of credit cards increases, cases of credit card misuse and illegal transactions that are not carried out by customers are also becoming more frequent. This causes financial losses for consumers as well as legal uncertainty over the rights and obligations between banks and customers. Financial growth in Islam must be closely monitored and regulated in terms of its legal and regulatory status to avoid actions that are explicitly prohibited in the sharia [1].

Various cases show that credit card abuse does not only occur domestically, but also across countries. For example, in June 2023, a Jenius credit card customer from Bank BTPN reported through the @yourlastnameis Twitter account that he was charged IDR 22 million for a transaction that occurred in the United States, even though he had never been abroad and did not receive an OTP code on his phone. A similar case was also experienced by Mira, a BCA credit card customer, whose card was illegally used from Singapore for Netflix transactions six times between December 2022 and January 2023, even though she never left Indonesia and her card was under her supervision. Another more detrimental case befell the victim in Jakarta due to a credit card break-in by a perpetrator from Palembang, which caused a loss of IDR 1.1 billion. These three cases confirm that the banking digital security system still has loopholes that endanger consumers.

In the context of national law, consumer protection is regulated in Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, OJK Regulation No. 6/POJK.07/2022 concerning Consumer

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

and Community Protection in the Financial Services Sector. Meanwhile, from the perspective of Islamic law, DSN-MUI Fatwa Number 54/DSN-MUI/X/2006 provides a sharia basis for customer protection through the principles of justice and legal contracts.

Previous studies on this problem have also been carried out by several researchers before. Annisa Medyana Akhiar's research entitled "Forms of Legal Protection and Bank Responsibility for Credit Card User Losses Due to Negligence in Supervision by Banks", emphasizes the importance of banks' responsibility for negligence in supervising their systems. The main focus of the study was on how banks should act actively to protect consumers from credit card crime. Meanwhile, research by Brigita Cynthia Liwandra Denata and Luluk Lusiati Cahyarini entitled "Legal Protection for Credit Card Holders for Unjustified Bills", focuses more on the need for transparency and customer rights in dealing with invalid bills. This research emphasizes the responsibility of banks in managing transactions accurately and responsibly. In contrast to the two studies, this study not only examines bank responsibility from a positive legal perspective, but also examines this issue from the sharia perspective by referring to DSN-MUI Fatwa Number 54/DSN-MUI/X/2006.

This study aims to find out the normative review of consumer protection regulations in the financial services sector (banks), to analyze DSN-MUI's fatwa on unauthorized transactions and forms of customer protection, to find out the form of protection provided by banks to credit card users, and, to find out the form of responsibility of banks for illegal transactions experienced by customers.

Thus, this study is expected to provide a comprehensive understanding of the urgency of legal protection for consumers who use credit cards, as well as assess banks' normative and sharia responsibilities for the occurrence of adverse illegal transactions.

II. RESEARCH METHODS

The type of research is juridical-normative, with a conceptual approach and a statute approach [2]. The conceptual approach is used to see the perspective of DSN MUI fatwa Number 54/DSN/MUI/X/2006 on consumer protection for credit card holders against transaction bills that are not made by customers. The statute approach is used to analyze laws and regulations related to this issue, including Law Number 8 of 1999 concerning Consumer Protection, Law Number 10 of 1998 concerning Banking, Law Number 27 of 2022 concerning Personal Data Protection, POJK No. 6/POJK.07/2022 concerning Consumer Protection in the Financial Services Sector and other regulations. Data is collected through document studies and then data is processed qualitatively and analyzed using deductive logic.

III. RESULTS AND DISCUSSION

A. Normative Review of Consumer Protection Regulations in the Financial Services Sector (Banks)

Consumer protection is an essential aspect of the national legal system that aims to maintain a balance between the interests of business actors and consumer rights. In the context of the financial services sector, especially banking, this protection is becoming increasingly important as the complexity of digital financial services increases and the potential risk of data misuse, electronic fraud, and illegal transactions that are not carried out by the customer itself. Normatively, consumer protection has received recognition and legal guarantees through various laws and regulations [3].

One of the most basic legal bases is Law Number 8 of 1999 concerning Consumer Protection (UUPK). In Article 4 of the UUPK, it is explained that consumers have the right to comfort, security, and safety in using goods and/or services, including financial services provided by banks [4]. This article is the constitutional basis for protecting customers from the risk of losses due to unsafe services or inadequate security systems from banks.

