EL-ECOSY: JURNAL EKONOMI DAN KEUANGAN ISLAM
Vol. 05, No. 02 July 2025, Pages. 151-164
Available at https://jurnal.unsur.ac.id/elecosy/index

ANALYSIS OF SKIMMING ACTIONS IN SHARIA BANKING TRANSACTIONS: A SHARIA ECONOMIC LAW PERSPECTIVE

Reksa Jayengsari[1*], Alfira Eka Fauziah[2]
[1*,2]Magister Akuntansi Universitas Islam Bandung
**Corresponding Author Email:*reksaecha22@gmail.com,
alfiraekafauziah02@gmail.com

Recieved: May 2025	Accepeted: June 2025	Published: July 2025

ABSTRAK

Teknologi informasi dan komunikasi di industri keuangan syariah terus berkembang. Kemajuan tersebut memungkinkan pula berkembangnya tindakan kejahatan digital salah satunya adalah Skimming. Skimming adalah jenis kejahatan digital dimana data nasabah dicuri secara ilegal melalui perangkat tersembunyi di ATM atau alat pembayaran elektronik. Studi ini bertujuan untuk menyelidiki bagaimana transaksi skimming terjadi dalam perbankan syariah dari perspektif hukum ekonomi syariah. Penelitian ini menggunakan pendekatan kualitatif dengan metode deskriptif analitis. Data berasal dari undang-undang perbankan syariah, buku hukum Islam, laporan lembaga keuangan, dan kasus skimming yang terjadi. Hasil penelitian menunjukkan bahwa prinsip-prinsip hukum ekonomi syariah seperti keadilan, amanah, dan perlindungan harta (ḥifẓ al-māl) bertentangan dengan tindakan skimming. Selain itu, tindakan ini memenuhi unsur ghasab, yang berarti pengambilan tanpa izin, tadlis, yang berarti penipuan, dan sariqah, yang berarti pencurian. Jika kelalaian sistem menyebabkan skimming, bank syariah bertanggung jawab secara hukum dan moral untuk melindungi klien. Studi ini membantu perkembangan literatur hukum ekonomi syariah tentang kejahatan siber dan mendorong perbankan syariah untuk meningkatkan sistem keamanan yang didasarkan pada nilai-nilai Islam.

Kata Kunci: Bank Syariah; Hukum Ekonomi Syariah; Keamanan Digital; Maqashid Syariah; Skimming

ABSTRACT

Information and communication technology in the Islamic financial industry continues to develop. This progress also allows for the development of digital crime, one of which is skimming. Skimming is a type of digital crime in which customer data is stolen through hidden devices installed in ATMs or electronic payment devices. This study aims to investigate how skimming transactions occur in Islamic banking from the perspective of Islamic economic law. This study uses a qualitative approach with analytical descriptive methods. The data comes from Islamic banking laws, Islamic law books, financial institution reports, and cases of skimming that have occurred. The results of the study demonstrate that the principles of Islamic economic law, such as justice, trustworthiness, and the protection of assets (ḥifẓ al-māl), are incompatible with skimming actions. In addition, this

action fulfills the elements of ghasab, which means taking without permission, tadlis, which means fraud, and sariqah, which means theft. If system negligence causes skimming, Islamic banks are legally and morally responsible for protecting clients. This study contributes to the development of Islamic economic law literature on cybercrime and encourages Islamic banking to enhance its security systems by Islamic values.
Keywords: *Digital Security, Islamic Bank; Islamic Economic Law; Maqashid Syariah; Skimming*

A. INTRODUCTION

The Islamic financial industry, comprising Islamic banks, has undergone a significant transformation due to advancements in information and communication technology. Digital financial tools, including ATMs, debit cards, mobile banking, and internet banking, have made financial transactions easier for the public. More than 98% of transactions are conducted digitally through mobile banking applications (Bank Indonesia, 2023). Several central Islamic banks in Indonesia, such as Bank Syariah Indonesia (BSI), have noted the continued growth of e-banking and mobile banking in the Islamic banking sector. This indicates that consumers are becoming increasingly reliant on technology for financial transactions. In Indonesia, Islamic financial technology (fintech) is experiencing rapid growth. Islamic fintech transactions in Indonesia reached USD 6.1 billion in 2023 and are expected to increase to USD 11 billion by 2027.

