AL RISALAH: Jurnal Ilmu Syariah dan Hukum

VOLUME 26 NO 2, NOVEMBER 2026
P-ISSN: 2252-8334 / E-ISSN: 2550-0309
This work is licensed under a Creative Commons Attribution 4.0 International License
https://doi.org/10.24252/al-risalah.v26i2.70321

Protecting Victims of Digital Triangle Fraud Through A Mitigation Model Within The Jurisdiction of The South Ogan Komering Ulu Resort Police

Zelania[1*], Wendy Melfa[2]
[1]E-mail: zelania937@gmail.com
[2]E-mail: wendymelfa2309@gmail.com
[1,2]Universitas Bandar Lampung, Indonesia
*corresponding author

Article history:
Received in revised form: 10 July 2026
Acceptance date: 31 July 2026
Available online: 22 August 2026

Keywords:
Victims' Constitutional Rights; State's Positive Obligations; Legal Mitigation; Triangular Fraud Scheme; Digital Fraud.

How to Cite:
Zelania, & Melfa, W. (2026). Protecting Victims of Digital Triangle Fraud Through A Mitigation Model Within The Jurisdiction of The South Ogan Komering Ulu Resort Police. Al-Risalah Jurnal Ilmu Syariah Dan Hukum, 26(2). https://doi.org/10.24252/al-risalah.v26i2.70321

License:
Copyright (c) The authors (2026)

This work is licensed under a Creative Commons Attribution 4.0 International License.

Abstract

Digital triangle fraud causes financial, psychological, and social harm because offenders manipulate identities, communications, and transactional relationships between sellers and buyers. This study aimed to analyze victims' constitutional rights, assess the effectiveness of law enforcement and mitigation within the jurisdiction of the South Ogan Komering Ulu Resort Police, and formulate a protection model centered on victim recovery. It combined normative legal research with statutory, conceptual, case, comparative, and empirical approaches. Legal materials were collected through a literature review, while primary data were obtained through observations and interviews with two Criminal Investigation Unit officers and two local residents. The data were analyzed qualitatively through legal substance, legal structure, and legal culture. The findings show that property protection, personal data, personal security, and legal certainty fall within victims' constitutional rights. However, case handling remains suboptimal because the regulatory framework remains sectoral, interagency coordination is limited, digital evidence-tracing capabilities are uneven, and public transaction literacy remains low. The study proposes an integrated model comprising prevention, rapid response, law enforcement, and recovery through education, the interruption of fund flows, electronic evidence preservation, asset tracing, restitution, case updates, and psychological and social support. Protection should be measured by both offender accountability and the fair and comprehensive restoration of victims' rights and well-being.

INTRODUCTION

The migration of human activities into the digital sphere has transformed not only the ways in which people communicate but also transaction patterns and the nature of the associated criminal risks. The ease with which information can be transferred and electronic transactions conducted has enabled fraud to be perpetrated through the manipulation of communications, identities, and trust among users. Akinbowale et al. emphasize that digital fraud is a global phenomenon requiring specific policy responses at both organizational and governmental levels. Their chapter further identifies applicable digital fraud mitigation strategies and provides practical guidance for developing plans capable of withstanding cyber threats.[1] From a victim-centered perspective, Halder argues that victimology cannot exclude consideration of victims' rights.[2] This proposition suggests that an analysis of cyber victimization is inadequate if it focuses exclusively on the offense and the offender without treating victims' rights and needs as integral considerations in legal policymaking. Accordingly, digital fraud should not be framed solely as a cybersecurity issue or an offense against property. It must also be understood as a matter concerning the protection of victims' rights and the state's responsibility to establish a system of protection capable of addressing the distinctive characteristics of crime in the digital sphere.

