**Legal Autonomous Web-based Governance (LAW)**
Vol. 1, No. 3, February 2027, pp. 273∼282
E-ISSN: 3164-6794 | P-ISSN: 3164-6697


# Legal Protection Against Online Fraud in Electronic Transactions

Adinda Khairunnisa[1*], Adella Ramadhanty Pratiwi[1], Badriyah[1], Dippo Alam[1]
[1]Faculty of Law, Universitas Islam Syekh Yusuf, Indonesia
[1]Adinda17khairunnisa@gmail.com, [1]dearamadhanty7@gmail.com, [1]badriahalbaihaqi@gmail.com, [1]dippoalam0811@gmail.com
***Corresponding Author**

**Article Info**

***Article history:***

Submission, April 24, 2026
Revised, July 07, 2026
Accepted, October 16, 2026
Published, October 31, 2026

***Keywords:***

Criminal Code
Electronic Transactions
Legal Protection
Online Fraud

**ABSTRACT**

This research is motivated by the increasing number of online fraud cases in electronic transactions, which have caused losses to the public and the challenges facing law enforcement in the digital era. **The purpose of** this research is to analyze the legal perspective on online fraud and the effectiveness of existing regulations in providing legal protection for victims. **The method** used in this research is a normative legal approach with a statutory approach and literature review, which examines various legal provisions, such as the Criminal Code (KUHP) and the Electronic Information and Transactions Law (UU ITE). **The findings** indicate that Indonesia's existing legal framework, particularly the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), provides a legal basis for addressing online fraud, but its practical effectiveness remains constrained by difficulties in authenticating digital evidence, limited digital forensic capacity, and insufficient public awareness of transaction security. **The analysis** further identifies a gap between the availability of legal provisions and their effective implementation. **Accordingly, this study** recommends strengthening digital evidence-handling procedures, improving law enforcement expertise, enhancing preventive obligations for digital platforms, and expanding public digital literacy programs to improve legal protection for victims of online fraud.

*This is an open access article under the CC BY 4.0 license.*

DOI: https://doi.org/10.68012/law.v1i3.174
This is an open access article under the CC BY license (https://creativecommons.org/licenses/by/4.0/)
©Authors retain all copyrights

## 1. INTRODUCTION

The rapid development of digital technology has brought significant changes to various aspects of people's lives, including electronic transactions [1]. Ease of internet access and the increasing use of digital platforms such as e-commerce, social media, and online payment applications have created an increasingly complex and dynamic digital economic ecosystem [2]. However, behind this progress, various legal issues have also emerged, one of which is the rise in online fraud. Based on data from the Indonesian National Police and reports from various cybersecurity agencies, digital-based fraud cases have increased significantly each year, in line with the increasing number of internet users in Indonesia, which has exceeded 200 million users [3]. Fraud methods are also increasingly diverse, ranging from phishing and social engineering to fraud in online transactions [4]. This shows that digital transformation not only brings opportunities but also risks that need to be seriously anticipated through a comprehensive legal approach [5]. In a global context, this phenomenon is also related to the achievement of the Sustainable Development Goals (SDGs), particularly

Goal 16, Peace, Justice, and Strong Institutions, which emphasizes the importance of a strong, transparent legal system capable of protecting society from crime, including cybercrime [6]. From the perspective of technology law and digital governance, online fraud in electronic transactions raises interconnected issues concerning the enforcement of cybercrime regulations, the reliability of electronic evidence, cybersecurity, and the protection of transaction users [7]. Examining these issues within the Indonesian legal framework provides a basis for assessing how legal institutions and regulatory mechanisms can respond to risks arising from the digital economy [8]. Although Indonesia has various regulations governing electronic transactions, such as the Electronic Information and Transactions Law (UU ITE), the implementation of the law against online fraud cases still faces various challenges [9]. One major problem is the difficulty in obtaining digital evidence, which often requires specialized technical expertise and adequate digital forensic infrastructure. Furthermore, legal loopholes and mismatches between technological developments and existing regulations also hinder law enforcement [10]. This problem is exacerbated by the low digital literacy of the public, which makes them vulnerable to fraud. From the perspective of law enforcement, the limited human resources with competency in information technology also poses a serious obstacle. Against this background, the study examines how Indonesia's existing legal framework addresses online fraud in electronic transactions, with particular attention to evidentiary challenges, law enforcement capacity, and the need for regulatory adaptation [10].