The Customer's rights are: a) The Customer has the right to receive protection for savings or accounts deposited in a bank. Based on Article 29 paragraph (3) of Law No. 8 of 1999 concerning Consumer Protection. Based on the principle of prudence, b) The Customer has the right to obtain information related to the possibility of the risk of loss in connection with the customer's transactions made through the bank. Based on Article 29 Paragraph (4) of the UUPK, c) The Customer is entitled to compensation for funds or accounts lost or stolen from the bank holding the deposit rights. In addition, there is also legal protection received by depository customers against all risks of loss arising from a policy or arising from business activities carried out by the bank [5].

In addition to the UUPK, Law Number 10 of 1998 concerning Amendments to Law Number 7 of 1992 concerning Banking is also an important legal basis in providing protection to customers. This law regulates the principles, functions, and activities of banking business that must be carried out with the principle of prudential banking and responsibility in managing public funds [6]. In Article 29 paragraph (2) of the Banking Law, it is stated that banks are required to have an internal control system and a reliable information system to ensure the implementation of banking business activities in a healthy and reasonable manner.

In addition, strengthening the protection of customer data is also strengthened by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) [7]. This law confirms that every data controller, including banks and financial institutions, is obliged to keep customers' personal data secure and prevent illegal access by third parties. In the context of credit card break-ins, the bank's negligence in maintaining personal data such as card numbers and transaction data is a violation of the provisions of Article 39 and Article 58 of the PDP Law. If there is a data leak that causes losses, the bank can be subject to administrative and criminal sanctions in accordance with Article 67 and Article 70 of the PDP Law. Therefore, consumer protection in the digital era is not only related to the security of the transaction system, but also the comprehensive protection of personal data managed by banks.

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

This provision explicitly asserts that banks have a legal and operational obligation to ensure that their systems are safe, accurate, and protected from leaks and abuse. If the bank fails to implement a proper security system that results in a break-in or illegal transaction, then the bank can be held accountable by law.

Protection of consumers is also affirmed in Financial Services Authority Regulation (POJK) No. 6/POJK.07/2022 concerning Consumer and Community Protection in the Financial Services Sector [8]. This POJK contains technical provisions for all financial services business actors, including banks, in ensuring holistic consumer protection, namely through:

1) Information Transparency

Every financial institution is obliged to provide clear and accurate information to consumers about the products and services offered.

2) Protection of Consumer Personal Data

Financial institutions must not misuse or leak consumers' personal data, and are obliged to protect such data from unauthorized third parties.

3) Complaint and Dispute Resolution Services

POJK requires banks to provide an easily accessible, responsive complaint mechanism, and fair dispute resolution.

4) Liability for Losses Due to System Errors

In the event of a system failure or procedural error that is detrimental to consumers, the responsibility lies with the bank, unless it can be proven that the customer has committed gross negligence. This regulation emphasizes the principle of bank responsibility for the security and validity of transactions carried out digitally. For example, in the event of a transaction with a significant value that is not acknowledged by the customer, the bank cannot immediately charge the bill unless there is strong evidence that the customer is negligent, such as voluntarily giving the OTP to another party.

Article 1365 of the Civil Code (KUHPerdata) can also be used as the basis for a lawsuit against the bank if there is a loss due to negligence or unlawful acts. Consumers can sue the bank if it can be proven that the losses experienced are the result of non-fulfillment of legal obligations by the bank, for example the absence of system security or failures in the transaction authorization process [9]. According to Law No. 11 of 2008 No. Law No. 19 of 2016 concerning Electronic Information and Transactions (ITE Law), it emphasizes the protection of electronic systems and personal data, which is very relevant in the context of digital financial transactions. If the bank does not have a system that complies with digital security standards, then it is a form of negligence that can be processed legally.

OJK Circular Letter No. 14/SEOJK.07/2014 regulates the importance of an effective consumer complaint service system. When problems occur, customers have the right to get a transparent complaint channel that can be followed up with a fair solution. Bank Indonesia Regulation (PBI) No. 16/1/PBI/2014 concerning Consumer Protection of Payment System Services also strengthens this. This PBI stipulates that payment system operators, including banks, are obliged to provide protection to consumers for the use of payment instruments, both in terms of system security, clarity of information, and dispute resolution. Banks are also required to ensure that every digital transaction must go through strong authentication stages, such as One Time Password (OTP), biometrics, or similar technology. If the system fails to provide notification or verification, then the bank must be responsible for the losses incurred, unless there is negligence on the part of the customer.