Fraud in the digital sphere has become increasingly complex because technology has diminished the relevance of territorial boundaries and enabled different stages of an offense to be carried out across multiple locations, through different electronic means, and with the involvement of different parties. Cross identifies jurisdiction as one of the most pressing challenges in addressing digital fraud. Although law enforcement has traditionally been grounded in the principle of territoriality, the Internet has fundamentally altered this framework.[3] Curtis and Oxburgh found that cybercrime victims experienced confusion over whether incidents should be reported through the Action Fraud website or directly to the police, as well as uncertainty regarding what information should be reported and which authority should receive the report.[4] These

---

[1] O. E. Akinbowale, M. P. Mashigo, dan M. F. Zerihun, *Understanding and Mitigating Cyberfraud in Africa* (AVARSITY Books, 2024), p. 301, https://doi.org/10.4102/aosis.2024.BK485

[2] Debarati Halder, *Cyber Victimology: Decoding Cyber-Crime Victimisation* (Routledge, 2022), p. xii, https://doi.org/10.4324/9781315155685

[3] Cassandra Cross, "'Oh We Can't Actually Do Anything About That': The Problematic Nature of Jurisdiction for Online Fraud Victims," *Criminology & Criminal Justice*, 20(3) (2020), p. 358, https://doi.org/10.1177/1748895819835910

[4] Jessica Curtis dan Gavin Oxburgh, "Understanding Cybercrime in 'Real World' Policing and Law Enforcement," *The Police Journal: Theory, Practice and Principles*, 96(4) (2023), p. 581, https://doi.org/10.1177/0032258X221107584

findings demonstrate that uncertainty regarding which incidents should be reported and which institution should receive the report can create confusion for both victims and law enforcement officers responsible for addressing cybercrime. This problem is particularly acute in transaction related digital fraud, where time is critical to limiting losses. Fragmented reporting mechanisms, unclear response channels, and coordination delays may allow funds to be transferred onward and make electronic evidence increasingly difficult to trace before law enforcement can intervene effectively.

One form of transaction related digital fraud requiring particular attention is triangle fraud, a scheme in which an offender positions themselves between two parties with legitimate transactional interests. The scheme operates by isolating communications between the seller and the buyer, presenting each party with a different account of the offender's identity or role in the transaction, and subsequently directing the payment or delivery of goods in accordance with a fabricated narrative. This fragmentation of information may cause one party to transfer funds or release goods on the basis of a mistaken understanding of the transaction, only to discover later that the offender has manipulated both the communications and the transaction. Luong and Ngo emphasize that scam-related fraud is not constrained by geographical or physical boundaries.[5] Technology-facilitated fraud can be perpetrated without physical proximity because offenders can establish communication, gain victims' trust, and manipulate them through digital means. Utami and Purwanti explain that social engineering offenses can be committed through the manipulation of human vulnerabilities.[6]

In other words, fraud does not always succeed because of failures in technological systems; it may instead result from the exploitation of trust, fear, or an individual's tendency to act on information provided by a party perceived as legitimate. Based on these characteristics, this study conceptualizes triangle fraud as a fraudulent configuration in which an offender positions themselves between two legitimate parties, controls the narrative surrounding their identities, separates their communication channels, or directs payment instructions in a manner that causes each party to understand the transaction differently. This fragmentation of information may lead the seller to believe that they are dealing with a legitimate buyer, while the buyer may believe that they are transacting with the owner of the goods or an authorized party. The central

[5] Hai Thanh Luong dan Hong Minh Ngo, "Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective," *Laws*, 13(6) (2024), p. 2, https://doi.org/10.3390/laws13060070.
[6] Putu Devi Yustisia Utami dan Ni Putu Purwanti, "Strengthening Legal Protections Against Social Engineering in Digital Banking: Challenges, Gaps, and Recommendations," *Masalah-Masalah Hukum*, 54(2) (2025), p. 215, https://doi.org/10.14710/mmh.54.2.2025.214-226.

issue, therefore, lies not only in the offender's deception but also in the capacity of the legal system to prevent such manipulation, interrupt it as it occurs, and provide redress for its consequences.

This protective mandate is grounded in the fourth paragraph of the Preamble to the 1945 Constitution of the Republic of Indonesia, which affirms the state's objective of protecting all Indonesians and the entire Indonesian homeland. In the context of an increasingly digital society, this mandate must be interpreted as encompassing the protection of citizens against threats arising from electronic transactions and cyberspace.