This research also contributes to strengthening law-based public policies to support a safe and sustainable digital ecosystem, in line with SDGs goal 9 (Industry, Innovation, and Infrastructure) and goal 16 [11]. Therefore, analyzing the effectiveness of regulations and law enforcement practices is crucial in building public trust in electronic transaction systems [12]. Based on the background and problems mentioned above, this study aims to answer several main questions that are the focus of the study [13]. First, how are the legal regulations in force in Indonesia regarding online fraud crimes in electronic transactions, and to what extent are these regulations able to provide legal protection for the public? Second, what are the dynamics and challenges in the application of the law to online fraud cases, both in terms of evidence, law enforcement, and institutional aspects? Third, is there a need to develop or update regulations that are more adaptive to the development of digital technology, and what policy recommendations can be proposed to increase the effectiveness of legal protection in the future. Previous studies have examined online fraud from several perspectives, including cybercrime trends, digital evidence, fraud detection technologies, and legal protection for victims [14]. However, these perspectives need to be connected more explicitly to explain how the adequacy of legal provisions interacts with evidentiary constraints, institutional capacity, and preventive mechanisms in electronic transactions. To address this analytical gap, the present study employs an integrated normative legal analysis of online fraud in Indonesia [15]. It examines the relationship between the applicable legal framework, the practical challenges of law enforcement, and technology-oriented preventive measures [16]. Its contribution lies in synthesizing these dimensions to identify implementation gaps and formulate legal and institutional recommendations for strengthening victim protection in the digital economy [17]. Furthermore, this research is also expected to increase public awareness of the importance of security in electronic transactions, thereby minimizing the risk of crime in the digital era [18].

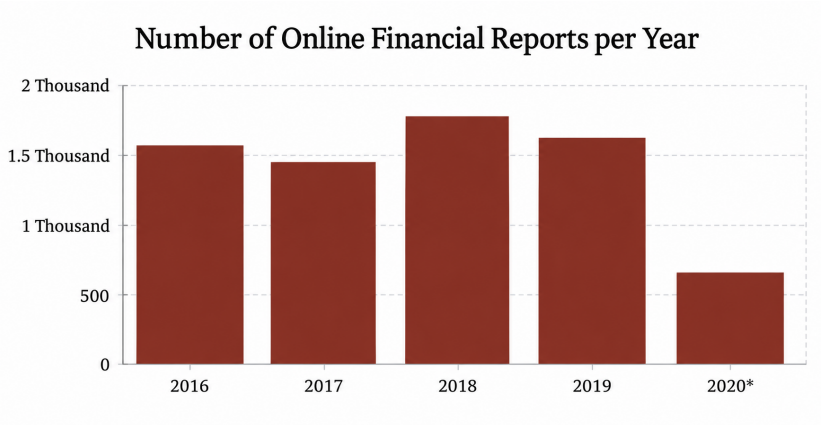



Figure 1. Reported Online Fraud Cases in Indonesia, 2020–2024

Figure 1 illustrates the reported cases of online fraud in Indonesia from 2020 to 2024, showing a

significant upward trend in reported incidents over the five-year period. The increase from approximately 4,500 reports in 2020 to approximately 14,000 reports in 2024 highlights the growing challenges associated with the expansion of electronic transactions and digital platforms [19]. This trend reinforces the importance of effective legal protection against online fraud, particularly through stronger enforcement of the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP) [20]. However, the increasing number of reports also emphasizes the need to address practical enforcement challenges, including the authentication of electronic evidence, limited digital forensic capabilities, and insufficient public awareness of transaction security [21]. Therefore, Figure 1 supports the need for an integrated approach that combines effective legal enforcement, institutional capacity building, preventive measures by digital platforms, and improved public digital literacy to strengthen legal protection in Indonesia's digital economy [22].

## 2. LITERATURE REVIEW

The development of digital technology has driven a major transformation in the economic transaction system, known as electronic transactions. Electronic transactions are legal activities conducted using electronic devices and the internet as the primary medium, regulated by various national regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions (UU ITE) and its amendments [23]. In this context, electronic transactions not only create efficiency and convenience, but also give rise to new legal risks, particularly related to data security and the potential for cybercrime. The literature shows that economic digitalization without a strong security system and regulations will increase vulnerability to cybercrime, including online fraud [24]. Online fraud itself is defined as the act of manipulating or misusing information technology to obtain unlawful benefits at the expense of others [25]. It takes various forms, such as phishing, scams, impersonation, and marketplace-based fraud. In criminal law studies, this act is closely related to the elements of fraud as stipulated in the Criminal Code (KUHP), but its digital characteristics make it more complex in terms of proof and law enforcement [26].

From a legal perspective, addressing online fraud requires a multidisciplinary approach that combines criminal law, cyber law, and information technology. The existing literature reflects two complementary perspectives on online fraud regulation [27]. The first emphasizes the importance of statutory provisions in establishing the legal basis for prosecuting offenders, while the second highlights the practical difficulties of translating these provisions into effective enforcement [28]. The distinction is important because the existence of a legal prohibition does not automatically ensure successful prosecution or adequate victim protection. In online fraud cases, the effectiveness of legal remedies also depends on the availability and integrity of electronic evidence, the technical competence of investigators, and coordination among relevant institutions [29]. Consequently, the central analytical issue is not solely whether legal provisions exist, but whether the legal framework and enforcement mechanisms operate effectively together. This synthesis supports an integrated assessment of substantive law, evidentiary procedures, institutional capacity, and preventive governance in electronic transactions [30]. Furthermore, the theory of legal protection states that the state has an obligation to guarantee public security, including in the digital space [31]. In this regard, legal protection is not only repressive (Taking action against perpetrators), but also preventive, such as digital literacy education and improving transaction security systems [32]. Other studies have emphasized the importance of digital forensics in the evidentiary process, as electronic evidence is easily altered, deleted, or falsified [33]. Therefore, the capacity of law enforcement officials to understand digital technology is a key factor in successfully handling online fraud cases [34].

