PRIVIETLAB

Menara Prima Lantai 29 Jl. DR. Ide Anak Agung Gde Agung, RT.5/RW.2, Kuningan, Kuningan Tim., Kecamatan Setiabudi, Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12950
Telp: +628131000351
http://privietlab.org/

priviet lab.
RESEARCH & PUBLISHING

Jakarta, 18 August 2026

ACADEMIC ACCEPTANCE LETTER

PRIVIET SOCIAL SCIENCES JOURNAL (PSSJ)

Volume 6, Issue 8, 2026

Title: A Review of Islamic Criminal Law on Criminal Acts in the Banking Sector (Analysis of Sanctions for the Criminal Act of Carding)

To: Muhammad Harris Danial, Irwansyah, Riadhus Sholihin

Ar-Raniry State Islamic University

We are pleased to inform you that your manuscript entitled "A Review of Islamic Criminal Law on Criminal Acts in the Banking Sector (Analysis of Sanctions for the Criminal Act of Carding)" has been accepted for publication in the Priviet Social Sciences Journal (PSSJ).

This acceptance is granted based on the journal's editorial and review process. However, publication will proceed only after the authors have completed all required final editorial revisions.

The manuscript is scheduled for publication in Volume 6, Issue 8, August 2026. Please note that failure to complete the required revisions or editorial requirements within the specified timeline may result in the postponement or rescheduling of publication.

With kind regards,

Jakarta, 18 August 2026
Founder PRIVIETLAB

Dr Mochammad Fahlevi, S.Pd.I., M.M., M.A., M.Ud., AWP

Priviet Social Sciences Journal
E-ISSN 2798-6314
P-ISSN 2798-866X
https://doi.org/10.55942/pssj.v6i3.1323

Volume X
Issue X
December Edition XXXX

A Review of Islamic Criminal Law on Criminal Acts in the Banking Sector (Analysis of Sanctions for the Criminal Act of Carding)

Muhammad Harris Danial[1] Irwansyah[2] Riadhus Sholihin[3]
[1 2 3] Ar-Raniry State Islamic University, Banda Aceh
[1]*e-mail: 220104005@student.ar-raniry.ac.id*
[2]*e-mail: irwansyah@ar-raniry.ac.id*
[3]*e-mail: riadhus.sholihin@ar-raniry.ac.id*

ABSTRACT

This study examines the crime of carding from the perspective of Islamic criminal law in response to the rise of cybercrime in modern digital transactions. The problem addressed is how Islamic law classifies carding within the structure of fiqh jināyah and how the regulation of this act can be constructed through Islamic legal principles. The research questions focus on: (1) how carding is viewed in Islamic criminal law, and (2) how the jarīmah of carding is regulated according to Islamic legal studies. This research employs a normative juridical method with a conceptual approach, using primary sources such as the Qur'an, Hadith, and classical and contemporary fiqh literature, as well as secondary sources including academic journals and legal regulations. The findings reveal that although carding resembles tadlis (fraud) in substance, it does not fulfill the classical requirements of hudūd due to the absence of physical taking from a protected place (hifz). Therefore, the most appropriate classification is jarīmah ta ʿ zīr, where punishment is determined based on judicial discretion, maslahah (public interest), and the protection of property (hifz al-māl) within maqāsid al-syarīʿah. The study concludes that Islamic criminal law possesses normative flexibility to address modern cybercrimes through the ta ʿ zīr mechanism without departing from its foundational principles.

Keywords: carding, Islamic criminal law, ta'zīr, fiqh jināyah, cybercrime.

1. INTRODUCTION

Advances in information technology have changed the way people live and increased efficiency in the business world, but they have also created threats in the form of cybercrime that disrupts security. Internet-based technology has significant social impacts, supporting public welfare while also presenting challenges to human rights. As a tool for law enforcement, this technology requires adjustments within the legal framework so that it can continue to be applied effectively (Hartono, 2016). Information technology has now become an important element, both in the present and in the future. The term "Online" refers to a condition in which a device or system is connected to and able to interact with the internet or other networks. When a person or device is "online," it means that they are actively using the internet or a computer network to communicate, exchange data, or access various digital resources. The internet, as an integral part of the information technology revolution, functions as a channel of communication and information that accelerates the dissemination of knowledge and supports various human activities (Alcianno, 2014).