The protection of victims of digital fraud has a constitutional dimension. Article 28D(1) of the 1945 Constitution of the Republic of Indonesia affirms that every person is entitled to legal recognition, guarantees, protection, and fair legal certainty, as well as equal treatment before the law.[7] Furthermore, Article 28G(1) affirms every person's right to protection of their person, family, honor, dignity, and property under their control, as well as the right to security and protection from threats that induce fear.[8] The state's responsibility to guarantee these rights is further affirmed in Article 28I(4), which provides that the protection, advancement, enforcement, and fulfillment of human rights are the responsibility of the state, particularly the government.[9] In assessing the development of cyber law, these constitutional provisions may serve as a benchmark for evaluating the extent to which the formulation and development of regulations governing the digital sphere provide the public with protection, a sense of security, and fair legal certainty. This position is consistent with the constitutional basis for the enactment of Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions. Its preambular "In View of" clause expressly refers to "Article 28D(1), Article 28E, Article 28F, Article 28G(1), Article 28I, and Article 28J" of the 1945 Constitution of the Republic of Indonesia.[10]

---

[7] Dewan Perwakilan Rakyat Republik Indonesia. (n.d.). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*. https://www.dpr.go.id/dokumen/jdih/undang-undang-dasar

[8] Mahkamah Konstitusi Republik Indonesia. (2026, May 5). *Pemohon tambah alat bukti penyalahgunaan data pribadi*. https://www.mkri.id/berita/pemohon-tambah-alat-bukti-penyalahgunaan-data-pribadi-24987

[9] Komisi Nasional Hak Asasi Manusia Republik Indonesia. (2021, November 8). *Bergerak bersama demi pemenuhan hak bagi penyandang disabilitas*. https://www.komnasham.go.id/komnas-ham-bergerak-bersama-demi-pemenuhan-hak-bagi-penyandang-disabilitas

[10] Republik Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905. https://jdih.komdigi.go.id/produk_hukum/view/id/884/t/undangundang%2Bnomor%2B1%2Btahun%2B2024

Hermanto et al. argue that legal development often fails to keep pace with evolving legal needs.[11] Technological change can generate legal needs that evolve faster than regulatory frameworks can adapt. Cyber law reform must therefore be comprehensive and capable of anticipating emerging developments. Irawan et al. further caution that law may be reduced to mere written text if institutions lack the capacity to implement it effectively.[12] This means that the enactment of legal norms is insufficient without institutions, technical frameworks, and operational mechanisms capable of implementing and enforcing them. On this basis, the state's responsibility toward victims of digital fraud should not be reduced to the mere existence of criminal provisions and the possibility of punishing offenders. Viewing the issue through the state's positive obligations requires an examination of the legal and institutional measures that have actually been established to protect victims against foreseeable risks, interrupt the escalation of harm, and provide mechanisms for redress once victimization has occurred.

Indonesia has established several legal instruments that form the substantive and procedural legal framework for addressing fraud in electronic transactions. These instruments include Law No. 27 of 2022 on Personal Data Protection,[13] Law No. 1 of 2024 on the Second Amendment to Law No. 11 of 2008 on Electronic Information and Transactions [14], Law of the Republic of Indonesia Number 1 of 2023 on the Criminal Code[15], as amended by Law of the Republic of Indonesia Number 1 of 2026 on Criminal Sanction Adjustment,[16] and Law of the Republic of Indonesia Number 20 of 2025 on the

[11] Bagus Hermanto, A. I. Nur, dan I. Zulfa, "Dinamika Pengaturan Hukum Siber Indonesia: Refleksi Putusan Mahkamah Konstitusi dalam *Ius Constituendum*," *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional*, 14(2) (2025), p. 315, https://doi.org/10.33331/rechtsvinding.v14i2.2045