Furthermore, research in the field of law and technology indicates a gap between technological developments and existing regulations (Regulatory Lag) [35]. This often leads to laws being reactive, rather than proactive, in addressing cybercrime. Several alternative approaches proposed in the literature include more adaptive regulatory reforms, the application of techno-legal principles, and strengthening cross-sectoral cooperation between government, the private sector, and the public [36]. At the international level, the Council of Europe's Convention on Cybercrime (Budapest Convention) provides a framework for criminalizing specified cybercrime-related conduct and facilitating international cooperation in criminal investigations and electronic evidence gathering [37]. Within the European Union, Directive 2013/40/EU establishes minimum rules concerning criminal offences and sanctions against attacks on information systems and promotes cooperation among competent authorities [38]. These instruments offer useful comparative perspectives on legal harmonization, investigative cooperation, and the handling of technology-related offences. However, their provisions should not be assumed to apply directly to Indonesia. Instead, they can serve as comparative references

for assessing how Indonesia might strengthen cross-border cooperation, clarify investigative procedures, and improve the effectiveness of its domestic cybercrime framework [39]. Such comparison should also consider differences in legal systems, institutional capacity, and applicable procedural safeguards. Furthermore, the integration of technologies such as Artificial Intelligence (AI) into digital security systems is also being developed to detect fraud patterns more quickly and accurately [40]. Addressing online fraud is relevant to SDG 16, which emphasizes effective institutions and access to justice, and SDG 9, which supports resilient infrastructure and innovation. These goals provide a broader policy context for examining legal protection and security in electronic transactions [41]. Thus, this literature review confirms that research on the legal review of online fraud is not only academically relevant but also has broad practical implications in supporting SDG in the digital era [42].

## 3. RESEARCH METHODS

This study employs a normative juridical approach to examine the legal framework governing online fraud in electronic transactions in Indonesia [43]. The analysis focuses on the relevant statutory provisions, the legal requirements for establishing online fraud offenses, the treatment of electronic evidence, and the implications of identified implementation challenges for legal protection [44]. These dimensions are examined using statutory and conceptual approaches, supported by relevant legal literature and documented cases where available.

This approach was chosen because the research aims to analyze legal aspects conceptually and systematically based on relevant laws and regulations, such as Law Number 11 of 2008 concerning Electronic Information and Transactions and its amendments, as well as the Criminal Code (KUHP). The research applies statutory, conceptual, and case-based approaches. The statutory approach examines the relevant provisions governing online fraud, electronic transactions, and electronic evidence. The conceptual approach is used to interpret legal protection, cybercrime, and preventive legal mechanisms. The case-based analysis examines documented online fraud cases that are relevant to the research questions and provide information about the application of legal provisions in practice. Cases should be selected according to their relevance to electronic transactions, the availability of reliable legal documentation, and their ability to illustrate evidentiary or enforcement challenges. Each selected case is analyzed by identifying the relevant legal issues, applicable provisions, treatment of electronic evidence, and implications for victim protection. The analysis then compares the resulting observations with the statutory framework and conceptual arguments to identify gaps between legal norms and their implementation. This study relies on secondary legal research materials, which are classified into primary, secondary, and tertiary legal materials. Primary legal materials comprise relevant legislation and regulations, while secondary legal materials include scholarly publications and legal analyses. Tertiary legal materials consist of reference sources used to clarify relevant legal terms and concepts.

Primary legal materials include laws and regulations such as the ITE Law, the Criminal Code, and other related regulations governing electronic transactions and cybercrime. Secondary legal materials include scientific journals, books, research articles, and academic publications relevant to the research topic, particularly those discussing cybercrime, online fraud, and legal protection in digital transactions. Meanwhile, tertiary legal materials include legal dictionaries, encyclopedias, and other sources that support understanding of the terms and concepts used in the research. Data collection techniques are carried out through library research, namely by collecting and reviewing various literature and legal documents relevant to this research.

