

Unveiling Gharar and Maysir in Digital Fraud: Shariah Perspectives on Account Hijacking and Identity Theft

Zee Athaya Sayidina¹, Triyono Adi Saputro²

¹ Department of Islamic Law, Faculty of Islamic Studies, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia

² Department of Islamic Law, Faculty of Islamic Studies, Universitas Muhammadiyah Surakarta, Surakarta, Indonesia

Abstract. The rapid development of digital technology has increased the risk of cybercrime. Account hijacking and identity theft, for example, may cause financial losses and undermine trust in digital economic systems. Many studies focus on technical and legal approaches to cybercrime. However, limited research examines these issues from the perspective of Islamic economic ethics. This study examines account hijacking and identity theft through the lens of *gharar* (uncertainty and deception) and *maysir* (unjustified gain) in Islamic commercial jurisprudence. This research employs a qualitative normative legal approach. It uses literature analysis of Islamic jurisprudence and cybercrime studies to examine the ethical implications of these practices within the framework of Shariah economic principles. The findings indicate that account hijacking and identity theft involve elements of deception, uncertainty, and unlawful appropriation of wealth. These acts contradict the principles of justice and fairness in Islamic economic transactions. This study contributes by providing a Shariah-based ethical framework for understanding cybercrime in the digital economy.

Keywords: digital fraud; account hijacking; identity theft; gharar and maysir

1 Introduction

The expansion of digital technologies has significantly transformed the global economic system by accelerating financial transactions, communication, and online service delivery. However, this transformation has also created new opportunities for cybercriminal activities, including hacking, identity theft, and online fraud, which exploit vulnerabilities in digital systems and financial platforms. Globally, cybercrime has become a major challenge affecting both developed and developing economies. Cybercrime has become a significant concern in the digital economy, particularly as individuals and businesses increasingly rely on online services and digital financial transactions. These developments expose users to

¹ Corresponding author: zeeathaya17@gmail.com

various forms of cybercrime that may cause financial losses and undermine confidence in digital economic systems (Anderson et al., 2013).

The global nature of cyber fraud demonstrates that digital financial crimes are no longer limited to specific jurisdictions but have become cross-border issues requiring international legal responses and stronger regulatory frameworks. At the same time, the rapid pace of digital transformation has outstripped the development of adequate regulatory and ethical frameworks, highlighting the need to examine the intersection of technology, law, and morality in financial ecosystems.

Internationally, countries have adopted different legal and regulatory approaches to address cybercrime and protect digital financial transactions. For example, the European Union has introduced the Digital Operational Resilience Act (DORA), which establishes a common framework for managing information and communication technology risks and strengthening digital operational resilience in the financial sector (Buttigieg & Zimmermann, 2024). Similarly, Singapore has established regulatory requirements for financial institutions concerning technology risk management and cybersecurity through the Monetary Authority of Singapore (Monetary Authority of Singapore, n.d.). Although these approaches differ in scope and implementation, they reflect a shared international concern regarding unauthorized access, misuse of personal information, and the security of digital financial systems. Nevertheless, regulatory and technological measures do not fully address the normative question of whether financial benefits obtained through deception and unauthorized access are legitimate. This issue provides a basis for examining digital fraud through Islamic economic law, particularly the concepts of *gharar* and *maysir*.

In digital financial systems, trust and security are fundamental to user adoption and sustainability. Cyber risks such as fraud, data misuse, and unauthorized access remain major barriers to the growth of financial technology (fintech) services. While technological innovations such as blockchain and artificial intelligence offer new security solutions, they also introduce increasingly sophisticated forms of cybercrime. This dual nature of technological development underscores the importance of not only technical safeguards but also ethical frameworks to ensure secure and trustworthy digital financial environments.

Among various forms of cybercrime, account hijacking and identity theft are particularly prevalent in the digital economy. These practices involve unauthorized access to digital accounts and the misuse of personal data to obtain financial benefits, often resulting in financial loss and erosion of institutional trust. In corporate contexts, such actions may also reflect broader issues of fraud, abuse of authority, and unethical digital conduct that compromise organizational credibility.