[12] B. Irawan et al., "Perspective of State Sovereignty in Law Enforcement Related to Cyberlaw Jurisdiction," *LAW REFORM*, 21(1) (2025), p. 124, https://doi.org/10.14710/lr.v21i1.68760

[13] Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

[14] Republik Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

[15] Republik Indonesia. (2023). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842. https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

[16] Republik Indonesia. (2026). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2026 tentang Penyesuaian Pidana*. Lembaran Negara Republik Indonesia Tahun 2026 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 7153. https://peraturan.bpk.go.id/Details/337869/uu-no-1-tahun-2026

Criminal Procedure Code.[17] In their analysis of cybercrime under the new Criminal Code, Suseno et al. argue that the law often fails to keep pace with technological developments.[18] In this context, criminal law reform does not, in itself, immediately prevent cybercrime because technological change may outpace both legal development and the institutional capacity to implement the law. Accordingly, the legal issue to be examined is not merely whether Indonesia has legal provisions that can be invoked against perpetrators of fraud. The more fundamental question is whether these instruments collectively establish an integrated victim-protection chain encompassing prevention, incident interruption and loss containment, electronic evidence preservation, fund tracing, law enforcement, and victim redress. The fragmentation of protective functions across different legal regimes and institutions may create a gap between the normative recognition of rights and the system's capacity to provide victims with timely protection suited to the characteristics of electronic transactions.

At the institutional level, the Indonesian National Police plays a central role in preventing cybercrime, enforcing the law, and providing protection and services to members of the public who become victims of such offenses. Its authority extends beyond conducting inquiries and investigations after an offense has occurred to establishing response mechanisms capable of preventing further losses and preserving electronic evidence. The effectiveness of protection afforded to victims of triangle fraud therefore depends largely on the capacity of the police to receive reports, trace transactions, coordinate with banks and electronic system providers, and take prompt legal action.

This issue assumes a concrete dimension within the jurisdiction of the South Ogan Komering Ulu Resort Police (Polres Ogan Komering Ulu Selatan). The growing use of online transactions among local communities has not always been accompanied by commensurate improvements in digital literacy, early-detection mechanisms, and access to rapid response after funds have been transferred. At the institutional level, the handling of triangle fraud must be assessed in terms of personnel capacity, the availability of facilities for tracing digital evidence, cross-jurisdictional coordination, and the speed of communication with banks and electronic system providers. These circumstances indicate the need to examine the gap between the normative recognition of victims' rights and the effectiveness of victim protection at the local level. The

[17] Republik Indonesia. (2025). *Undang-Undang Republik Indonesia Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. Lembaran Negara Republik Indonesia Tahun 2025 Nomor 188, Tambahan Lembaran Negara Republik Indonesia Nomor 7149. https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025

[18] Sigid Suseno et al., "Cybercrime in the New Criminal Code in Indonesia," *Cogent Social Sciences*, 11(1) (2025), p. 7, https://doi.org/10.1080/23311886.2024.2439543

effectiveness of law enforcement and mitigation efforts in this study is assessed through three elements of the legal system: legal substance, legal structure, and legal culture. Legal substance concerns the adequacy and harmonization of the regulations governing responses to triangle fraud. Legal structure encompasses institutional capacity, authority, supporting facilities, and interagency coordination. Legal culture relates to digital literacy, awareness of the importance of reporting incidents, public vigilance, and the responsiveness of law enforcement authorities to the distinctive characteristics of digital fraud.

Previous studies have examined fraud and cybercrime from diverse perspectives. Cross examines jurisdictional challenges in online fraud, while Curtis and Oxburgh investigate how cybercrime is understood and the practical constraints encountered in policing. Luong and Ngo focus on the transnational nature of fraud, whereas Suseno et al. analyze the legal treatment of cybercrime under Indonesia's new Criminal Code. Within Indonesian scholarship, Irawan et al. focus on state sovereignty and jurisdiction in cyber law; Utami and Purwanti analyze protection against social engineering in digital banking; and Hermanto et al. examine the regulatory dynamics of Indonesian cyber law. Sun and Gu employ a multilayered framework of responsive law enforcement strategies to discuss the protection of victims of cyber fraud.[19] Responses to cyber fraud can be structured across multiple strategic layers and need not depend on a single law enforcement instrument.