The data analysis technique used was descriptive qualitative analysis, which involves interpreting and reviewing the collected data and then systematically organizing it to answer the research problem formulation. The analysis was conducted by examining the alignment between applicable legal norms and actual practices, particularly in handling online fraud cases. Furthermore, the strengths and weaknesses of existing regulations were analyzed, as well as identifying legal loopholes potentially exploited by criminals. This analysis also considered the effectiveness of the law in protecting the public and its relevance to the ever-changing development of digital technology. The results of the analysis were then used to formulate constructive recommendations to improve the quality of regulation and law enforcement in the field of electronic transactions. To ensure research validity, source triangulation was conducted using reliable national and international references. The research also upheld academic honesty and objectivity, aiming to provide a comprehensive legal analysis of online fraud and contribute to the development of cyber law in Indonesia.

## 4. RESULTS AND DISCUSSION

Research results show that online fraud in electronic transactions in Indonesia has experienced a significant increase, both in terms of the number of cases and the complexity of the modus operandi. Based on an analysis of various previous reports and studies, online fraud is no longer limited to conventional methods such as simple sales fraud, but has evolved into more sophisticated forms such as phishing, social engineering, fraud-based investment fraud, and identity impersonation through social media. This phenomenon demonstrates that cybercriminals are able to adapt quickly to technological developments and digital user behavior. From a regulatory perspective, the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP) have actually provided a sufficient legal basis for prosecuting perpetrators. However, in practice, effective law enforcement still faces various obstacles, particularly in terms of digital evidence, tracking perpetrators across regions, and limited human resources competent in the field of information technology. The findings can be organized into three interrelated dimensions. First, the legal framework provides a basis for addressing online fraud, but its practical effectiveness depends on the clarity and applicability of the relevant provisions. Second, enforcement outcomes depend on the integrity of electronic evidence, the availability of digital forensic facilities, and investigators' technical competence. Third, preventive protection requires coordinated action by public institutions, digital platforms, and electronic transaction users. These dimensions indicate that improving legal protection requires more than statutory enforcement it also requires institutional readiness and effective prevention mechanisms. Although existing regulations provide a legal basis for addressing online fraud, their effectiveness depends on the ability of law enforcement agencies to establish the relevant elements of an offense through reliable digital evidence. Consequently, strengthening legal protection requires not only regulatory enforcement but also improved forensic capacity, institutional coordination, and preventive measures that are consistent with applicable legal principles.

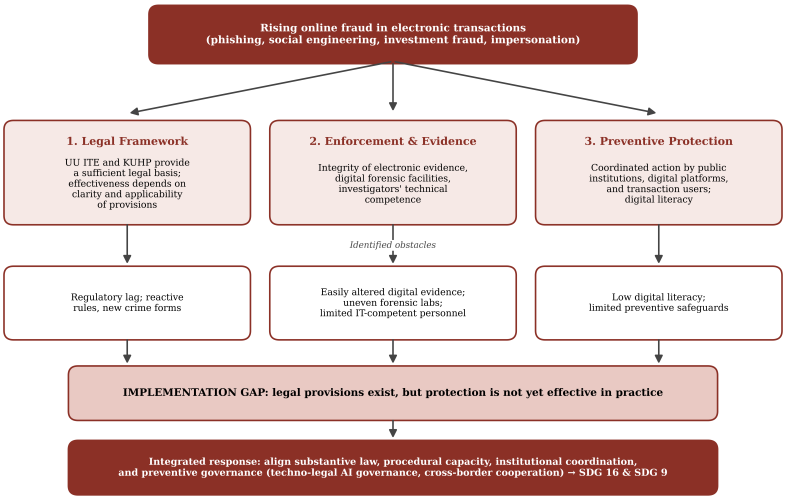



Figure 2. Framework of the implementation gap in legal protection against online fraud

Figure 2 summarizes the findings as three interrelated dimensions: the legal framework, enforcement and evidence, and preventive protection. Each dimension faces its own obstacle, namely regulatory lag, difficulties in authenticating digital evidence and limited forensic capacity, and low digital literacy. Together these obstacles produce an implementation gap, in which legal provisions exist but do not yet translate into effective protection. Closing the gap requires aligning substantive law, procedural capacity, institutional coordination, and preventive governance, which supports SDG 16 and SDG 9.

The identified implementation gap suggests that the effectiveness of online fraud regulation cannot be assessed solely by the existence of statutory provisions. Legal protection depends on whether investigators can obtain and authenticate electronic evidence, whether institutions possess the technical capacity to process that evidence, and whether victims can access effective remedies. These factors are interdependent unclear procedures or limited forensic resources may weaken the practical application of otherwise relevant legal provisions, while inadequate preventive safeguards may allow fraud to occur before law enforcement becomes involved.