The rapid advancement of internet technology has given rise to a phenomenon known as "Cybercrime," or cybercrime, involving illegal acts carried out through internet networks. Examples of

cybercrime cases occurring in Indonesia include credit card hacking, website hacking, theft of personal data such as email, and data manipulation using weak passwords (Eliasta, 2016). Credit cards, as payment instruments that enable transactions without the use of cash, are issued by financial institutions such as banks. Credit cards have now become an important element of modern life, replacing cash for purchasing goods and services from merchants that accept such cards, in line with advances in e-commerce technology (Chandra, 2019). Careful attention is required to protect the banking industry from white-collar crimes, such as banking crimes and criminal acts in the banking sector. One cybercrime that frequently occurs today is credit card fraud (carding), in which perpetrators (carders) use credit card data to conduct payment transactions. Carding can be carried out through both offline and online transactions. Although it is a common problem in Indonesia, the country's legal system still has shortcomings and ineffective oversight in handling such cases (Hartono, 2016).

According to recent research conducted by the Texas-based security company Clearcommerce, Indonesia ranks first among countries of origin of cyber fraud perpetrators. It was also reported that approximately 20 percent of total credit card transactions from Indonesia conducted through the internet constitute cyber fraud. Meanwhile, data from the Indonesian National Police indicate that an average of 200 cybercrime cases handled are generally dominated by credit card fraud targeting foreign countries such as the United States, Australia, and Canada, with perpetrators originating from major cities such as Yogyakarta, Bandung, Jakarta, and Riau (Ginara et al., 2022). Efforts to enforce the law against violations or crimes committed by insiders within banks, particularly those involving the theft of public funds, require adequate regulation. One legal instrument that can be used to address negligence, misconduct, and crimes committed by bank insiders is criminal law. The government has issued various regulations to address these problems, such as Article 35 of Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE), which states, "Any Person intentionally and without right or unlawfully manipulates, creates, alters, deletes, or damages Electronic Information and/or Electronic Documents with the purpose of making such Electronic Information and/or Electronic Documents appear as if they were authentic data" (Law No. 11 of 2008).

The fundamental difference between carding and sariqah lies in the method and target used to obtain property or information. Carding is an illegal activity involving the use of credit or debit card data without the owner's permission, usually to conduct fraudulent online transactions or exploit stolen card information. Meanwhile, sariqah in Islamic law refers to direct theft, which involves the physical taking of property that can be perceived by the senses. In Islamic criminal law, theft is regarded as a serious violation because it infringes upon individual ownership rights. Sanctions against perpetrators of theft may vary depending on several factors, such as the value of the stolen item, the method of theft, and the perpetrator's social status. Previous research relevant to this study includes research by Rausyan Fikri, which examines the criminal act of online credit card hacking based on Law Number 19 of 2016 concerning Electronic Information and Transactions (UU ITE). The study focuses on how the UU ITE regulates credit card hacking, the effectiveness of law enforcement against perpetrators, and forms of legal protection for victims, emphasizing the importance of technological support and international cooperation in combating cybercrime (Fikri, 2025).

2. LITERATURE REVIEW

Jaenudin and Nisa, through their study entitled Islamic Criminal Law Analysis of Cyber Crimes on Consumers in E-Commerce Transactions, examine cybercrime that harms consumers in e-commerce transactions from the perspective of Islamic criminal law. The study explains that various forms of cybercrime, such as online fraud, data theft, and misuse of electronic information, constitute acts contrary to the principle of property protection (hifz al-māl) in maqāsid al-syarīʿah. Because these forms of crime are not explicitly regulated in the nash, they are categorized as jarimah taʿzīr, meaning that the form and severity of the sanctions are left to the government or judge, taking into consideration the public interest and the extent of the losses caused (Jaenudin and Nisa, 2021).