Although these studies provide an important foundation, the review of eight journal articles identified no study that simultaneously addresses digital triangle fraud as a matter of victims' constitutional rights and the state's positive obligations while assessing the effectiveness of victim protection through the dimensions of legal substance, legal structure, and legal culture at the resort police level. Previous studies have also not integrated protection before fraud occurs, the rapid containment of further losses, and victim recovery into a single mitigation model tailored to the jurisdiction of the South Ogan Komering Ulu Resort Police. This gap provides a basis for developing a protection model that connects constitutional guarantees, institutional capacity, and the needs of victims of transaction-related cybercrime.

The novelty of this study lies in its integration of constitutional rights guarantees, an assessment of the effectiveness of the legal system at the resort police level, and the reconstruction of a three-stage victim protection model: Protect, Contain, and Restore.

[19] J. Sun dan S. Gu, "Responsive Policing for Cyberfraud Prevention: An Empirical Inquiry into the Regulatory Pyramid to Protect Cyberfraud Victims in China," *Policing and Society*, 36(2) (2025), p. 232, https://doi.org/10.1080/10439463.2025.254823

Protect represents measures undertaken before fraud occurs, particularly public education and transaction risk mitigation. Contain focuses on prompt responses to limit further losses, preserve transaction trails, and secure electronic evidence. Restore places the restoration of victims' rights and redress for their losses at the center of post-fraud protection.

On the basis of this gap, the study addresses three issues: (1) the legal construction of citizens' constitutional rights to property protection and personal security in the context of digital triangle fraud; (2) the effectiveness of law enforcement and triangle fraud mitigation within the jurisdiction of the South Ogan Komering Ulu Resort Police, assessed through legal substance, legal structure, and legal culture; and (3) the reconstruction of an ideal legal protection model to ensure legal certainty and restore the rights of victims of transaction-related cybercrime.Accordingly, this study aims to analyze the constitutional status of citizens' rights to property protection and personal security in the context of digital triangle fraud; evaluate the effectiveness of law enforcement and mitigation efforts within the jurisdiction of the South Ogan Komering Ulu Resort Police through the dimensions of legal substance, legal structure, and legal culture; and reconstruct a legal protection model that integrates measures to protect victims, contain further losses, and restore victims' rights.

METHODS

This study employed normative legal research conducted through library-based research. This methodological design was selected because the study focused on examining the legal construction of victims' constitutional rights, the state's positive obligations, and the interconnections among legal norms governing the mitigation of triangle fraud in digital transactions. Gunardi defines normative legal research as a form of legal inquiry that treats law as a structured system of norms.[20] Nugroho et al. explain that normative legal research is employed to provide a prescriptive justification for a particular legal phenomenon.[21] This study combines an examination of legal norms with an analysis of their implementation in the handling of digital triangle fraud within the jurisdiction of the South Ogan Komering Ulu Resort Police.

---

[20] Gunardi, *Buku Ajar Metode Penelitian Hukum* (Jakarta: Damera Press, 2022), p. 13. https://lintar.untar.ac.id/repository/penelitian/buktipenelitian_10287001_11B030924141233.pdf

[21] Sigit Sapto Nugroho, Anik Tri Haryani, dan Farkhani, *Metodologi Riset Hukum* (Sukoharjo: Oase Pustaka, 2020), p. 36. https://unmermadiun.ac.id/repository_jurnal_penelitian/Sigit%20Sapto%20Nugroho/URL%20Buku%20Ajar/BUKU%20METODOLOGI%20RISET%20HUKUM.pdf

The study employs five research approaches: a statutory approach, a conceptual approach, a case approach, a comparative approach, and an empirical approach. The statutory approach is used to examine and harmonize constitutional norms and legislation governing electronic information and transactions, personal data protection, criminal law, criminal procedure, policing, and victim protection. The conceptual approach is used to conceptualize victims' constitutional rights and the state's positive obligations. The case approach examines the characteristics and patterns of triangle fraud on the basis of documented cases and related information. The comparative approach examines the regulatory frameworks and cyberfraud mitigation mechanisms adopted in other countries. The empirical approach examines the implementation of law enforcement and triangle fraud mitigation within the jurisdiction of the South Ogan Komering Ulu Resort Police.