Therefore, the principal challenge is not simply regulatory insufficiency, but the need to align substantive law, procedural capacity, institutional coordination, and preventive governance. This interpretation indicates that improvements in legal protection should be evaluated through both the adequacy of the regulatory framework and its practical implementation. In terms of evidence, research results indicate that electronic evidence often poses a major challenge in the judicial process. Digital evidence is easily manipulated, deleted, or falsified, requiring specialized expertise in digital forensics. Furthermore, the unequal distribution of digital forensic laboratory facilities in Indonesia hinders the investigation process. From the victim's perspective, low digital literacy also exacerbates the situation, as many people do not understand the risks and how to secure electronic transactions. This demonstrates that legal protection depends not only on regulations but also on public preparedness to face digital threats. This discussion demonstrates that preventative approaches such as digital literacy education and raising cybersecurity awareness are as important as repressive approaches through law enforcement. In other words, strategies to combat online fraud must be holistic and involve various parties, including the government, the private sector, and the public.

Table 1. Implementation Challenges, Their Impact on Legal Protection, and Policy Responses

| **Aspect** | **Main Challenge** | **Impact on Legal Protection** | **Policy Response** |
|---|---|---|---|
| Legal Framework | UU ITE and KUHP provide a sufficient basis, but regulations are reactive and lag behind new fraud modes | Provisions exist but are not fully effective in practice | Adaptive regulatory reform |
| Electronic Evidence | Digital evidence is easily manipulated, deleted, or falsified | Weakens proof of the elements of an offense | Standardized evidence-preservation and authentication procedures |
| Forensic Capacity and Human Resources | Forensic laboratories are unevenly distributed and few investigators are IT-competent | Slows investigation and perpetrator tracing across regions | Strengthen forensic infrastructure and investigator expertise |
| Public Digital Literacy | Many users do not understand transaction risks and security | Fraud occurs before law enforcement becomes involved | Digital literacy education and cybersecurity awareness |
| AI-Based Fraud Detection | Risk of false positives, unrecognized fraud patterns, and biased data | Possible unjustified account restrictions and loss of legal certainty | Algorithmic governance with audits, human review, and data protection |
| Cross-Border Cooperation | Cybercrime is borderless | Hinders handling of cross-jurisdiction cases | Legal harmonization and cooperation among law enforcement agencies |

Table 1 shows that the effectiveness of legal protection depends on more than the existence of statutory provisions. Each challenge, from evidence authentication and forensic capacity to public literacy, AI governance, and cross-border cooperation, affects how far legal provisions can be applied in practice. The corresponding policy responses therefore need to be implemented together, combining repressive enforcement with preventive measures, in line with the holistic strategy discussed above.

Furthermore, the analysis indicates an urgent need for regulatory reforms that are more adaptive to technological developments. Existing regulations tend to be reactive and unable to anticipate the various new forms of crime that continue to emerge. A techno-legal approach should consider not only the use of AI for early fraud detection but also the governance of the algorithms that support these decisions. AI systems can assist digital platforms in identifying unusual transaction patterns, detecting suspicious account behavior, and prioritizing cases for further investigation. However, their effectiveness depends on data quality, model vali-

dation, appropriate access controls, and continuous monitoring. Poorly designed systems may generate false positives, overlook unfamiliar fraud patterns, or reproduce biases in historical data. Accordingly, algorithmic governance should establish clear responsibilities for system operators, require documented performance evaluation and audit procedures, and provide human review for consequential decisions. Data collection and processing must also comply with applicable privacy and data protection requirements. AI-generated alerts should be treated as indicators for further assessment rather than conclusive evidence of criminal conduct. For legal enforcement purposes, decisions should remain supported by admissible evidence and established procedural safeguards. These measures can help ensure that AI-based fraud prevention strengthens consumer protection without undermining accountability, fairness, or legal certainty.

Cross-border cooperation is essential to address the borderless nature of cybercrime through legal harmonization and stronger law enforcement collaboration. These efforts also support SDG 16 and SDG 9 by strengthening justice, institutions, innovation, and digital infrastructure while promoting a secure and sustainable digital economy.

## 5. MANAGERIAL IMPLICATIONS

The findings of this study highlight the importance of strengthening coordination among policymakers, law enforcement agencies, and digital platform providers to improve legal protection against online fraud in electronic transactions. Law enforcement institutions should enhance investigators' digital forensic expertise, standardize electronic evidence preservation procedures, and improve coordination with financial institutions to facilitate the tracing of fraudulent transactions. Digital platform providers should implement risk-based fraud monitoring systems, establish accessible complaint mechanisms, respond promptly to suspicious activities, and strengthen consumer data protection. Where AI is used for fraud detection, platform managers should ensure adequate human oversight, regular performance evaluations, and transparent procedures to prevent unjustified account restrictions. Furthermore, government institutions and digital service providers should collaborate in developing digital literacy programs to help users recognize phishing, social engineering, and identity impersonation. These measures require clear institutional responsibilities and periodic evaluations to ensure effective implementation, strengthen public trust in electronic transactions, and support the development of a secure and sustainable digital economy in line with SDGs 9 and 16.