This is especially relevant to the following credit card breach cases:

1) Jenius (Bank BTPN) customer case – Fictitious transaction of IDR 22 million from the US (June 2023)

The customer received a bill for a transaction of IDR 22 million made from the United States, even though he had never traveled abroad and did not receive an OTP request at all. This case shows the failure of the authentication and supervision system on the part of the bank, which is directly contrary to the provisions of PBI No. 16/1/PBI/2014 and POJK No. 6/POJK.07/2022 related to the responsibility of financial institutions for losses due to system errors. The absence of notifications or OTPs is evidence of weak transaction verification, so banks cannot immediately impose responsibility on customers.

2) *Case of Mira, BCA customer – Credit card break-in from Singapore via Netflix (December 2022 – January 2023*)

The transaction occurred six times through Netflix even though the physical card was in Mira's hand in Indonesia and without OTP delivery. This indicates that there is illegal access to credit card data that should be protected to the maximum by banks. According to Article 1365 of the Civil Code and the ITE Law, banks can be sued for negligence or failure of security systems, including in terms of personal data protection. What's more, POJK and PBI emphasize banks' obligations to maintain the security of cross-border transactions and safeguard consumers' rights to obtain a valid authorization system.

3) The case of break-in by Riandi and Davis with a loss of IDR 1.1 billion (Palembang – Jakarta)

This case shows how cybercriminals from outside the victim's domicile can take advantage of loopholes in the banking system to conduct transactions without valid authorization. If the transaction is not detected quickly by the bank's system, or the system does not perform appropriate verification (such as IP Address location, real-time notifications, or OTPs), then this is a violation of the principles of "know your customer" and risk management as stipulated in the PBI, as well as the principles of transparency and consumer protection according to POJK and the Banking Law.

The three cases above show that weaknesses in the digital banking security system can lead to huge losses that should not be charged to consumers. Based on various regulations that have been mentioned, both from the Banking Law, PBI No. 16/1/PBI/2014, POJK No. 6/POJK.07/2022, the ITE Law, to the Civil Code, the legal responsibility for the failure of the verification and risk control system lies with the bank.

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

Therefore, in this digital era, consumer protection must be the main orientation of banking policy, not just an administrative formality. Regulatory alignment with consumers is the foundation of public trust in a fair, accountable, and sustainable national financial system [10].

B. DSN-MUI Fatwa Review Against Illegal Transactions and Customer Protection

Consumer protection is very important in Islamic law. In Islam, consumer protection law refers to economic justice based on Islamic economic principles [11]. DSN-MUI Fatwa Number 54/DSN-MUI/X/2006 concerning Sharia Credit Cards emphasizes the importance of the principles of fairness, transparency, and protection of customers in every financial transaction. Although it does not explicitly discuss illegal or unauthorized transactions, the substance of this fatwa contains basic sharia values that can be used as a basis to protect customers from losses arising from credit card misuse [12].

One of the main principles in sharia transactions is the akad (legal agreement). Transactions that are not based on a clear contract or do not obtain the consent of the customer are considered invalid in the perspective of Islamic law. Therefore, charging customers for transactions that have never been carried out or are not approved is clearly contrary to the principles of justice and sharia principles.

The following three cases reflect the importance of customer protection, especially for credit card holders:

1) The Case of Bank BTPN Jenius

In June 2023, a Bank BTPN customer through a Jenius credit card received a bill of IDR 22 million for transactions that occurred in the United States. He admitted that he had never been abroad and did not receive an OTP code during the transaction.

If analyzed from the perspective of DSN-MUI Fatwa No. 54/2006 [13]: First, the transaction is not carried out on the basis of a valid contract, because there is no consent from the card owner. Second, the absence of an OTP request is proof that the bank's security system has failed to implement the prudential principle. Third, in sharia, the principle of "al-ghurm bil-ghunm" (there should be no loss without profit) is the basis that the customer should not bear losses for transactions that he did not make.

2) Mira Case BCA Credit Card Break-In from Singapore

Mira, a BCA credit card customer, was a victim of a card breach by a party that made six transactions through the Netflix service from Singapore, even though she was in Indonesia and never gave approval or received an OTP. In sharia, this transaction contains elements of gharar (ambiguity) and zulm (injustice), because there is no contract or authorization from the cardholder; *then* the bank does not succeed in preventing suspicious foreign transactions, even though the card physically does not change hands and the DSN Fatwa states that fees (ujrah) are only valid if the services or benefits are actually provided and approved by the customer.