The journal article discussed by Meerangani et al., entitled Cybercrime and Its Violation of Digital Platform Security: An Islamic Law Perspective, examines cybercrime as a violation of digital platform

security from the perspective of Islamic law. This research emphasizes the concept of digital ownership, rights of control over electronic data, and the importance of maintaining information security as part of property protection in Islam. The authors argue that acts such as hacking, phishing, skimming, and data theft constitute violations of property rights that may be punished according to the principles of fiqh jinayah, even though the objects of the crimes have no physical form. Therefore, Islamic law is considered capable of accommodating developments in digital crime through the application of the concept of jarimah ta'zīr (Meerangani et al., 2022).

A study published by Apipuddin et al., entitled Integrating Electronic Information and Transaction Law (UU ITE) and Islamic Criminal Law: Addressing Malware-Based Data Theft, discusses data theft using malware by integrating the provisions of the UU ITE and Islamic criminal law. The study explains that malware is used as a means of illegally obtaining electronic information, thereby causing losses to individuals and institutions. From the perspective of Islamic law, data theft through malware is viewed as a violation of trust and property rights that does not fulfill the classical elements of theft (sariqah), and is therefore more appropriately classified as jarimah ta'zīr. The study also emphasizes the importance of harmonizing national law with Islamic principles in combating cybercrime (Apipuddin et al., 2024).

Ahmad Nurun and Qibtiyah, in their study entitled Konstruksi Hukum Pidana terhadap Kejahatan Sibernetik dalam Bingkai Maqasid al-Syari'ah, examine the construction of Islamic criminal law concerning various forms of cybercrime through the maqāsid al-syarī'ah approach. The study explains that cybercrime is a modern form of crime that threatens the protection of property (hifz al-māl), honor (hifz al-'ird), and public security, thereby giving the state authority to establish jarimah ta'zīr sanctions against perpetrators. In addition, the study develops a punishment framework oriented toward prevention, public protection, and rehabilitation of perpetrators so that the objectives of the sharia can be achieved comprehensively (Ahmad and Qibtiyah, 2025).

3. DATA AND METHODS

The type of research used in this study is normative juridical research. This legal research is prescriptive in nature. The approach used in this study is the conceptual approach. The data sources in this study include primary sources consisting of the Qur'an, classical and contemporary fiqh books, as well as applicable laws and regulations, and secondary sources consisting of books, scientific journals, academic articles, theses, undergraduate theses, and dissertations relevant to the topic of carding in Islamic law.

4. RESULTS AND DISCUSSION

3.1. The Concept of Carding as a Criminal Act in Banking

The criminal act of carding is one form of crime within the realm of cybercrime that has developed rapidly alongside advances in information technology, particularly in the banking sector and electronic transaction systems. In general, carding is defined as the act of obtaining, possessing, and using another person's credit or debit card data unlawfully to conduct financial transactions for personal benefit. In legal studies, carding is often equated with credit card fraud, namely a form of fraud committed by using a credit card facility without the permission of its lawful owner. Carding practices are carried out through various methods, such as data theft, system hacking, online fraud (phishing), and data duplication using certain devices (skimming) (Tambunan et al., 2023). From the perspective of criminal law, carding is an unlawful act that contains not only elements of fraud, but also theft and illegal access to electronic systems. Therefore, carding is no longer viewed as a conventional crime, but as a modern technology-based crime requiring special treatment. In addition, carding has a transnational crime character because perpetrators, victims, and the media used may be located in different jurisdictions. This creates challenges for law enforcement, particularly in terms of evidence and inter-state coordination (Kamilah, 2022).

In practice, criminal acts in the banking sector are not limited to carding, but encompass various forms of crime related to financial systems and information technology. One of the most common forms is credit card fraud or carding itself, which is carried out by using credit card data illegally without the owner's consent. There is also skimming, namely the act of duplicating card data through a particular

device installed on an ATM or EDC machine, allowing the data to be used by perpetrators to conduct illegal transactions. Another frequently occurring crime is phishing, namely an attempt at fraud by creating fake websites or electronic messages that resemble official institutions such as banks, with the aim of obtaining sensitive information from customers, such as card numbers, PINs, and passwords. In addition, banking system hacking is carried out by breaching a bank's security system to obtain access to customer data or transaction systems. Equally important, identity theft is also a form of crime in the banking sector, in which perpetrators use another person's identity without permission to conduct financial activities. In further developments, the use of malware and spyware has also become a serious threat because such software can secretly steal user data without the user's awareness (Qammaddin et al., 2023).