From the perspective of Islamic economics, fraudulent digital practices are inconsistent with Shariah principles that emphasize justice, transparency, and the lawful protection of wealth. The concept of *gharar* provides a relevant framework for examining uncertainty and deceptive practices in digital transactions, particularly when such practices undermine transparency and consumer protection (Aqmal et al., 2025). While these principles have been widely discussed in traditional and modern financial contexts, their application to contemporary digital fraud remains limited. Integrating Islamic ethical principles into digital financial governance therefore offers a valuable perspective for enhancing both compliance and public trust, particularly in Shariah-compliant financial systems.

Despite the growing body of literature on cybercrime, most studies focus primarily on technical, legal, and behavioral dimensions, with limited attention to ethical and normative analysis from the perspective of Islamic economic law. As a result, there is a lack of comprehensive frameworks that connect contemporary cybercrime practices with classical Islamic legal and ethical principles. This gap highlights the need for an interdisciplinary approach that integrates cybersecurity studies with Islamic commercial jurisprudence.

In particular, the application of *gharar* and *maysir* to analyze cybercrimes such as account hijacking and identity theft remains underexplored. These practices involve deception, manipulation of information, and unauthorized appropriation of digital assets, which may reflect elements prohibited in Islamic economic law. However, systematic analysis linking these concepts to modern digital fraud is still insufficient.

Therefore, this study aims to analyze account hijacking and identity theft through the concepts of *gharar* and *maysir* within Islamic economic law. By doing so, it seeks to bridge the gap between classical Islamic jurisprudence and contemporary digital challenges, while providing an ethical framework for understanding cybercrime in the digital economy. This study also contributes to the development of Shariah-based digital governance by offering insights for policymakers and financial institutions in designing ethical, secure, and trustworthy digital financial systems.

2 Method

This study employs normative legal research using conceptual and doctrinal approaches to examine cybercrime practices, particularly account hijacking and identity theft, from the perspective of Islamic economic law. Normative legal research is appropriate for examining legal norms, principles, and doctrines, while the conceptual approach facilitates the analysis of relevant legal concepts and scholarly perspectives (Negara, 2023).

The legal materials consist of primary and secondary sources. Primary legal materials include Indonesian legislation concerning electronic transactions and personal data protection, particularly Law No. 11 of 2008 on Electronic Information and Transactions, as amended by Law No. 19 of 2016 and Law No. 1 of 2024, and Law No. 27 of 2022 on Personal Data Protection. Secondary legal materials include books, journal articles, and previous studies related to cybercrime, digital fraud, and Islamic economic law. Islamic legal sources, including relevant Qur'anic verses, Islamic legal maxims, and scholarly literature on Islamic commercial jurisprudence, are also examined to identify the principles governing *gharar*, *maysir*, and the prohibition of unlawful acquisition of wealth.

The collected legal materials are analyzed qualitatively through doctrinal and conceptual analysis. The analysis involves examining relevant statutory provisions, interpreting Islamic legal principles, and relating these frameworks to the characteristics of account hijacking and identity theft. These practices are assessed in terms of deception, uncertainty, unauthorized control over digital assets, and the acquisition of financial benefits without valid authorization. The findings are then used to evaluate the legal implications of these practices under Indonesian law and their compatibility with the principles of Islamic economic law, particularly *gharar*, *maysir*, and the prohibition of unlawful appropriation of wealth.

3 Results and Discussion

3.1 Results

3.1.1 Account Hijacking as Unlawful Appropriation (*Akl al-Mal bi al-Batil*)

Account hijacking constitutes a form of digital fraud in which an unauthorized party gains control over another person's account and may use that access to obtain financial benefits or conduct transactions without the account holder's valid consent. This practice can occur through phishing, credential theft, malware, or the exploitation of security vulnerabilities. In digital financial services, successful authentication does not necessarily establish that a

transaction has been initiated by the legitimate account holder, particularly when login credentials have been obtained through deception or unauthorized means. Consequently, the technical completion of a transaction should be distinguished from its substantive legitimacy. When an individual uses another person's account to transfer or obtain assets without valid authorization, the conduct raises concerns regarding the protection of property rights and the legitimacy of financial transactions.

The international dimension of account hijacking is reflected in the broader economic consequences of cybercrime. Anderson et al. (2013) examine the direct, indirect, and defensive costs associated with cybercrime, highlighting its implications beyond individual victims and national jurisdictions. This broader perspective is relevant to account hijacking because unauthorized access to digital financial accounts may generate financial losses for account holders while imposing additional costs on financial institutions for fraud detection, incident response, and asset recovery. From the perspective of Islamic economic law, these consequences reinforce the importance of protecting property (*hifz al-mal*) and preventing the unlawful appropriation of wealth (*akl al-mal bi al-batil*).