3) Break-in Case by Riandi and Davis – Loss of IDR 1.1 Billion

This case involved a credit card break-in with a loss value of Rp 1.1 billion. The perpetrator was domiciled in Palembang, while the victim was in Jakarta. Transactions that occurred without permission and with the victim's knowledge again showed the bank's weak security system. Within the framework of the DSN-MUI fatwa: *First*, banks as card issuers have a moral and legal responsibility to ensure the security of data and transactions. *Second, the* failure to prevent large-scale break-ins reflects the non-fulfillment of the principle of trust that is the basis of the relationship between customers and Islamic financial institutions. *Third,* the act of imposing losses on the victim is contrary to the value of justice upheld in Islam.

The three cases above show that the principles in the DSN-MUI Fatwa No. 54/2006 are very relevant to be applied in dealing with the dynamics of digital crime in the banking sector. The essence of the fatwa emphasizes that:

1) Banks are obliged to provide reliable and accountable security systems;
2) Transactions that do not have the customer's approval do not have a legal basis either in sharia or positive law;
3) The initial responsibility lies with the bank, not the customer, especially when the security system fails to perform its functions.

Thus, this fatwa not only serves as a technical guide for the implementation of sharia credit cards, but also as a consumer protection instrument that emphasizes the principles of justice, trust, and prudence [14].

C. The form of protection provided by banks for credit card users

The UUPK provides an important legal basis in protecting the rights of consumers, including credit card users. The relevance of the case of Jenius and Mira, the consumer did not receive the OTP request and felt that he did not make a transaction. This refers to Article 4 letters a and c, where consumers are entitled to security and correct information. Article 19 of the UUPK gives consumers the right to get compensation if it is proven that the loss is not due to their negligence. In both cases, the consumer is in Indonesia and did not receive the OTP, indicating no negligence on their part. The case of the break-in by Riandi and Davis shows that the losses occurred due to external crimes. If the bank does not have an adequate security system, then under Article 8 and Article 19, the bank can be held liable for losses [15].

Law No. 10 of 1998 concerning Banking requires banks to carry out the principle of prudence and maintain the confidentiality of customer data. Relevance to all three cases, transactions are carried out from abroad, without OTP. This shows the possibility of data leakage, violations of Article 29 paragraph (2) concerning internal control, and potential violations of Article 40 regarding the confidentiality of customer data. If the data security system is inadequate so as to cause an invalid transaction, then the bank violates Article 2 on the obligation to implement the principle of prudence [16].

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

In addition to the regulations that have been mentioned, the protection of credit card users is also strengthened by Law Number 27 of 2022 concerning Personal Data Protection (PDP Law). This law is an important milestone in ensuring the security of customers' personal data, especially in digital banking transactions. In Article 39 of the PDP Law, it is stipulated that data controllers, including financial services institutions such as banks, have an obligation to protect personal data from being illegally accessed by unauthorized parties. This includes sensitive information such as credit card numbers, verification codes (CVVs), and transaction data. Furthermore, Article 58 paragraph (1) states that failure to prevent unauthorized access to personal data is a violation of the law. If this causes losses to the data subject (in this case the customer), then according to Article 67 and Article 70, the bank may be subject to administrative or criminal sanctions, depending on the level of the error and its impact.

The relevance of the PDP Law is very evident in the case of Mira (BCA customer) and Jenius Bank BTPN customer. In both cases, the customer never gave approval for transactions made from abroad and did not receive OTP notifications. This indicates the possibility of leakage or misuse of customers' personal data, which should be under the full supervision and responsibility of the bank as the data controller. If it is proven that the bank is negligent in implementing the data security standards set out in the PDP Law, then the bank can not only be held civilly liable under the UUPK, but can also be subject to sanctions according to the PDP Law.

Furthermore, PBI No. 14/2/PBI/2012 concerning Credit Cards regulates the protection of credit card consumers through information transparency, complaint resolution, and data security [17]. The relevance to the case is that Article 9 requires banks to provide accurate information about transaction risks. If the customer does not understand the risk of a cross-border break-in, the bank may be considered negligent. Then, Articles 22-24 require banks to provide complaint services. In the case of Jenius and Mira, the customer has the right to file a complaint and receive a prompt and fair response. And Article 28 requires data protection. The cases of Mira and Jenius show a failure in the data protection system (no OTP), which can be evidence of this PBI violation.