The development of the criminal act of carding cannot be separated from advances in information technology and the increasing use of digital transaction systems in people's lives. Initially, carding was carried out in simple ways, such as physically stealing credit cards and using them directly. However, with the development of the internet and digital technology, carding modus operandi have become increasingly sophisticated and difficult to detect. Today, carding has developed into various forms, such as using credit card data for online transactions on e-commerce platforms without the physical presence of the card. In addition, illegally obtained credit card data are also traded through illegal forums on the internet, commonly known as the dark web, thereby expanding the network of this crime globally. Another development is the use of automated systems to conduct large numbers of illegal transactions within a short period, known as automated fraud. In addition, perpetrators use social engineering techniques, namely psychological manipulation of victims to obtain sensitive information by impersonating trusted parties. These developments are influenced by various factors, such as technological advances, weak digital security systems, low public awareness of data security, and economic incentives to obtain profits quickly (Sarles Gultom et al., 2023).

The chronology of criminal cases related to carding, as presented on the Scammer Payback YouTube channel, generally begins with the perpetrator approaching the victim. Perpetrators usually contact victims by telephone, e-mail, or pop-up displays on computer devices while impersonating official parties, such as banks, technical services, or government agencies. At this stage, perpetrators use psychological manipulation techniques (social engineering) to build the victim's trust so that the victim is willing to follow the instructions given. After the victim has been influenced, the perpetrator then directs the victim to provide sensitive information, such as credit card numbers, OTP codes, and other personal data. In some cases, perpetrators also ask victims to download certain applications that allow remote access to the victim's device. This stage is the core of carding crime because perpetrators obtain financial data that will later be used to conduct illegal transactions (Scammer Payback, 2023). Subsequently, after obtaining the data, perpetrators exploit it by using credit card data to conduct unauthorized online transactions or by selling the data on illegal internet forums. In practice, perpetrators often use third parties known as money mules to withdraw the proceeds of crime, thereby complicating efforts by law enforcement authorities to trace the funds (Federal Bureau of Investigation, 2023).

In Scammer Payback content, the fraud perpetrators are then confronted by a scambaiter who impersonates a victim in order to uncover the modus operandi used. In some cases, the perpetrators' networks are traced to the centers of scam operations, and data are collected and subsequently reported to the authorities. These actions aim to stop criminal activities and educate the public about the dangers of digital fraud (Pierogi, 2022). The final stage of the case chronology is disclosure and prevention, in which the information obtained is used to warn the public to be more vigilant against various fraud schemes, including carding. Thus, the case chronology presented shows a systematic pattern of crime, beginning with victim manipulation, data theft, and the use of data for illegal financial gain (Wikipedia contributors, 2023).

3.2. Carding as a Criminal Act in Legislation from the Perspective of Islamic Criminal Law

An act can be categorized as a criminal offense if it fulfills certain elements. The same applies to the criminal act of carding, which must fulfill several elements in order to be legally prosecuted. The first element is the existence of an unlawful act, namely the perpetrator's act of accessing or using credit card

data without valid authorization. This act clearly contradicts applicable legal provisions, both under general criminal law and specific laws concerning information technology. The second element is fault or mens rea, namely the perpetrator's intention or deliberate purpose to commit a crime and obtain an unlawful benefit. This element is important for distinguishing intentional acts from those occurring due to negligence. The third element is the existence of an actual act or actus reus, namely the use of another person's credit card data to conduct illegal transactions. In addition, the element of loss is also important in carding crimes because such acts cause financial losses to both customers and banking institutions. The final element is the use of information technology as the primary means of committing the crime. This is a distinctive characteristic of carding as part of cybercrime. In the context of Indonesian law, these elements are closely related to the provisions of the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE), which regulate illegal access, data manipulation, and electronic-based fraud (Diansah et al., 2021).