This development aligns with the government's efforts to enhance public participation and understanding of Islamic finance nationwide. With a compound annual growth rate (CAGR) of around 17%, the Islamic fintech industry is projected to reach USD 306 billion globally by 2027. This growth is driven by the increasing demand for Sharia-compliant financial services, particularly in Muslim-majority countries, as well as the widespread adoption of digital technology (Financial Services Authority, 2023).

With the development of data and advances in information and communication technology in the banking sector, digital crimes such as skimming and theft of customer data by attaching illegal devices to ATMs have also become possible. Skimming is a form of crime that utilizes electronic devices, such as skimmers, to duplicate customer ATM card information (Romli, L., 2015). The

Financial Services Authority (OJK) (2021) defines skimming as the theft of customer debit and credit card data using a special device called a skimmer, which copies data from the card's magnetic strip. This data is then used to withdraw funds without the customer's knowledge.

According to data from the Financial Transaction Reports and Analysis Center (PPATK), digital-based banking crimes, including skimming, are increasing year after year. Meanwhile, according to data from the Financial Services Authority (OJK), hundreds of public reports regarding alleged ATM skimming were recorded in various regions of Indonesia throughout 2022 and 2023, including those involving Islamic banks. From 2013 to May 2023, the OJK received 72,618 complaints related to fraudulent methods, including skimming, phishing, social engineering, and sniffing, which accounted for 6.5 percent of the 1,116,175 complaints filed.

The 2022 BSI sustainability report noted that the Prima ATM network experienced 232 cases of suspected skimming. Sixty-four of these cases were on the ATM Bersama network. However, BSI stated that there were no complaints of material losses or violations of customer privacy (Katadata, 2023). In a case study published by Legal Reform in Nevita Sari (2020), BNI Syariah was required to refund all customer losses caused by credit card skimming and to return the funds within seven business days, by the Consumer Protection Law.

Skimming can have detrimental effects on both customers and banks. Customers can suddenly lose money without realizing that an irresponsible person has stolen and misused their ATM or debit card data. Furthermore, this practice creates a sense of insecurity when using digital banking facilities due to the violation of customer data privacy. One of the most common psychological effects is a loss of trust in the bank as an entity responsible for maintaining the confidentiality of customer data. For banks, skimming can harm the institution's image and reputation, especially for Islamic banks, which are based on trust and fairness. Banks are required to increase spending to strengthen security systems, such as implementing anti-skimming measures, improving transaction authentication technology, and developing more sophisticated fraud detection systems. Furthermore, banks must repay lost customer funds.

Skimming can result in losses for both customers and banks, in the form of refunds, reputational damage, and increased system security costs (Hamzah, 2005). Skimming crimes result in the loss of customer funds, violations of personal data protection, and a loss of trust in digital banking services (OJK, 2021).

Islamic banking, which operates based on Islamic sharia principles, particularly those concerning transactions, is naturally guided by the principles of justice (al-'adl), honesty (shidq), trustworthiness (amanah), and safeguarding the welfare (maslahah) of all parties. Skimming is a crime that violates positive law and the fundamental values of Islamic transactions. To safeguard public funds, Islamic banks must have strict security systems and risk mitigation procedures.

Any transaction that unjustly results in the loss of another person's assets is considered a sin under Islamic economic law. Consequently, illegal acts such as skimming violate the principles of justice (al-'adl) and honesty (shidq) in transactions (Antonio, 2001). Because they fail to safeguard assets (ḥifẓ al-māl) and instead cause damage to the Islamic financial system, cybercrimes such as skimming are contrary to the maqāṣid al-syarī‘ah (obligatory objectives of Islamic law) (Mardani, 2012).