Based on POJK No. 1/POJK.07/2013 and POJK No. 6/POJK.07/2022, the principles of consumer protection are established, including justice, information disclosure, and complaint handling. The relevance to the case is *First,* the Principle of Information Disclosure: If the bank does not notify the potential risk of international transactions without an OTP, then it violates the principle of openness. Complaint Handling: The bank is obliged to resolve the complaint within 20 working days. In the case of Jenius, if the complaint is not acted upon immediately, the bank violates this provision. *Second,* Responsibility for Unauthorized Transactions: If the bank does not prove that its system has contributed and reliable in preventing fraud, then according to POJK, the bank is responsible for customer losses.

D. Form of Responsibility by the Bank for Illegal Transactions Experienced

Illegal transactions experienced by bank customers, especially credit card holders, are an increasingly frequent occurrence as the digitization of payment systems increases. In the legal context, banks have an absolute responsibility to protect customers from all forms of data misuse and unauthorized transactions. These responsibilities are comprehensively regulated in various national legal instruments and sharia fatwas.

First, according to Law No. 8 of 1999 concerning Consumer Protection (UUPK), banks as business actors are obliged to provide protection to consumers from losses due to the negligence of service providers. In Article 4 and Article 7, it is emphasized that consumers have the right to a sense of security and business actors are responsible for losses due to the use of traded goods and/or services. If the customer suffers losses due to a credit card breach, the bank is obliged to compensate the loss if it is proven that there is a system or service security negligence [18].

Second, Law No. 10 of 1998 concerning Banking states that banks are obliged to apply the principle of prudence in all their business activities (Article 29 paragraph 3). If there is a credit card breach and the bank cannot prove that the transaction was carried out legally by the customer, then the bank can be considered negligent in carrying out the function of supervision and security of its system.

Third, Law Number 27 of 2022 concerning Personal Data Protection (PDP Law) is also a very important legal instrument in determining the form of bank responsibility for illegal transactions experienced by customers. This law expressly regulates the obligation of every personal data controller (including banks) to maintain the security, integrity, and confidentiality of customer data from unauthorized access.

Fourth, POJK No. 1/POJK.07/2013 concerning Consumer Protection in the Financial Services Sector emphasizes that financial service institutions are obliged to provide a consumer complaint system and resolve it effectively and fairly. Article 29 of the POJK emphasizes the bank's responsibility to address system errors, abuses, or negligence that cause losses to consumers. This is in line with the principles of transparency, accountability, and fairness in financial services. Bank Indonesia (PBI) regulations such as PBI No. 16/1/PBI/2014 and PBI No. 18/40/PBI/2016 stipulate that payment system service providers are obliged to ensure the security and reliability of the payment system [19]. When illegal transactions occur due to weak system security or negligence in verifying transactions (e.g. no OTP request), then the bank must be fully responsible for the losses suffered by the customer [20].

Fifth, from a sharia perspective, DSN-MUI Fatwa No. 54/DSN-MUI/X/2006 concerning Sharia Credit Cards emphasizes the importance of the principle of justice (al-'adl) and trust in carrying out contracts. If there is a transaction that is not carried out by the customer, the bank must first investigate and prove the validity of the transaction. If it is not proven, then the burden of payment should not be charged to

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

the customer. This fatwa affirms that profits obtained from transactions that contain ambiguity (gharar) or fraud (tadlis) are haram and such transactions are considered fasid (legal defects) [21].

The following are three cases that reflect the weak protection of credit card customers and the importance of bank accountability:

1) Bank BTPN Jenius Case (June 2023)

A Jenius customer from Bank BTPN shared his experience through the Twitter account @yourlastnameis, that he was billed IDR 22 million for a credit card transaction that he did not make. The transaction takes place in the United States, while the customer is in Indonesia and does not receive an OTP code request. This indicates the potential for data leaks or a double verification system that fails to function. In the legal context, banks should not necessarily charge the customer the bill, but rather conduct a thorough investigation and provide compensation if it is proven that it is not the customer's fault.