The criminal act of carding, as part of cybercrime, is essentially not explicitly regulated in a single specific provision under Indonesian positive law. However, the substance of the act can be addressed through various applicable laws and regulations, particularly the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). These two legal instruments serve as the main basis for prosecuting carding perpetrators, although the approaches used differ, namely a conventional approach and an information-technology-based approach. From the perspective of the KUHP, carding may be classified as fraud as regulated in Article 378 of the KUHP, which provides that anyone who, with the intention of unlawfully benefiting himself or another person, by using a false name or false status, deception, or a series of lies, induces another person to surrender an object, is threatened with imprisonment for a maximum of four years for fraud. In the context of carding, the use of another person's credit card data without permission may be categorized as deception to obtain an unlawful benefit. In addition, carding may also be associated with the theft provision under Article 362 of the KUHP, which states that anyone who takes an object, wholly or partly belonging to another person, with the intention of unlawfully possessing it, is threatened with imprisonment for a maximum of five years or a fine of up to Rp900,000, particularly when viewed from the aspect of taking data or information that has economic value (Soesilo, 2013).

However, the use of the KUHP in dealing with carding crimes has limitations because the KUHP was essentially drafted before the development of modern information technology. Consequently, many aspects of carding cannot be optimally addressed by the KUHP, particularly those relating to illegal access to electronic systems and manipulation of digital data. This has encouraged the enactment of specific regulations governing technology-based crimes, namely the Electronic Information and Transactions Law (UU ITE). Under the UU ITE, carding crimes may be prosecuted through several provisions that specifically regulate acts involving illegal access and misuse of electronic data. One relevant provision is Article 30 of the UU ITE, which states: "Any Person intentionally and without right or unlawfully accesses a Computer and/or Electronic System belonging to another Person by any means." A person who violates Article 30 paragraph (1) of the UU ITE may be sentenced to imprisonment for a maximum of 6 years and/or a fine of up to Rp600 million. In carding practices, perpetrators often illegally access banking systems or databases to obtain credit card data, so such conduct fulfills the elements of this article (Law Number 19 of 2016).

In addition, Article 32 of the UU ITE (Law No. 11 of 2008) prohibits illegally altering, adding to, reducing, or transferring electronic information/documents belonging to another person. Violators face a maximum imprisonment of 8–10 years and/or a fine of Rp2–5 billion. In the context of carding, stealing and using credit card data may be categorized as a form of illegal transfer or control of electronic information. Furthermore, Article 35 of the UU ITE (Law No. 11 of 2008) prohibits the unauthorized manipulation, creation, alteration, deletion, or destruction of electronic information/documents so that they appear to be authentic. Violation of this article is intended to prevent fraud and is punishable by imprisonment for a maximum of 12 years and/or a fine of up to Rp12 billion, which is also relevant to carding practices, particularly in cases involving the use of falsified or manipulated data (Diansah et al., 2021). The techniques used in carding crimes are fundamentally closely related to the elements of criminal

offenses regulated in the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). Each technique used by perpetrators is not merely a modus operandi, but also reflects the fulfillment of the elements of unlawfulness, intent (mens rea), an actual act (actus reus), and the resulting loss. Phishing and social engineering techniques, for example, demonstrate the element of fraud as regulated in Article 378 of the KUHP. In these techniques, perpetrators intentionally use deception and a series of lies while impersonating trusted parties to deceive victims into providing sensitive data such as credit card numbers and security codes. Such conduct fulfills the element of intent to unlawfully benefit oneself, while also fulfilling the element of active conduct in the form of psychological manipulation of the victim (Tambunan et al., 2023).

Furthermore, skimming, shoulder surfing, and dumpster diving techniques can be associated with the elements of theft as regulated in Article 362 of the KUHP because perpetrators take data or information with economic value without authorization. Although the object taken is not a physically tangible object, developments in modern law have recognized that electronic data also have value as legal objects. Therefore, taking credit card data without permission may be categorized as unlawful control over another person's property (Kamilah, 2022). Meanwhile, hacking, malware, spyware, and data breach techniques are closely related to the provisions of the UU ITE, particularly Article 30, which regulates illegal access to electronic systems. Perpetrators intentionally and without authorization access another party's computer or electronic system to obtain credit card data. In addition, the use of malware to steal data also fulfills the elements of Article 32 of the UU ITE, which prohibits the transfer or control of another person's electronic information without authorization (Qammaddin et al., 2023).