Given this background, it is urgent to analyze skimming practices from the perspective of Islamic economic law, as solutions based on Islamic values can be used to address the challenges of the digital era, which is rife with potential errors. Therefore, the purpose of this study is to explain the definition and modus operandi of skimming in the Islamic banking transaction system, analyze skimming in Islamic banking transactions based on the principles of Islamic economic law, and examine the forms of accountability of Islamic banks to customers who experience losses due to skimming from a Sharia perspective.

This research is expected to enrich the study of Islamic economic law, particularly in addressing the growing complexity of cybercrime issues in the Islamic financial sector, and provide practical benefits for Islamic banks through recommendations for strengthening transaction security systems and customer protection based on Islamic principles.

B. METHODOLOGY

This study employed a qualitative approach. Qualitative research is a method for observing and understanding how individuals or groups address social or humanitarian issues (Creswell, 2014). The descriptive-analytical research method aims to provide an in-depth overview of skimming practices in Islamic banking transactions and examine them from the perspective of Islamic economic law.

This study utilized secondary data, obtained through library research, including Law Number 21 of 2008 concerning Islamic Banking, Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE) and its amendments, the Criminal Code (KUHP), and the DSN-MUI Fatwa regarding Islamic banking. Secondary data was also obtained from books and scientific journals on Islamic economic law, reports from the Financial Services Authority (OJK), Bank Indonesia (BI), and the Financial Transaction Reports and Analysis Center (PPATK), as well as current news reports related to skimming cases in Islamic banks, as well as studies on Islamic jurisprudence (fiqh muamalah) and the maqashid (maqashid) of sharia.

The data collection technique in this research was conducted through document studies of relevant laws and regulations, fatwas, literature, and academic publications. Content analysis was used to analyze the collected data. This will examine the meaning, content, and relevance of the legal material to the research object. The analysis was conducted systematically, descriptively, and critically.

C. RESULTS AND DISCUSSION

1. Skimming in Islamic Banking Transactions

Skimming, a type of cybercrime, involves the theft of customer data through unauthorized devices installed in ATMs or EDCs. Rohman (2020) states that skimming is a type of electronic banking crime that has evolved due to technological advances. Perpetrators exploit system weaknesses and customer negligence to obtain confidential information illegally. Sharia banks adhere to Islamic principles in their operations, but can still engage in cybercrimes like skimming. This is because their service infrastructure, including ATMs, EDCs, and

communication networks, still utilizes the same technology as conventional banks. As a result, the security vulnerabilities exploited by criminals are the same.

From the perspective of Law Number 21 of 2008 concerning Sharia Banking, the term skimming is not mentioned. However, this act can be considered an abuse of the Sharia banking system and a violation of prudential principles, which are the fundamental principles of Sharia banking in Indonesia. Article 27 states that Sharia banks are obliged to maintain the confidentiality of customer data and/or information. Because customer data is stolen and misused by both external and internal parties who fail to maintain integrity, the practice of skimming directly violates this principle. From the perspective of Law No. 11 of 2008 concerning Electronic Information and Transactions (ITE) and its amendments through Law No. 19 of 2016, skimming is carried out by illegally accessing ATM systems or EDC devices using tools designed to steal electronic information such as card numbers and PINs.

This falls under Article 30 paragraphs 1 and 2, for accessing another party's electronic system to obtain data without permission. Article 30 paragraph (1) states that any person who intentionally and without authority or unlawfully accesses another person's computer and/or electronic system by any means. Article 30 paragraph (2) states that any person who intentionally and without authority or unlawfully accesses a computer and/or electronic system by any means to obtain electronic information and/or electronic documents is guilty of a criminal offense.