2) Case of Mira, BCA Credit Card Customer (December 2022 - January 2023)

Mira had a break-in of a credit card used to transact six times on Netflix from Singapore, even though she had never been abroad and the credit card remained in her hands. No OTP request came in when the transaction occurred. This case highlights the weak system of transaction location detection and double verification by banks. If referring to POJK and PBI, this failure shows systemic negligence that makes the bank subject to administrative sanctions and obliged to compensate customers for losses.

3) Rp 1.1 Billion Break-in Case by Riandi and Davis

In this case, two perpetrators named Riandi and Davis broke into the credit card of the victim who lived in Jakarta, while the perpetrator was in Palembang. The total losses suffered by the victims reached Rp 1.1 billion. This case illustrates the weak protection and fraud detection system by banks, as well as the importance of cooperation between banks, network providers, and legal authorities. If the bank is unable to identify and prevent such suspicious transactions, then the bank is legally obliged to be responsible for the loss.

If the bank fails to carry out its responsibilities as stipulated in laws and regulations and sharia fatwas, there are several legal consequences that can be imposed. Based on Article 62 of the UUPK, business actors who violate the provisions of the UUPK can be subject to criminal sanctions in the form of a maximum prison sentence of five years or a maximum fine of Rp 2 billion [22]. In addition, customers can also claim compensation through a civil lawsuit. Sanctions according to the Banking Law, Banks that violate the principle of prudence and cause losses to customers may be subject to administrative sanctions by Bank Indonesia or the Financial Services Authority. These sanctions include reprimands, freezing of business activities, and revocation of business licenses. If a serious violation is found, corporate criminal liability or criminal liability may be imposed on the bank management.

Based on the PDP Law, in the context of illegal transactions, if it is proven that the customer's personal data such as credit card numbers, OTPs, or other authentication information has been accessed by a third party without permission, the bank can be considered negligent in carrying out its obligations in accordance with Article 39 and Article 58 of the PDP Law. Failure to prevent the leakage of personal data is a form of violation of the law that can be subject to administrative sanctions (Article 67) or even criminal sanctions (Article 70) if the losses are massive and intentional.

In POJK No. 1/POJK.07/2013, violations of consumer protection provisions can be subject to administrative sanctions in the form of: a) Written reprimand, b) Administrative fines, c) Restrictions on business activities, d) Freezing of business activities, e) Revocation of business licenses. PBI gives authority to Bank Indonesia to impose sanctions on banks that neglect to maintain the security of the transaction system. Sanctions by PBI include: a) Written warning, b) System repair obligations, c) Fines, d) Freezing of certain services, e) Additional sanctions in accordance with BI's policy.

Meanwhile, according to the Fatwa, DSN-MUI is not criminally or administratively binding, but has normative power in the Islamic financial system. Violation of the fatwa can cause: a) The declaration of the contract as fasid (legal defect), b) The profits obtained from illegal transactions are considered ghulul (not halal), c) Sharia moral and ethical sanctions enforced by the Sharia Supervisory Board (DPS), d) Potential dispute resolution through the National Sharia Arbitration Board (BASYARNAS).

To reduce and avoid the risk of illegal transactions that are detrimental to customers, prevention efforts must be carried out comprehensively through two main approaches, namely preventive and repressive.

1) Preventive Prevention (Prevention Before A Violation Occurs)

This effort is anticipatory and aims to prevent illegal transactions from happening in the first place. The form includes:

a) Improvement of Digital Security Systems: Banks are required to regularly upgrade technological security systems, including two-factor authentication (2FA), encrypted OTP delivery, biometric verification, and suspicious transaction detection algorithms.

b) Periodic Audits of Security and Operational Systems: Conduct security audits and penetration tests regularly to identify security gaps that have the potential to be exploited by third parties or hackers.

c) Continuous Customer Education: Improving consumer digital literacy by conveying information on the risk of digital fraud, the importance of safeguarding personal data, and reporting methods in the event of transaction irregularities. This is in accordance with the mandate of Article 4 and Article 6 of the UUPK.

d) Implementation of Know Your Customer (KYC) and Anti-Money Laundering (AML) Principles: Strict implementation of KYC and AML can minimize identity

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

misuse and prevent the entry of criminals into the banking system.

e) *Socialization of DSN-MUI Fatwa in Sharia Banking:* Sharia banks need to emphasize the importance of the validity of contracts and fairness in the implementation of financial transactions, in accordance with sharia principles that prohibit unilateral losses (gharar and zulm).