From the perspective of Islamic economic law, account hijacking can be examined through the principle of *akl al-mal bi al-batil*, which prohibits the acquisition or appropriation of another person's wealth through illegitimate means. The Qur'an prohibits the wrongful consumption of others' wealth and emphasizes that commercial transactions should be based on mutual consent (Qur'an 2:188; 4:29). In account hijacking cases, the account holder's possession of an account and the credentials associated with it does not imply that an unauthorized party has acquired a legitimate right to use the account or dispose of its assets. Where funds are transferred without the owner's valid authorization, the transaction may constitute an unlawful appropriation of property. Therefore, the legal assessment of account hijacking should consider not only whether access was technically obtained but also whether the resulting use of the account was authorized and whether the transfer of assets had a legitimate legal basis.

The issue of uncertainty in digital transactions is also relevant to the concept of *gharar*. Aqmal et al. (2025), in their study of legal protection against *gharar* in Sharia e-commerce, explain that ambiguity, fraudulent practices, and insufficient transparency raise concerns regarding consumer protection and the legitimacy of digital transactions. Their analysis emphasizes the importance of clear contractual terms, adequate information, and responsibility in protecting consumers. Although their study focuses on e-commerce rather than account hijacking, its findings provide a conceptual basis for examining uncertainty in digital financial activities. In an account hijacking situation, the account holder may be unaware of a transaction, while the party initiating it may not possess valid authorization. This creates uncertainty regarding the identity and authority of the transacting party and the legitimacy of the resulting transaction. Accordingly, the principles of transparency and genuine consent are essential to assessing whether a digital transaction is consistent with Islamic economic law.

The prohibition of obtaining financial benefits through deceptive practices is further illustrated by (Yunita Sari et al., 2025), who analyze cash-swipe transactions from the perspective of Islamic economic law. Their study identifies dishonesty, fraud, and *riba* as elements that render such practices inconsistent with Islamic business ethics. The authors also emphasize that fraudulent financial practices undermine fairness, transparency, and trust in financial systems. Although cash-swipe transactions differ from account hijacking in their mechanisms, the study demonstrates the broader Islamic economic concern with financial benefits obtained through deceptive or illegitimate arrangements. A similar concern arises when perpetrators exploit unauthorized access to another person's account to transfer funds or obtain other financial advantages. Such conduct may be analyzed under *akl al-mal bi al-batil* because the benefit is acquired without a legitimate basis or valid authorization from

the rightful owner. This comparison does not establish that the two practices are legally identical; rather, it highlights the shared concern regarding dishonesty and the illegitimate acquisition of financial benefits.

The protection of digital accounts also depends on the reliability of the systems through which users access financial services. Alam et al. (2025), in their netnographic study of user feedback on Sharia fintech applications in Indonesia, analyze 129 reviews from five applications posted between July and December 2023. Their findings indicate that users generally appreciated the applications' ease of use and Sharia compliance, while negative feedback identified issues including payment delays, system errors, difficulties in account creation, and inadequate customer service. Although the study does not specifically investigate account hijacking or unauthorized financial transfers, it identifies operational challenges that are relevant to the broader discussion of digital financial service reliability and user protection. In the context of account hijacking, these concerns reinforce the importance of dependable account-management procedures and appropriate safeguards. From an Islamic economic perspective, such measures are consistent with the broader objectives of protecting wealth (*hifz al-mal*) and preventing harm (*la darar wa la dirar*). Nevertheless, technical safeguards must be accompanied by effective procedures for verifying authorization and responding to unauthorized transactions.

Taken together, these perspectives demonstrate that account hijacking should not be understood solely as a technical security incident. It also raises substantive legal questions concerning unauthorized access, the validity of consent, the protection of property, and the legitimacy of financial transactions. The principles of *akl al-mal bi al-batil* and *gharar* provide complementary analytical frameworks: the former addresses the wrongful acquisition of wealth, while the latter helps explain the uncertainty and lack of transparency that may arise when the identity or authority of a transacting party cannot be reliably established. Research on Sharia e-commerce, fraudulent financial practices, and user experiences with Sharia fintech applications provides additional context for understanding these concerns (Alam et al., 2025; Aqmal et al., 2025; Yunita Sari et al., 2025). However, the specific legal classification of an account hijacking incident depends on the facts of the case, including the method of access, the authorization status of the transaction, and whether financial assets were unlawfully obtained. Accordingly, the Islamic legal assessment should focus on protecting the rightful owner's assets, upholding genuine consent, and preventing harm.