## 6. CONCLUSION

Based on the research and discussion conducted, it can be concluded that online fraud in electronic transactions in Indonesia has experienced a significant increase in line with the development of digital technology and high internet usage by the public. Existing regulations, such as the Electronic Information and Transactions Law (UU ITE) and the Criminal Code (KUHP), essentially provide a sufficient legal basis for prosecuting online fraudsters. However, in practice, effective law enforcement still faces various obstacles, particularly in terms of digital evidence, limited human resources with technological competencies, and a lack of supporting infrastructure such as digital forensics laboratories. Furthermore, low digital literacy among the public is also a factor that increases the risk of online fraud. This research also emphasizes that handling online fraud cannot rely solely on a repressive approach through law enforcement but needs to be supported by a comprehensive preventative approach, such as increasing public education and awareness regarding electronic transaction security. Furthermore, regulatory updates are needed that are more adaptive and responsive to technological developments to anticipate the ever-evolving modes of cybercrime. A techno-legal approach that integrates legal aspects with technological innovation, such as the use of AI in fraud detection systems, is also a relevant solution to increase the effectiveness of legal protection.

The findings support several practical recommendations for strengthening online fraud prevention and legal protection. First, policymakers should review the consistency and adequacy of existing regulations, clarify procedures for handling electronic evidence, and establish proportionate accountability requirements for relevant digital service providers. Second, law enforcement institutions should strengthen investigators' digital forensic capabilities, improve evidence-preservation procedures, and enhance coordination with financial institutions and other relevant authorities in tracing fraudulent transactions. Third, digital platform providers should implement risk-based fraud monitoring, accessible reporting mechanisms, timely responses to suspicious activities, and transparent procedures for handling consumer complaints. Where AI-based detection systems are

used, providers should maintain appropriate human oversight, document system performance, and establish safeguards against unjustified account restrictions. Finally, public institutions and platform providers should cooperate in delivering digital literacy programs that help users recognize phishing, impersonation, and other common fraud techniques.

These measures should be supported by clear institutional responsibilities, appropriate procedural safeguards, and periodic evaluation of their implementation. These efforts are crucial not only for providing legal protection to the public but also for supporting the creation of a safe, trustworthy, and sustainable digital ecosystem. The findings contribute to the discussion of cyber law in Indonesia by identifying regulatory and implementation challenges in protecting users of electronic transactions. The practical implications of this study emphasize the need for coordinated action among policymakers, law enforcement institutions, and digital platform providers. Priority measures include improving the implementation of electronic evidence procedures, strengthening digital forensic capacity, establishing accountable fraud-monitoring practices, and expanding public digital literacy. The responsible use of AI should be supported by transparency, human oversight, and appropriate data protection safeguards. Collectively, these measures can contribute to stronger legal institutions under SDG 16 and more resilient digital infrastructure under SDG 9, while improving the practical protection of users in electronic transactions.

## 7. DECLARATIONS

### 7.1. About Authors

Adinda Khairunnisa (AK) https://orcid.org/0009-0001-1809-3087
Adella Ramadhanty Pratiwi (AR) https://orcid.org/0009-0007-9674-2883
Badriyah (BB) https://orcid.org/0009-0009-2620-9666
Dippo Alam (DA) https://orcid.org/0009-0003-5488-4710

### 7.2. Author Contributions

Conceptualization: DA and AK; Methodology: AR and BB; Software: DA and AR; Validation: BB and AK; Formal Analysis: DA and BB; Investigation: BB and AK; Resources: AR; Data Curation: AR and BB; Writing Original Draft Preparation: AK and AR; Writing Review and Editing: BB; Visualization: AR; All authors, AK, AR, BB and DA have read and agreed to the published version of the manuscript.

### 7.3. Data Availability Statement

The data presented in this study are available on request from the corresponding author.

### 7.4. Funding

The authors received no financial support for the research, authorship, and/or publication of this article.

### 7.5. Institutional Review Board Statement

Not applicable.

### 7.6. Informed Consent Statement

Not applicable.

### 7.7. Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## REFERENCES

[1] J. Matheri, "The effect of emerging digital security solutions on fraud risk management in the banking sector in kenya," Ph.D. dissertation, Strathmore University, 2024.
[2] E. M. Ali, F. Dirgantara, and D. Darmawan, "Legal protection of consumers in online transactions: A case study of online fraud in indonesia," *International Journal of Service Science, Management, Engineering, and Technology*, vol. 6, no. 3, pp. 27–38, 2024.