Previous studies have shown that skimming still occurs in Islamic banks despite the use of several security technologies such as chip cards and data encryption. Several factors contribute to this, including a lack of customer digital literacy, insufficient public awareness about Islamic banking security, and inadequate internal bank oversight of ATMs and EDC devices. A study by Wahyudi & Haryono (2021) on ATM security systems in Islamic banks found that technical supervision and customer literacy were suboptimal, resulting in weaknesses. The Financial Services Authority (OJK) (2020) stated that one factor contributing to the increased likelihood of skimming fraud is the lack of regular physical audits of ATMs. Islamic banks do not frequently inspect the physical condition of ATMs; however, installing skimmers in less secure locations, such as dark, deserted areas

or those without CCTV, increases the likelihood of criminal fraud. According to Sari & Nasution (2022), a lack of awareness of digital banking security procedures can lead to customers becoming victims of skimming and other cybercrimes. Many Islamic bank customers in Indonesia remain unfamiliar with digital technology, making them vulnerable to digital fraud, such as skimming and phishing.

The skimming incident experienced by Bank Syariah Indonesia occurred in 2021 and 2022. Following its merger into Bank Syariah Indonesia (BSI), an increase in phishing incidents and potential skimming was reported as part of the digital threats they face. Although no significant cases have been widely reported, BSI acknowledges efforts to improve digital security, including its ATM infrastructure. According to the BSI 2022 Annual Report, one approach to risk reduction is the implementation of EMV chip-based security technology and a real-time fraud detection system to monitor and prevent illegal transactions, including skimming (BSI Annual Report, 2022).

Ideally, Islamic banks should integrate fraud prevention systems based on the maqasid sharia (protection of property and life), specifically safeguarding wealth (hifz al-mal) and life (hifz al-nafs), with conventional security measures such as identity verification and encryption. According to Antonio (2001), the principle of trustworthiness in the Islamic financial system demands complete protection of customer rights and data.

From a management perspective, Islamic banks must strengthen their digital security systems in line with Sharia principles, such as maslahah (benefit) and dharar (prevention of harm). One suggested approach is to educate customers on digital literacy principles rooted in Islam, conduct more frequent information technology audits, and collaborate with financial authorities to identify suspicious activities early.

It can be concluded that skimming is a significant problem for the Sharia banking system, based on the literature review. To ensure that sharia principles remain in banking services, a combination of strong technology and a thorough understanding of sharia is necessary in digital financial governance.

2. Sharia Economic Law Views on Skimming Actions

In the perspective of Islamic economic law, skimming is not merely a

violation of positive law but also a breach of the fundamental values of Islam. Islamic economic law is founded upon principles derived from the Qur'an, the Sunnah, and the ijtihad of scholars, with the primary objective of promoting public welfare (maslahah) and preventing harm or corruption (mafsadat) in the economic life of society.

Law Number 21 of 2008 concerning Islamic Banking uses sharia principles as the formal legal basis for implementing sharia-compliant banking activities (Kholid, 2018). The following explains the relationship between each principle of Islamic economic law and the practice of skimming:

a. Al-Maslahah Principle

The principle of al-maslahah aims to realize benefits and prevent damage in all economic activities (muamalah). One form of this is the protection of assets which are part of maqāṣid al-syarī‘ah. The act of skimming, which results in the illegal loss of property, is a form of damage that must be prevented and eradicated. Therefore, all business actors and banking institutions are required to design a robust security system as a means to safeguard the interests of the people and prevent digital banking crimes from occurring.

b. Principle of Monotheism

In Sharia economic law, the principle of monotheism views every economic activity as part of worshiping Allah SWT and as a moral responsibility to fellow humans. The act of skimming, which involves the theft and misuse of someone's account information for personal gain, constitutes a betrayal of trust and a violation of fundamental values and social responsibility. Therefore, skimming is not only a worldly crime, but also a form of denial of the value of monotheism in the Sharia economic system.

c. The Principle of Justice

Justice is a fundamental principle in the Islamic economic system, requiring every transaction to be proportional, transparent, and without harm to either party. Skimming creates significant inequality and injustice between the perpetrator and the victim, as the perpetrator takes unlawful

advantage of the injured party without their consent. This violates the spirit of justice as affirmed in Law No. 21 of 2008 concerning Islamic Banking, which stipulates that banking activities must be based on the principles of justice, equity, and benefit. Therefore, skimming is a direct violation of the value of justice in Islamic economics.

d. The Principle of Amar Ma'ruf Nahy Munkar

The principle of amar ma'ruf nahi munkar in the Islamic Banking Law requires that all business activities be conducted by Islamic law, while simultaneously rejecting all forms of practices that conflict with Sharia, such as usury, gharar, maisyir, and other haram activities. Skimming violates the principle of nahi munkar (forbidding evil) because it involves elements of theft (sariqah), fraud (tadlis), and theft (ghasb) of legitimate property. Skimming not only harms customers financially but also undermines the values of fairness and trust in the banking system.