In addition, the use of automated fraud techniques and the involvement of other parties such as money mules demonstrate the element of participation (deelneming) in criminal law. In the context of the UU ITE, manipulating data or using falsified data to conduct transactions may be prosecuted under Article 35, which regulates the manipulation of electronic information so that it appears to be legitimate. Thus, carding crimes are often committed in an organized manner and involve more than one perpetrator (Hendri Diansah et al., 2021).

3.3. Carding as a Criminal Act from the Perspective of Islamic Criminal Law

The development of information technology has given rise to various forms of crime that were unknown in the classical period, one of which is the criminal act of carding. Carding is the act of obtaining, possessing, or using another person's credit or debit card data without authorization to conduct electronic transactions that benefit the perpetrator and harm the card owner. From the perspective of Islamic criminal law, there is debate over whether carding is more appropriately categorized as sariqah (theft) or tadlīs (fraud). In the author's view, carding is closer to the concept of tadlīs because the primary means used by perpetrators is not the secret taking of property, but rather deception, information manipulation, identity impersonation, and misuse of electronic systems (Zaidan, 2006). In fiqh muamalah literature, tadlīs is defined as concealing a defect, providing false information, or employing deception so that another party suffers a loss in a transaction (Az-Zuhaili, 2008).

The essential elements of tadlīs are lying (al-kadhib), misleading (taghrir), and abuse of trust resulting in the unlawful transfer of property. These elements are highly relevant to carding practices because perpetrators obtain payment card data through phishing, social engineering, skimming, malware, or hacking techniques and then use the victim's identity as if they were the lawful cardholder to conduct electronic transactions (Kamilah, 2022). Unlike sariqah, carding does not fulfill all the elements of theft under Islamic law. The majority of fuqaha stipulate that the object of sariqah must be tangible property (mal), have economic value, be kept in a secure place (hirz), and be taken secretly by the perpetrator (Audah, 1992). In carding practices, what is initially taken is not tangible property, but electronic data such as card numbers, PINs, CVVs, or cardholder identities. Such data are then used as a means of obtaining financial gain through electronic transactions. Therefore, the element of physical taking required for sariqah is not fully fulfilled. Conversely, the characteristics of carding more closely reflect the practice of tadlīs because perpetrators impersonate identities (identity deception) and mislead electronic payment systems into believing that the transaction was conducted by the lawful cardholder. In Islamic fiqh, the Prophet

Muhammad (peace be upon him) explicitly prohibited all forms of fraud in muamalah, as he said: "Whoever deceives is not one of us." (Reported by Muslim) (Muslim, n.d., Hadith No. 102).

This hadith demonstrates that Islam pays serious attention to all forms of fraud, whether committed directly or through electronic media. Although the form of deception during the Prophet's time differed from modern cybercrime, the legal substance remains the same, namely an act of deceiving another party in order to obtain an unlawful benefit. In addition, the Qur'an also prohibits acquiring property through false means, as stated by Allah SWT: "And do not consume one another's wealth unjustly..." (QS. Al-Baqarah [2]: 188). This verse has a general meaning encompassing all forms of unlawful control over property, including through information technology manipulation. Thus, carding, as a form of misuse of electronic data to obtain financial gain, can be categorized as consuming another person's property through false means.

In contemporary fiqh jinayah, many scholars argue that cybercrime, including carding, does not fulfill the requirements for the application of hudud punishment, but is more appropriately classified as jarimah ta'zir. This is because the modus operandi and objects of the crime were unknown in the classical period and therefore were not explicitly regulated in the nash. Consequently, the form and type of punishment are left to the ulil amri, taking into consideration the level of danger, the losses caused, and the public interest (Audah, 1992).