3.1.2 Identity Theft and Deception (*Gharar*)

Identity theft may involve elements of *gharar fahish* because it involves the deliberate manipulation of personal data to construct false identities, resulting in significant information asymmetry between transacting parties. This condition invalidates informed consent, which is a fundamental requirement in Islamic commercial transactions, as one party operates under misleading assumptions regarding the identity of the counterparty. In digital financial systems, transactional validity is highly dependent on the accuracy and authenticity of identity verification. Therefore, when identity is falsified, the entire contractual basis of the transaction becomes defective, as the element of mutual recognition between parties is fundamentally compromised.

Mechanistically, identity theft operates through the unauthorized acquisition and misuse of personal credentials such as login information, biometric data, or digital identification records to impersonate legitimate users within financial systems. This process enables perpetrators to bypass authentication mechanisms and initiate transactions that appear legally valid but are substantively fraudulent. As a result, the victim is unknowingly placed in a

position where their identity is used as an instrument of deception, creating a hidden asymmetry in information that distorts the transactional environment. This aligns with findings in cybersecurity research that identify information asymmetry and identity manipulation as central drivers of digital fraud.

From an international perspective, identity-related crime often has a transnational dimension, particularly when digital services, electronic communications, and the individuals involved are located in different jurisdictions. The United Nations Office on Drugs and Crime emphasizes the importance of international cooperation in investigating identity-related crime because such cases may involve multiple countries and different legal systems (United Nations Office on Drugs and Crime, 2011). This context demonstrates that identity theft is not merely a matter of unauthorized personal data use but may also undermine the reliability of digital transactions. From the perspective of Islamic economic law, the use of another person's identity to conduct transactions without valid authorization involves elements of *tadlis* (deception), while the resulting uncertainty regarding the identity and authority of the transacting party may raise concerns related to *gharar*. Accordingly, the legitimacy of such transactions should be assessed by considering the presence of genuine consent, valid authorization, and the rights of the parties involved.

From the perspective of Islamic commercial jurisprudence, such asymmetry reflects *gharar fahish*, as it introduces a level of uncertainty that directly affects the essence ('*aqd*) of the transaction. Unlike *gharar yasir*, which may be tolerated in limited circumstances, identity theft generates substantial uncertainty that undermines both transparency and contractual clarity. The presence of falsified identity eliminates the possibility of genuine consent (*ridha*) and disrupts the balance required in lawful exchange. In this regard, identity theft does not merely introduce risk but fundamentally alters the nature of the transaction itself, rendering it invalid under Shariah principles.

In addition to *gharar*, identity theft also overlaps with elements of *tadlis* (fraud through misrepresentation), as it involves intentional deception designed to mislead other parties. This dual classification suggests that identity theft cannot be fully captured by a single legal concept but rather represents a compounded violation within Islamic legal theory. The intentional construction of false identities demonstrates a deliberate effort to manipulate perception, which goes beyond uncertainty and enters the domain of active fraud. This reinforces the argument that cybercrime in digital environments often involves layered ethical breaches that require multidimensional analysis rather than isolated categorization.

The persistence of identity theft is associated not only with technological vulnerabilities but also with human behavior and information security practices. Crossler et al. (2013) emphasize the importance of behavioral factors in information security research, providing a broader basis for understanding how individual actions and security-related practices can affect information security. In the context of identity theft, inadequate security awareness, weak password management, and susceptibility to phishing may increase users' exposure to identity-based attacks. This suggests that addressing identity theft requires not only technological safeguards but also greater user awareness and effective information security practices.

From a legal and ethical standpoint, identity theft results in the invalidation of transactions and the unlawful transfer of rights and obligations. Since the affected party does not provide genuine consent, any resulting transaction lacks legitimacy and may be classified as void (*batil*). Furthermore, such practices violate fundamental Islamic principles, including justice ('*adl*), transparency, and the prohibition of harm (*la darar wa la dirar*), as they impose financial and psychological losses on victims without their knowledge or approval. The misuse of identity also erodes the integrity of digital financial systems, as it undermines the reliability of identity-based verification mechanisms that are essential for modern transactions.