[3] P. M. Preciado Martínez, R. F. Reier Forradellas, L. M. Garay Gallastegui, and S. L. Náñez Alonso, "Comparative analysis of machine learning models for the detection of fraudulent banking transactions," *Cogent Business & Management*, vol. 12, no. 1, p. 2474209, 2025.
[4] D. Marsela, Y. Yudhistira, and B. Fawaid, "Legal protection of consumers in online business: a criminal law perspective in handling fraud and identity theft," *Research Horizon*, vol. 4, no. 3, pp. 99–106, 2024.
[5] A. R. Dzuhriyan, S. I. Permana, and M. K. A. Gufron, "Consumer legal protection in online transactions: Challenges and opportunities in indonesia's digital economy," *Justice Voice*, vol. 3, no. 1, pp. 9–16, 2024.
[6] A. Ahmed, A. Shah, T. Ahmed, S. Yasin, F. E. A. Longa, W. Hussaini, and M. Zubair, "Ai-driven innovations in modern banking: From secure digital transactions to risk management, compliance frameworks, and ai-based atm forecasting systems," *Journal of Management Science Research Review*, vol. 4, no. 3, pp. 1145–1183, 2025.
[7] P. Celestin *et al.*, "How e-commerce law is evolving to address consumer protection and digital marketplace regulations," *Brainae Journal of Business, Sciences and Technology*, 2024.
[8] M. S. Mansyah *et al.*, "Legal protection for victims of fraud in online buying and selling transactions from the perspective of islamic law," *Justice Law Review*, vol. 1, no. 1, pp. 37–65, 2025.
[9] H. Bhanawat and A. Khang, "An examination of data protection and cyber frauds in the financial sector," in *Data-Driven Modelling and Predictive Analytics in Business and Finance*. Auerbach Publications, 2024, pp. 345–360.
[10] M. H. R. C. Sutartono, N. Handayati, M. S. Borman, and D. D. Sidarta, "A legal analysis of fraud in online transactions," *Awang Long Law Review*, vol. 8, no. 4, pp. 1007–1013, 2026.
[11] A. Patel, R. Ranjan, R. K. Kumar, N. Ojha, and A. Patel, "Online dispute resolution mechanism as an effective tool for resolving cross-border consumer disputes in the era of e-commerce," *International Journal of Law and Management*, vol. 68, no. 5, pp. 854–870, 2026.
[12] A. A. Malik, W. Azeem, and M. Asad, "Online shopping, cyber frauds and fraud prevention strategies," *International Journal for Electronic Crime Investigation IJECI*, vol. 8, no. 1, pp. 49–56, 2024.
[13] D. Widijowati, "Enhancing consumer protection in electronic commerce transactions," *Research Horizon*, vol. 3, no. 4, pp. 283–290, 2023.
[14] A. Erica, L. Gantari, O. Qurotulain, A. Nuche, and O. Sy, "Optimizing decision-making: Data analytics applications in management information systems," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 115–122, 2024.
[15] M. Sulaiman, N. H. Pakpahan, and A. R. Putra, "Analysis of the validity and effectiveness of electronic contracts in legal protection of digital transactions in indonesia," *Journal of Social Science Studies*, vol. 3, no. 1, pp. 41–46, 2023.
[16] D. E. Rose, J. Van Der Merwe, and J. Jones, "Digital marketing strategy in enhancing brand awareness and profitability of e-commerce companies," *APTISI Transactions on Management*, vol. 8, no. 2, pp. 160–166, 2024.
[17] N. D. Rizkia, W. A. Hidaya, D. T. Kaemirawati, R. R. Novianty, and Y. Febrianty, "Legal protection of consumers in electronic transactions: Challenges and future prospects," *Journal Equity of Law and Governance*, vol. 4, no. 2, pp. 307–315, 2024.
[18] M. C. Ramadhan, D. K. Dewi, and Y. M. Saragih, "The legal protection in crime of e-commerce transactions," *Jurnal Akta*, vol. 10, no. 1, 2023.
[19] A. Aulia, C. Sukmadilaga, I. Avianti, D. Rosdini, and E. K. Ghani, "The role of esg and digitalization driving sustainable agropreneurship in emerging market," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 51–62, 2026.
[20] R. Rajendran, "Data breach fraudulence and preventive measures in e-commerce platforms," in *Advancements in cybercrime investigation and digital forensics*. Apple Academic Press, 2023, pp. 161–184.
[21] F. Sugianto, E. Sukardi, and T. Michael, "Comparison of legal consumer protection systems in e-commerce transactions to support digital economic growth in indonesia," *Dalat University Journal of Science*, pp. 39–51, 2022.
[22] T. F. Sudarma, F. Festiyed, M. Fadilah, S. Diliarosta, R. Tanjung, and G. Yao, "Effects of mobile learning on critical thinking skills using problem based learning," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 339–350, 2026.
[23] D. M. Ibrahim, Y. Hidayat, and F. F. Wasitaatmadja, "Legal protection of banking customers who are victims of information and electronic transaction crimes," *Jurnal Ilmiah Penegakan Hukum*, vol. 11, no. 1,