This approach provides flexibility for the state to impose sanctions on carding perpetrators through national criminal provisions without contradicting the principles of Islamic law. Based on the foregoing discussion, it can be understood that carding is closer to the concept of tadlīs than sariqah. This is because the essence of carding lies in fraud, identity manipulation, abuse of trust, and the unlawful acquisition of property through false means. Although the perpetrator ultimately obtains financial gain, that gain is obtained through the mechanism of misleading an electronic system, rather than through the secret taking of tangible property as characteristic of sariqah. Therefore, from the perspective of Islamic criminal law, carding is more appropriately viewed as a form of modern fraud (tadlīs) that falls within the category of jarimah ta'zir.

Based on the entire discussion presented above, the author argues that the criminal act of carding is more appropriately classified as a form of tadlīs (fraud) than sariqah (theft) from the perspective of Islamic criminal law. This is based on the characteristics of carding, which emphasize deception, identity manipulation, abuse of trust, and electronic system engineering to obtain unlawful benefits. Unlike sariqah, which requires the secret taking of tangible property from a qualified place of safekeeping (hirz), carding is carried out through the use of electronic data as the primary object of the crime. Thus, the substance of carding does not lie in the physical taking of property, but rather in acts of deception that cause another person's property to be transferred to the perpetrator through an unauthorized electronic transaction mechanism. Therefore, in the author's view, the approach that classifies carding as tadlīs is more consistent with the principles of contemporary fiqh muamalah and fiqh jinayah than directly analogizing it to sariqah.

Based on this construction, the author also argues that carding perpetrators are more appropriately subjected to ta'zir punishment. This is because carding is a modern form of crime that is not explicitly regulated in the Qur'an or hadith and does not fulfill the elements required for the application of hudud punishment for the jarimah of sariqah. As a jarimah ta'zir, the determination of the type and severity of punishment is left to the ulil amri or judge, taking into consideration the level of loss, social impact, sophistication of the modus operandi, and the interests of protecting society and the financial system. Thus, the novelty of this study lies in the conceptual reconstruction that positions carding as a form of tadlīs in Islamic criminal law, so that the basis of criminal liability is no longer oriented toward the concept of conventional theft, but rather toward the concept of fraud manifested through the misuse of information technology and electronic transactions. This novelty is expected to enrich contemporary fiqh jinayah studies while serving as a conceptual foundation for formulating law enforcement against cybercrime in accordance with technological developments and the principles of Islamic law.

REFERENCES

Al-Kasānī, A. B. (t.t.). *Badā'iʿ al-sanā'iʿ fī tartīb al-sharā'iʿ*. Dār al-Kutub al-'Ilmiyyah. Al-Nawawī, Y. I. S. (t.t.). *Al-majmūʿ syarhal-muhadzdzab*. Dār al-Fikr.

Federal Bureau of Investigation. (2023). *Internet crime report*.

Ibn Qudāmah, A. I. A. (t.t.). *Al-mughnī*. Maktabah al-Qāhirah.

Hartono, B. (2013). Penerapan sanksi pidana terhadap tindak pidana carding. *Pranata Hukum, 8*(2), 168–177. https://doi.org/10.36448/pranatahukum.v8i2.141

Gani, A. G. (2014). Pengenalan teknologi internet serta dampaknya. Jurnal Sistem Informasi Universitas Suryadarma, 2(2), 71–86. https://doi.org/10.35968/jsi.v2i2.49

Ketaren, E. (2016). Cybercrime, cyber space, dan cyber law. Jurnal TIMES, 5(2), 35–42. https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/issue/view/12

Chandra, Y. U., Karya, S., & Hendrawaty, M. (2019). Decision support systems for customer to buy products with an integration of reviews and comments from marketplace e-commerce sites in Indonesia: A proposed model. International Journal on Advanced Science, Engineering and Information Technology, 9(4), 1171–1176. https://doi.org/10.18517/ijaseit.9.4.6505

Ginara, I. G. K., Widyantara, I. M. M., & Styawati, N. K. A. (2022). Kriminalisasi terhadap kejahatan carding sebagai bentuk cyber crime dalam hukum pidana Indonesia. Jurnal Preferensi Hukum, 3(1), 138–142. https://doi.org/10.22225/jph.3.1.4673.138-142

Kamali, M. H. (2019). *Crime and punishment in Islamic law: A fresh interpretation*. Oxford University Press. https://doi.org/10.1093/oso/9780190910648.001.0001

Pierogi. (2022). *Scammer Payback: Fighting back against online scammers*.