Therefore, identity theft should be understood not merely as a form of cybercrime but as a structural ethical failure that disrupts the foundational principles of Islamic economic transactions. It simultaneously embodies *gharar fahish* through uncertainty, *tadlis* through intentional deception, and results in legal invalidity due to the absence of consent. Addressing this issue requires not only technical safeguards but also the integration of ethical awareness, user responsibility, and institutional accountability to restore transparency and fairness in digital financial ecosystems.

3.1.3 *Unjust Enrichment and Maysir*

Both account hijacking and identity theft involve unjust financial gain obtained without legitimate effort or mutual consent. This occurs because perpetrators exploit system vulnerabilities and manipulate access or identity in order to transfer economic benefits without engaging in lawful exchange. In such cases, the gain is not derived from productive activity or mutually agreed transactions, but from opportunistic and unauthorized control over digital assets. Unlike conventional economic activities, where value is created through exchange, production, or service, these practices rely on the extraction of value from existing systems without contributing any real economic output.

Mechanistically, this form of gain is achieved through the successful execution of exploitative actions such as unauthorized access, credential manipulation, or identity falsification, which allow perpetrators to capture financial benefits while externalizing the risks to victims. The outcome of such actions is inherently uncertain, as it depends on the success of system exploitation and the failure of detection mechanisms. This introduces a probabilistic dimension similar to speculative gain, where the perpetrator engages in actions with uncertain outcomes but potentially high returns. In this sense, the process does not follow a structured contractual exchange but rather resembles opportunistic extraction under conditions of uncertainty and asymmetrical information.

These characteristics closely reflect the concept of *maysir* in Islamic commercial jurisprudence, where financial gain is obtained through uncertain and unjust mechanisms rather than legitimate economic activity. While classical *maysir* is often associated with gambling, the underlying principle lies in the presence of gain without commensurate effort and the transfer of wealth based on uncertain or exploitative conditions. Cybercrime practices extend this logic into the digital domain, where uncertainty is not generated through games of chance but through manipulation of technological systems and information asymmetry. Although account hijacking and identity theft may generate unlawful financial gains, such gains should not automatically be classified as *maysir*. The more direct Shariah concern is the unlawful appropriation of wealth (*akl al-mal bi al-batil*), while *tadlis* and *gharar* may be relevant where deliberate deception or material transactional uncertainty is established. The application of *maysir* therefore requires a separate and carefully justified analogy with its established meaning in Islamic commercial jurisprudence.

The broader implications of cybercrime in digital financial systems are also reflected in research on financial crime in digital payments. Wiwoho et al. (2021) explain that the real-time, non-face-to-face, and borderless characteristics of digital payment transactions create potential risks for financial crime. These characteristics provide important context for understanding how unauthorized access and identity manipulation may be exploited to obtain financial benefits. In account hijacking and identity theft cases, perpetrators may use digital systems to transfer assets without the legitimate owner's authorization. Such conduct should be distinguished from lawful economic activity because the financial benefit is obtained through unauthorized exploitation rather than a valid exchange of goods or services. From the perspective of Islamic economic law, this distinction supports the analysis of such gains

as potential instances of *akl al-mal bi al-batil*, rather than automatically classifying every form of illicit gain as *maysir*.

From an economic perspective, such gains resemble non-productive financial behavior that lacks real value creation and contributes to systemic inefficiencies. Resources are diverted from productive use toward defensive measures such as cybersecurity investments, fraud mitigation, and loss recovery, thereby increasing operational costs within financial systems (Anderson et al., 2013). This reinforces the view that cybercrime not only harms individual victims but also generates broader negative externalities that affect the stability and efficiency of digital financial ecosystems.

From a legal and ethical standpoint, the absence of valid consent and the presence of exploitation invalidate the legitimacy of any resulting transaction, rendering the gain unlawful (*haram*). Such practices violate fundamental principles in Islamic economic law, including justice (*'adl*), accountability, and the prohibition of harm (*la darar wa la dirar*). The transfer of wealth in these cases does not occur through mutually agreed exchange (*taradhi*), but through coercive or deceptive mechanisms that disadvantage one party. As a result, the gains obtained cannot be recognized as legally valid and may require restitution to restore justice between parties.