pp. 102–120, 2024.
[24] D. Widijowati, "Legal complexity in dealing with cyber crime in indonesia," *Research Horizon*, vol. 2, no. 6, pp. 597–606, 2022.
[25] I. Siswanti, H. A. Riyadh, L. C. Nawangsari, Y. F. Cahaya, and Y. M. Putra, "Integrating green banking into sustainable development strategies for commercial bank efficiency," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 8, no. 1, pp. 351–364, 2026.
[26] H. Singh, "Securing high-stakes digital transactions: a comprehensive study on cybersecurity and data privacy in financial institutions," *Available at SSRN 5267850*, 2023.
[27] E. Syarief, "Security concerns in digital transformation of electronic land registration: Legal protection in cybersecurity laws in indonesia." *International Journal of Cyber Criminology*, vol. 16, no. 2, p. 32, 2022.
[28] D. Apriani, V. T. Devana, A. P. Sagala, P. A. Sunarya, U. Rahardja, and E. P. Harahap, "Security using blockchain-based otp with the concept of iot publish/subscribe," in *Proceedings of the 1st International Conference on Frontier of Digital Technology Towards a Sustainable Society*, vol. 2808, no. 1. AIP Publishing LLC, 2023, p. 050001.
[29] I. Hasan and S. Rizvi, "Ai-driven fraud detection and mitigation in e-commerce transactions," in *Proceedings of Data Analytics and Management: ICDAM 2021, Volume 1*. Springer, 2022, pp. 403–414.
[30] A. Sediana, R. Saputra, R. Hardyansah, D. Darmawan, and R. K. Khayru, "Eradication of digital-based gambling: Dynamics of law enforcement in indonesia," *International Journal of Service Science, Management, Engineering, and Technology*, vol. 8, no. 1, pp. 55–63, 2025.
[31] B. Rawat, A. S. Bist, U. Rahardja, E. P. Harahap, and R. A. D. Septian, "Novel framework to define extended & mixed reality for online learning," in *2022 4th International Conference on Cybernetics and Intelligent System (ICORIS)*. IEEE, 2022, pp. 1–4.
[32] A. M. Ally, "Artificial intelligence (ai) and financial technology (fintech) in tanzania; legal and regulatory issues," *International Journal of Law and Management*, vol. 68, no. 4, pp. 723–741, 2026.
[33] P. A. Aidonojie, O. O. Ikubanni, and N. Okuonghae, "The prospects, challenges, and legal issues of digital banking in nigeria." *Cogito (2066-7094)*, vol. 14, no. 3, p. 186, 2022.
[34] Home Office, "World First Agreement to Tackle Online Fraud," GOV.UK, Nov. 2023, official UK Government news article, published 30 November 2023. [Online]. Available: https://www.gov.uk/government/news/world-first-agreement-to-tackle-online-fraud
[35] H. Herman, N. P. L. Santoso, A. Avandi, N. Septiani, and O. Sy, "Legal governance of artificial intelligence in sustainable digital business ecosystems," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 2, pp. 209–221, 2026.
[36] S. N. Azizah, "The adoption of fintech and the legal protection of the digital assets in islamic/sharia banking linked with economic development: A case of indonesia," *The Journal of World Intellectual Property*, vol. 26, no. 1, pp. 30–40, 2023.
[37] I. Imanuddin, R. D. Anggraeni *et al.*, "Construction of consumer protection against illegal online loan transactions as a means of ius constituendum in indonesia," *Jurnal IUS Kajian Hukum Dan Keadilan*, vol. 11, no. 3, pp. 539–556, 2023.
[38] Q. Aini, S. H. Lase, A. Adiwijaya, F. I. Ningrum, D. A. Prabowo, and T. Green, "Adaptive legal architectures for governing autonomoustechnologies in sustainable digital societies," *Legal Autonomous Web-based Governance (LAW)*, vol. 1, no. 1, pp. 56–67, 2026.
[39] Z. F. Frengky and G. Gunarto, "Legal protection for women in online fraud crimes," *Contrarius Series: Law & Social Justice*, vol. 1, no. 3, pp. 1–8, 2026.
[40] H. Aspan, A. Siregar *et al.*, "Banking secrecy and law enforcement: Challenges in investigating online fraud involving customer data," in *International Conference Epicentrum of Economic Global Framework*, 2026, pp. 2896–2914.
[41] T. B. Purnama, Z. Zulham, and N. Hidayat, "Empowering digital consumers: Legal literacy education for preventing online fraud in indonesia," *Jurnal Abdi Mas Adzkia*, vol. 5, no. 2, p. 28, 2025.
[42] G. Wau and M. L. Panggabean, "Legal protection for victims of cyber-fraud," *TATOHI: Jurnal Ilmu Hukum*, vol. 6, no. 4, pp. 176–180, 2026.
[43] I. N. Topani and A. Yati, "The development of criminal law in addressing digital fraud and cyber offenses," *Berajah Journal*, vol. 5, no. 11, pp. 445–458, 2025.
[44] M. A. Kabir, "A legal analysis on resolving recently growing online business frauds in bangladesh," *Law Reform*, vol. 18, no. 2, pp. 264–281, 2022.