Under Sharia law, skimming is a prohibited act because it unlawfully harms others. This act contains elements prohibited under Sharia Economic Law, namely:

a. Tadlis (Fraud)

Under Sharia law, skimming is considered a form of tadlis, or fraud. Shalih (2020) explains that the term tadlis is the plural form of the noun derived from dallasa, meaning "fraud or deception." Purba (2022:37) also defines tadlis as an act of deliberate fraud committed in an agreement or contract, by concealing material facts or providing misleading information to induce the other party to agree to the contract.

Skimming is carried out covertly using a hidden device to steal data from ATM or debit cards. Customers are unaware that their data has been copied or stolen, so when a transaction occurs, there is a hidden element of fraud. Therefore, according to Sharia law, skimming is a prohibited act because it contains elements of tadlis, which harm others and undermine trust in transactions.

1) Sariqah (Theft)

The act of skimming in Sharia law can also be categorized as a form

of sariqah or theft. According to Gunawan (2025:285), Sariqah is the act of taking other people's property secretly and by deception, without rights, from a safe storage place. Meanwhile, according to Wahbah Az-Zuhaili in Berutu (2020:46), sariqah is the act of taking other people's property from a storage place that is usually used to protect goods, carried out secretly.

If associated with skimming, the perpetrator secretly steals card data from ATMs or digital payment tools that are generally considered safe by users. This action was carried out without permission, unknown to the victim, and aimed to access and steal funds. Therefore, in the view of Sharia law, skimming falls under the category of sariqah because it fulfills the elements of theft, which is carried out in secret and is detrimental to the owner of the property.

2) Ghasab

Rashid et al. (2016:614) define ghasab as the act of using or taking advantage of another person's property without the owner's permission and knowledge, which is carried out unjustly. Meanwhile, according to Sa'diyah (2022:16), ghasab is the act of using another person's property without permission, even if the owner did not previously use the item. This act requires the perpetrator to replace any damage and to be aware of the owner's rights and expectations regarding the used item.

In the case of skimming, the perpetrator unjustly uses a customer's card data without permission to withdraw money from an account, even though the customer did not give consent and was unaware of the act. Therefore, according to Sharia law, skimming is also considered an act of ghasab because the perpetrator takes advantage of another person's property unlawfully and is liable for any losses incurred.

The legal perspective of Sharia economics on skimming is also supported by several previous studies, which show that this practice of digital banking data theft contradicts fundamental Islamic

values. Research by Sari (2019) shows that skimming is a form of system negligence that results in the loss of customer assets, requiring banks to provide protection and reimbursement. Furthermore, research by Sulha (2020) confirms that skimming can be categorized as sariqah (theft) because it is carried out secretly and uses deception to take someone else's property.

3. Forms of Responsibility of Islamic Banks for Customer Losses Due to Skimming from the Perspective of Islamic Economic Law

According to Islamic economic law, Islamic banks engage with their clients in a wadi'ah (deposit) or qardh (loan) contract, depending on the type of product and contract. If a bank fails to safeguard its clients' deposits, it is legally and morally responsible. One of the five main principles of the maqāṣid al-syarī‘ah (Islamic principles) is asset insurance (ḥifẓ al-māl). Loss of funds due to skimming constitutes a violation of the obligation to safeguard client assets (Al-Ghazali, al-Mustasfa in Kamali, 2008).

Islamic banks, as representatives or recipients of the client's trust, are responsible for maintaining the security and confidentiality of client funds. If negligence occurs due to the bank's internal security system, the bank will be liable. If the mudhari (the party entrusted with the wadi'ah) in a wadi'ah contract makes a mistake or fails to safeguard the deposited goods, they are responsible for compensating for any resulting losses (Karim, 2011).