Furthermore, the findings of this study indicate that cybercrime practices such as account hijacking and identity theft embody a dual violation: they combine elements of unlawful appropriation (*akl al-mal bi al-batil*) and unjust enrichment (*maysir*). While the former explains the illegitimacy of the transfer, the latter highlights the nature of the gain itself as exploitative and non-productive. This dual framework provides a more comprehensive understanding of cybercrime within Islamic legal theory, demonstrating that digital fraud operates across multiple dimensions of ethical and legal violation rather than fitting into a single category.

The persistence of such practices also suggests that existing digital financial systems may insufficiently address the ethical dimensions of economic behavior. While technical safeguards aim to reduce system vulnerabilities, they do not necessarily eliminate the incentive structures that enable exploitative gain. This highlights the importance of integrating Shariah-based ethical principles into institutional governance, particularly in shaping policies that discourage opportunistic behavior and promote accountability among users and system operators.

Consequently, cybercrime practices such as account hijacking and identity theft should be understood not only as legal violations but as structural ethical failures that undermine the normative foundations of Islamic economic systems. Addressing these issues requires a comprehensive approach that combines technical security measures with ethical governance frameworks, ensuring that digital financial systems are not only secure but also aligned with principles of fairness, transparency, and justice. This study therefore demonstrates that the concept of *maysir* remains highly relevant in the digital era, providing a critical lens for evaluating emerging forms of unjust enrichment within technologically mediated financial environments.

3.2 Discussion

3.2.1 Integrating Islamic Ethics into Digital Financial Governance

Digital fraud may involve *gharar* when material uncertainty concerns the identity of the parties, ownership of digital assets, authorization, or the legitimacy of a transaction. Deliberate misrepresentation or manipulation of material information may also be examined through the concept of *tadlis*. Nafsi et al. (2024) demonstrate the relevance of these principles

in online transactions by identifying unclear product information and price manipulation as practices that may undermine transparency and fairness. Although their study focuses on online auctions rather than account hijacking or identity theft, it provides a conceptual basis for examining deception and uncertainty in digital interactions. In the context of this study, these principles are applied to assess whether unauthorized access and identity manipulation undermine the legitimacy of digital financial transactions.

More importantly, this study finds that the persistence of cybercrime reflects a misalignment between system design and ethical accountability. Digital financial systems tend to prioritize efficiency and speed of transactions, often assuming that technical authentication is sufficient to validate legitimacy. However, the analysis shows that authentication does not necessarily reflect consent, particularly when credentials are compromised. This indicates that cyber risk is not only a failure of system protection but also a failure to incorporate legal protection mechanisms within transaction processes. In this context, *gharar* emerges not merely as uncertainty in outcome, but as uncertainty embedded within system logic, where users cannot fully verify whether a transaction genuinely reflects their intent.

From a legal and ethical standpoint, integrating *gharar* and *maysir* into governance frameworks reinforces core Islamic principles, including justice (*'adl*), transparency, and the prohibition of harm. The failure to regulate uncertainty and unjust enrichment results in transactions that are formally executed but substantively unjust, thereby undermining the legitimacy of digital financial systems. This condition shifts the evaluation of cybersecurity from a purely technical issue to a normative one, where the objective is not only to prevent system intrusion but to ensure that all transactions reflect lawful ownership, valid consent, and equitable exchange.

The analysis further indicates that cyber risk is shaped by the interaction between technological systems and human behavior. Weak user awareness, poor security practices, and organizational negligence contribute to the persistence of *gharar* and *maysir* within digital environments. However, this study goes further by showing that these behavioral weaknesses are not isolated issues, but are structurally enabled by systems that do not enforce legal accountability. Users are often positioned as the weakest link, yet the system design itself does not adequately compensate for predictable human error. This suggests that effective governance must move beyond awareness-based approaches and incorporate ethical safeguards directly into system architecture.

Aligning digital financial governance with Shariah principles can serve as a preventive strategy that addresses both structural and behavioral dimensions of cyber risk. This requires integrating Shariah-based legal principles into organizational policies, compliance frameworks, and digital governance mechanisms. Such an approach shifts cybersecurity from a purely reactive model focused on detecting and responding to attacks toward a preventive model that reduces opportunities for unauthorized access and fraudulent transactions. In this context, *gharar* and *tadlis* can help evaluate uncertainty and deception in digital transactions, while *akl al-mal bi al-batil* provides a more direct framework for assessing the unlawful acquisition of wealth. The application of *maysir* requires separate jurisprudential justification and should not be assumed in every case of digital fraud.