Soesilo, R. (2013). *Kitab Undang-Undang Hukum Pidana (KUHP) serta komentar-komentarnya lengkap pasal demi pasal*. Politeia. https://doi.org/10.24952/el-qanuniy.v6i1.2473

Apipuddin, A., Nasri, U., Mulyohadi, R. A., & Muslim, A. (2024). Integrating electronic information and transaction law (UU ITE) and Islamic criminal law: Addressing malware-based data theft. Al-Ahkam: Jurnal Ilmu Syari'ah dan Hukum, 9(2). https://doi.org/10.22515/alahkam.v9i2.10269

Diansah, H., dkk. (2021). Kebijakan hukum pidana terhadap tindak pidana carding. PAMPAS: Journal of Criminal Law, 3(1). https://doi.org/10.22437/pampas.v3i1.17704?utm_source=chatgpt.com

Fikri, R. (2025). Tindak pidana peretasan kartu kredit secara online berdasarkan Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Skripsi). https://repository.ar-raniry.ac.id/id/eprint/41517

Gunawan, H. (2022). Cybercrime dalam perspektif fiqh jināyah. Jurnal Hukum Islam. https://doi.org/10.24952/el-qanuniy.v6i1.2473

Gultom, S., dkk. (2023). Juridical analysis of cybercrime carding. Journal of Multidisciplinary. https://doi.org/10.70489/e47ma847

Jaenudin, J., & Nisa, R. R. (2021). Islamic criminal law analysis of cyber crimes on consumers in e-commerce transactions. Eduvest: Journal of Universal Studies, 1(4). https://doi.org/10.59188/eduvest.v1i4.33

Kamilah, A. (2022). Carding sebagai cyber crime dalam perspektif hukum perdata internasional. Jurnal Mimbar Justitia, 10(2). https://doi.org/10.35194/jhmj.v10i2.4841

Meerangani, K. A., dkk. (2022). Cybercrime and its violation of digital platform security: An Islamic law perspective. International Journal of Academic Research in Progressive Education and Development, 11(3). https://doi.org/10.6007/IJARPED/v11-i3/14564

Nurun, A., & Qibtiyah, M. (2025). Konstruksi hukum pidana terhadap kejahatan sibernetik (cybercrime) dalam bingkai maqasid al-syarī'ah. The Jure: Journal of Islamic Law, 2(2). https://journal.iaisyaichona.ac.id/index.php/the_jure/article/download/262/203

Qammaddin, dkk. (2023). Implementasi teknik forensik dalam cybercrime (carding). Jurnal REMIK, 7(1). https://doi.org/10.33395/remik.v7i1.12059

Sulha. (2021). Tinjauan hukum pidana Islam terhadap kejahatan carding. Jurnal Syariah dan Hukum. https://eprints.walisongo.ac.id/id/eprint/12853

Tambunan, U. J., dkk. (2023). Penegakan hukum tindak pidana carding berdasarkan UU ITE. Jurnal Gagasan Hukum, 6(2). https://doi.org/10.31849/jgh.v6i02.21830

‘Audah, A. Q. (1968). Al-Tasyri’ al-jinā’ī al-islāmī. Dār al-Kutub al-‘Ilmiyyah.
Wahbah az-Zuhaili. (1985). Al-Fiqh al-Islami wa Adillatuhu. Damaskus: Dar al-Fikr.
Majma’ al-Fiqh al-Islami. (1988). Qarar tentang Huquq al-Ibtikar wa al-Ta’lif. Jeddah: OKI.
Republik Indonesia. (2008). Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Republik Indonesia. (2016). Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
Scammer Payback. (n.d.). Channel YouTube Scammer Payback. Diakses dari https://www.youtube.com/results?search_query=scammer+payback
Wikipedia. (n.d.). Scammer Payback. Diakses dari https://en.wikipedia.org/wiki/Scammer_Payback