In Islamic jurisprudence (fiqh muamalah), Imam al-Ghazali and As-Syutubi stated that the maqasid al-shari'a aim to preserve five aspects of human life, one of which is wealth (al-māl). If an organization is responsible for another person's wealth, it is liable for losses caused by its negligence. In this case, a bank must compensate customers if skimming occurs due to negligence in the bank's security system. However, suppose the bank has made its best efforts (ikhtiar) to protect its customers, and skimming occurs due to unforeseen external factors. In that case, it must provide compensation based on maslahah and istihsan (considerations of public interest and justice).

According to Indonesian regulations, Law No. 21 of 2008 concerning Islamic Banking (Article 27), Islamic banks are required to maintain the

confidentiality of their customers' information. Failure to protect data from loss can be considered a violation of the principle of prudence and can result in administrative sanctions or civil lawsuits. Meanwhile, skimming perpetrators are subject to criminal penalties under the Electronic Information and Transactions (ITE) Law No. 21 of 2008. 11 of 2008 in conjunction with Law No. 19 of 2016, Articles 30–32. If proven negligent, the bank remains responsible for compensation.

In practice in Indonesia, several skimming cases have occurred, one of which occurred at Bank Syariah Mandiri (BSM) in 2018. Several BSM customers were affected by skimming in March 2018. Customers did not make any transactions but reported that their balances mysteriously disappeared. An investigation revealed that ATM Bersama machines connected to the BSM network were used to steal customer data. According to detikfinance (2018), some of BSM's actions include conducting digital and electronic forensic investigations to ensure the validity of customer claims. Clients are asked to complete a complaint form and provide supporting documents. BSM provides full reimbursement for losses after it is proven that the customer was not negligent. An official statement from BSM states that BSM has returned funds to clients who were victims of skimming. Client funds remain safe, and BSM is committed to maintaining public trust (Detik Finance, 2018).

Islamic banks can provide reimbursement to customers who have fallen victim to skimming, subject to certain conditions stipulated by the bank's internal regulations, OJK laws, and Islamic economic principles. The purpose of these conditions is to ensure that customers are not negligent and that the transactions are truly the result of electronic fraud. Customers should contact the bank immediately if they detect suspicious transactions or a lost balance. Banks typically set a reporting time of no more than 2 to 5 business days from the date of the incident. Reports can be made through the call center, customer service, or the nearest branch (Bank Indonesia, 2015).

Islamic banks in Indonesia provide reimbursement to customers who have fallen victim to skimming. This demonstrates the bank's commitment to consumer protection and the implementation of Islamic principles in practice. Islamic banks in Indonesia generally provide reimbursement to customers if it is proven that their

funds were lost due to the actions of a third party (skimming) rather than the customer's fault. This aligns with the principle of istihsan, which is a legal determination based on the benefit of the customer, aimed at protecting customer rights in Islamic finance. Banks that refuse to return losses without a valid reason violate the principles of justice and trust in the context of Sharia. They also do not fulfill the maqashid of sharia in safeguarding assets (ḥifẓ al-māl).

D. CONCLUSION

The act of skimming is a form of digital crime that is very detrimental, both to customers and Sharia banking institutions. Skimming is carried out covertly by stealing data from ATM or debit cards via illegal electronic means. This action results in financial losses, erodes customer confidence, and compromises the bank's reputation. In the context of positive law, skimming violates the provisions of the ITE Law and the Sharia Banking Law, which regulate data protection and electronic payment systems. From the perspective of Sharia economic law, skimming is an act that is contrary to Islamic values. This action contains elements of tadlis (fraud), sariqah (theft), and ghasab (taking without permission), all of which are prohibited in muamalah fiqh. Skimming also violates the fundamental principles of Sharia economics, including justice, trust, honesty, and asset protection. Therefore, skimming is not only prohibited by state law, but is also contrary to maqāṣid al-syarī'ah in maintaining the benefit of society. As the party entrusted with customer trust, Islamic banks have a moral and legal responsibility to maintain the security of customer funds and data. If system failures lead to skimming, the bank is obligated to provide compensation as a form of consumer protection. Preventive measures must also be strengthened, both through technology and customer education. An approach based on Sharia principles, such as maslahah (benefit) and justice, needs to be implemented to ensure Islamic finance remains trusted and relevant in the digital age.