2) *Repressive Prevention (Prevention After Violation)*

This approach is carried out to deal with violations that have occurred, ensure accountability, and provide a deterrent effect. The form includes:

a) *Prompt and Transparent Handling of Customer Complaints:* Banks must have a responsive complaint service unit and a fair and efficient dispute resolution mechanism. Handling must be carried out for a maximum of 5 working days in accordance with the provisions of POJK No. 6/POJK.07/2022.

b) *Providing Compensation to Injured Customers:* In accordance with Article 19 of the UUPK and the provisions of POJK, banks are obliged to provide refunds to customers for illegal transactions that are not recognized and are not caused by their negligence.

c) *Implementation of Sanctions on Negligent Banks:* The Financial Services Authority (OJK) needs to impose strict administrative sanctions (warnings, fines, restrictions on business licenses, and revocation of licenses) to banks that are proven to be negligent in maintaining security systems and violating consumer protection obligations.

d) *Cooperation with Law Enforcement Officials:* In cases of major breaches, banks are required to cooperate with the police and cyber crime investigators to trace the perpetrators and thoroughly investigate the digital crime network.

e) *System Evaluation and Internal Correction:* After a case of illegal transactions, the bank must conduct a thorough internal audit and fix security loopholes, SOPs, and verification flows so that similar incidents do not happen again.

By combining preventive and repressive approaches, banks can provide comprehensive protection to customers, while increasing public trust in the national banking system. This is in line with the principles of justice, responsibility, and legal protection which are at the core of the national legal system and sharia principles.

Therefore, it is important for regulators such as OJK and Bank Indonesia to increase periodic supervision and evaluation of digital transaction security systems in banks. On the other hand, banking institutions also need to strengthen their education and consumer protection systems, as well as provide a fast and effective complaint channel for customers who are victims of illegal transactions. In the context of Islamic banking, compliance with the DSN-MUI fatwa is not only normative, but is the main foundation in ensuring halal and fairness in every financial transaction. Thus, the synergy between regulations, financial institutions, supervisory authorities, and consumer awareness is the main key in building a safe, transparent, and fair financial system both in terms of positive law and Islamic law.

IV. CONCLUSION

This study concludes that the protection of credit card holders who experience illegal transactions is the main responsibility of banks, both legally positive and from a sharia perspective. The Consumer Protection Law, the Banking Law, the PDP Law, POJK, and PBI expressly require banks to ensure system security, information transparency, and provide a fair complaint and dispute resolution mechanism. When a transaction occurs that is not carried out by the customer, the bank is obliged to investigate and provide compensation if it is proven that it is not the customer's fault.

From the sharia side, DSN-MUI Fatwa Number 54/DSN-MUI/X/2006 emphasizes the importance of a valid contract, justice, and trust in every transaction. Transactions made without the consent or knowledge of the customer have no legal force and cannot be charged to the customer. Therefore, the responsibility for losses due to illegal transactions lies entirely on the bank's side.

The three cases analyzed in this study show that the digital banking security system still has loopholes, and legal protection for consumers is not fully optimal. Preventive (such as improving consumer security and education systems) and repressive efforts (such as providing compensation and sanctions for bank negligence) must be carried out comprehensively to ensure trust and justice for customers inthe digital era. The integration between national law and sharia principles is an important foundation in creating fair and sustainable consumer protection.

REFERENCES

[1] A. Taqyanto and F. Zahara, "Hukum Penggunaan Dana TBDSP untuk Pembiayaan Operasional Bank Syariah dalam Perspektif Fatwa MUI NO.123/DSN-MUI/XI/2018 (Studi Kasus Bank Sumut Syariah KCP Marelan Raya)," *J. Akunt. dan Pajak*, vol. 23, no. 2, pp. 1–9, 2022, [Online]. Available: https://jurnal.stie-aas.ac.id/index.php/jap/article/view/7397

[2] J. Ibrahim, *Teori dan Metodologi Penelitian Hukum Normatif dan Empiris*. Malang: Bayumedia Publishing, 2015.

[3] A. Sofyan, *Hukum Perlindungan Konsumen di Indonesia*. Jakarta: Kencana Prenada Media Group, 2013.

[4] *Undang-Undang Nomor 8 Tahun 1999 tentang Perlindungan Konsumen*.