Ultimately, integrating Islamic legal principles into digital financial governance can complement existing cybersecurity and regulatory frameworks by connecting technical safeguards with lawful ownership, valid consent, transparency, and accountability. Rather than treating ethical concerns as the sole cause of cybercrime, this approach recognizes that digital fraud can emerge from interactions among technological vulnerabilities, human behavior, and institutional weaknesses. Accordingly, Shariah principles can provide a normative framework for evaluating whether digital financial transactions respect the rights of the parties involved and whether appropriate mechanisms exist to prevent, investigate, and

address unauthorized transactions. This approach can contribute to digital financial systems that are more secure, transparent, and consistent with the principles of justice and the protection of wealth.

4 Conclusion

This study reveals that cybercrime, particularly account hijacking and identity theft, can be analyzed as a form of unlawful conduct under Indonesian law and Islamic economic law. Through normative legal analysis, these practices are associated with unlawful wealth appropriation (*akl al-mal bi al-batil*), deception (*tadlis*), and, under specific circumstances, elements that may be examined through the concept of *gharar* and the prohibition of unjustified gain. The findings indicate that unauthorized access, the misuse of personal identity, and the acquisition of financial benefits without valid authorization undermine the legal validity of transactions and the protection of property rights. These findings demonstrate the relevance of Islamic legal principles in analyzing digital fraud alongside Indonesian legislation on electronic information and transactions and personal data protection. This study contributes a normative legal perspective for assessing account hijacking and identity theft within the framework of Islamic economic law. Future research may examine the practical application of these legal principles in preventing and addressing digital fraud in financial institutions.

References

- Alam, A., Raihan, F. A., Al Bagir, M., Kurniawan, A. W., & Yusuf, J. Bin. (2025). Exploring User Feedback on Sharia FinTech Apps: A Netnographic Study in Indonesia. *International Journal of Informatics and Communication Technology (IJ-ICT)*, 14(2), 663–672. <https://doi.org/10.11591/ijict.v14i2.pp663-672>
- Anderson, R., Barton, C., Böhme, R., Clayton, R., van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2013). Measuring the Cost of Cybercrime. In *The Economics of Information Security and Privacy* (pp. 265–300). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-39498-0_12
- Aqmal, F. Z., Muthoifin, & Sana Ashraf. (2025). Legal Protection Against Gharar in Sharia E-Commerce: A Consumer Law Analysis in Support of the SDGs. *Profetika: Jurnal Studi Islam*, 26(02), 615–630. <https://doi.org/10.23917/profetika.v26i02.12036>
- Buttigieg, C. P., & Zimmermann, B. B. (2024). The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision. *ERA Forum*, 25(1), 11–28. <https://doi.org/10.1007/s12027-024-00793-w>
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future Directions for Behavioral Information Security Research. *Computers & Security*, 32, 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>
- Nafsi, S. U., Fahmi, C., & Sholihin, R. (2024). The Validity of Used Goods Auction Practices on Facebook Platform. *JURISTA: Jurnal Hukum Dan Keadilan*, 8(2), 622–643. <https://doi.org/10.22373/jurista.v8i2.195>
- Negara, T. A. S. (2023). Normative Legal Research in Indonesia: Its Originis and Approaches. *Audito Comparative Law Journal (ACLJ)*, 4(1), 1–9. <https://doi.org/10.22219/aclj.v4i1.24855>
- United Nations Office on Drugs and Crime. (2011). *Handbook on Identity-related Crime*. https://www.unodc.org/documents/congress/background-information/Corruption/Handbook_on_Identity-related_Crime_ENG.pdf

- Wiwoho, J., Kharisma, D. B., & Wardhono, D. T. K. (2021). Financial Crime in Digital Payments. *Journal of Central Banking Law and Institutions*, 1(1), 47–70. <https://doi.org/10.21098/jcli.v1i1.7>
- Yunita Sari, Muthoifin, Amel Saib, & Aboubacar Barry. (2025). Analysis of Cash Swipe Transactions in the Framework of Islamic Economic Law and Their Alignment with Sustainable Development Goals (SDGs). *Profetika: Jurnal Studi Islam*, 25(01), 259–272. <https://doi.org/10.23917/profetika.v25i01.3411>