REFERENCES

Addi Sulha, M. R. (2020). *Tinjauan Hukum Islam terhadap Kejahatan Carding di Internet*.

Antonio, M. S. (2001). *Bank Syariah: Dari Teori ke Praktik*. Gema Insani.

Az-Zuhaili, W. (2020). *Fikih Jinayat: Hukum Pidana Islam Dilengkapi Fatwa-Fatwa Kontemporer*.

Bank Indonesia. (2015). *Peraturan BI No. 16/1/PBI/2015 tentang Perlindungan Konsumen Jasa Sistem Pembayaran.*

Berutu, D. (2020). *Pengantar Fiqih Muamalah*.

Creswell, J. W. (2014). Research Design: Qualitative, Quantitative, and Mixed Methods Approaches (4th ed.). *Thousand Oaks, CA: SAGE Publications.*

Gunawan, H. (2023). *Fiqh Jinayah yang Responsif terhadap Isu-Isu Kekinian*.

Hamzah, A. (2005). *Cyber Crime: Kejahatan di Dunia Maya*. Sinar Grafika.

Kamali, M. H. (2008). *Shariah Law: An Introduction*. Oneworld Publications.

Karim, A. A. (2011). *Ekonomi Mikro Islami*. Raja Grafindo Persada.

Kholid, M. (2018). Prinsip-Prinsip Hukum Ekonomi Syariah dalam Undang-Undang tentang Perbankan Syariah. *Asy-Syari'ah: Jurnal Ilmu Syari'ah Dan Hukum*, *20*(2), 139–156.

Mardani. (2012). *Hukum Ekonomi Syariah di Indonesia*. Kencana.

Nasabah BSM Kehilangan Saldo, Ini Kata Bank Syariah Mandiri. (2018). *Detik Finance*.

OJK. (2021). *Edukasi Perlindungan Konsumen Perbankan*. www.ojk.go.id .

Otoritas Jasa Keuangan. (2020). *Panduan Pengendalian Risiko Teknologi Informasi pada Perbankan: Risiko Skimming.* OJK.

Otoritas Jasa Keuangan. (2023). *Laporan Perkembangan Keuangan Syariah Indonesia Tahun 2023*. OJK.

Purba, R. D. (2022). *Hukum Perikatan dan Perjanjian*.

Rasyid, H., & El-Sutha, S. H. (2017). *Panduan Muslim Sehari-hari*.

Rohman, F. (2020). Kejahatan Skimming dalam Perspektif Hukum Pidana dan Perlindungan Konsumen. *Jurnal Hukum Dan Ekonomi Syariah*, *8*(2), 105–112.

Romli, L. (2015). *Cyber Crime: Kejahatan Mayantara*. Refika Aditama.

Sa'diyah, N. (2022). *Ringkasan Fikih Lengkap II*.

Sari, N. (2019). Pertanggungjawaban BNI Syariah terhadap Nasabah Akibat Tindak Kejahatan Skimming Kartu ATM. *Reformasi Hukum*, *23*(2), 160–170.

Sari, N. (2020). Perlindungan Hukum Bagi Konsumen Nasabah Dalam Card Skimming (Studi Kasus Bank Bni Syariah Pusat Di Jakarta). *Reformasi Hukum*, *23*(2), 149–168.

Shalih, M. (2020). *Panduan Muslim Sehari-hari*.

Wahyudi, A., & Haryono, T. (2021). Evaluasi Sistem Keamanan ATM pada Bank Syariah: Kajian terhadap Risiko Skimming. *Jurnal Sistem Informasi Dan Keamanan*, *9*(1), 22–30.