[5] M. J. Kusuma, *Hukum Perlindungan Nasabah Bank*. Bandung: CV. Hikam Media Utama, 2020.

[6] *Undang-Undang Nomor 10 Tahun 1998 tentang Perbankan*.

[7] *Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi*.

[8] *Peraturan OJK Nomor 6/POJK.07/2022 tentang*

Volume 09, Number 02, Page 1245-1252
e-ISSN: 2598-120X; p-ISSN: 2598-117X

Perlindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan.

[9] V. A. Romdani, R. I. Tektona, and E. Zulaika, "Analisis Yuridis Kasus Card Trapping pada Nsabah BNI dalam Perspektif Hukum Perdata," *J. Supremasi*, vol. 15, no. 1, pp. 89–103, 2025.

[10] E. Irmawati, J. Pieries, and W. S. Widiarty, "Perlindungan Hukum atas Data Pribadi Nasabah Bank Pengguna Mobile Banking dalam Perspektif UU No 27 Tahun 2022 tentang Kebocoran Data," *J. Syntax Admiration*, vol. 5, no. 1, pp. 12–27, 2024, doi: https://doi.org/10.46799/jsa.v5i1.964.

[11] Zulham, *Hukum Perlindungan Konsumen*. Jakarta: Kencana, 2013.

[12] Mardani, *Hukum Ekonomi Syariah di Indonesia*. Jakarta: Kencana Prenadamedia Group, 2015.

[13] *Fatwa No. 54/DSN-MUI/X/2006 tentang Kartu Kredit Syariah*.

[14] S. J. Putra, Y. Yudesman, and S. Iska, "Analisis Hukum Ekonomi Syariah terhadap Fatwa DSN-MUI Nomor 54 Tahun 2006," *MARAS J. Penelit. Multidisiplin*, vol. 1, no. 3, pp. 532–542, 2023, doi: 10.60126/maras.v1i3.99.

[15] N. P. D. A. K. Prabandari, I. N. P. Budiartha, and A. A. S. L. Dewi, "Perlindungan Hukum Bagi Konsumen Nasabah BANK Pemegang Kartu Kredit yang Dibebankan Biaya Tambahan (Surcharge) oleh Merchant dalam Transaksi Pembayaran," *J. Prefer. Huk.*, vol. 3, no. 1, pp. 126–131, 2022, doi: 10.22225/jph.3.1.4671.126-131.

[16] B. C. L. Denata and A. Putrijanti, "Perlindungan Hukum bagi Pemegang Kartu Kredit atas Tagihan yang Tidak Benar," *Notarius*, vol. 16, no. 3, pp. 1483–1498, 2023, doi: 10.14710/nts.v16i3.40817.

[17] *Peraturan Bank Indonesia Nomor 14/2/PBI/2012 Tahun 2012 tentang Perubahan atas Peraturan Bank Indonesia Nomor 11/11/PBI/2009 tentang Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu*.

[18] N. T. Prayoga, I. N. Sujana, and N. M. P. Ujianti, "Perlindungan Hukum Nasabah Kartu Kredit dalam Perspektif Undang-Undang Nomor 8 Tahun 1999," *J. Prefer. Huk.*, vol. 2, no. 1, pp. 145–149, 2021, doi: 10.22225/jph.2.1.3060.145-149.

[19] *Peraturan Bank Indonesia Nomor 18/40/PBI/2016 Tahun 2016 tentang Penyelenggaraan Pemrosesan Transaksi Pembayaran*.

[20] Y. Setiawan, "Perlindungan Hukum terhadap Pemegangan Kartu Kredit dalam Klausula Baku Legal," *J. Commer. Law*, vol. 2, no. 1, 2022, doi: https://doi.org/10.29303/commercelaw.v2i1.1362.

[21] N. Faris and M. Winario, "Perlindungan Konsumen dalam Perbankan Syariah: Perspektif Hukum Ekonomi Syariah," *Multidiscip. J. Relig. Soc. Sci.*, vol. 1, no. 1, pp. 29–39, 2024, doi: 10.69693/mjrs.v1i1.46.

[22] W. Trihafsari and C. Permata, "Consumer Protection in Beach Tourism Objects From the Perspective of Maqashid Sharia (Study in the Sub-District of Mirror Beach, Serdang Bedagai District)," *Istinbath*, vol. 23, no. 1, pp. 202–214, 2024, doi: 10.20414/ijhi.v23i1.746.