The study draws on primary legal materials, secondary legal materials, and primary data. Primary legal materials include the 1945 Constitution of the Republic of Indonesia and laws and regulations governing electronic information and transactions, personal data protection, criminal law, criminal procedure, policing, and victim protection. Secondary legal materials are drawn from legal textbooks, literature on legal research methodology, national journals accredited by SINTA, and relevant international journals indexed in Scopus. Scholarly literature published between 2020 and 2026 is prioritized to ensure that the analysis reflects recent developments in cybercrime and victim protection.

Primary data were collected through field research conducted within the jurisdiction of the South Ogan Komering Ulu Resort Police. The research informants comprised two police officers assigned to Unit II of the Criminal Investigation Unit of the South Ogan Komering Ulu Resort Police and two residents of South Ogan Komering Ulu Regency, resulting in a total of four informants. The primary data provided information on mechanisms for receiving and processing reports, obstacles to tracing transactions and electronic evidence, coordination with relevant institutions, levels of public understanding, and the implementation of digital triangle fraud mitigation measures. The field data were used to contextualize the operation of law in practice and were not intended to produce statistical generalizations about the entire population of South Ogan Komering Ulu Regency.

Syarif et al. state that, in normative legal research, legal materials or secondary data are collected through a comprehensive literature review encompassing various

categories of legal sources. [22] Legal materials were collected through a literature review involving the identification, reading, recording, and classification of legislation, books, journal articles, official documents, and other legal sources relevant to the subject matter of the study. Primary data were collected through observation and direct interviews with the informants. The observations focused on the practices and mechanisms used to handle transaction-related cybercrime cases at the research site. The interviews were conducted to obtain information on law enforcement practices, institutional constraints, coordination in case handling, and the protection needs of victims of triangle fraud.

The collected legal materials and field data were processed through three stages: verification, classification, and systematization. Verification was conducted to ensure the completeness and relevance of the materials to the research focus. Classification involved grouping the legal materials and field data according to the legal construction of constitutional rights, the effectiveness of law enforcement, mitigation constraints, and the victim protection model. The materials and field data were then systematically organized according to the research questions, enabling a focused analysis of the relationship between legal norms and their implementation.

A qualitative analysis of a descriptive-prescriptive nature was conducted. The legal materials were analyzed through systematic interpretation, vertical and horizontal legal harmonization, and legal reasoning to explain the legal construction of victims' constitutional rights and the state's positive obligations. Data obtained from observations and interviews were analyzed by categorizing the information according to legal substance, legal structure, and legal culture. Legal substance was used to assess the adequacy and coherence of the regulatory framework; legal structure was used to evaluate institutional capacity, authority, facilities, and coordination; and legal culture was used to assess digital literacy, awareness of the importance of reporting incidents, and the responses of the public and law enforcement authorities to digital fraud. The normative and empirical findings were subsequently integrated to formulate a digital fraud mitigation model comprising measures to Protect victims, Contain further losses, and Restore victims' rights.

[22] Muhammad Syarif et al., *Metode Penelitian Hukum* (Padang: Get Press Indonesia, 2024), p. 112. https://www.researchgate.net/profile/Mohamad-Hidayat-Muhtar/publication/381460823_METODE_PENELITIAN_HUKUM/links/666e76f8de777205a32ff37b/METODE-PENELITIAN-HUKUM.pdf

RESULTS AND DISCUSSION

1. The Legal Construction of Citizens' Constitutional Rights to Property Protection and Personal Security in the Context of Digital Triangle Fraud

Indonesia, like other states, is obliged to adopt national policies that ensure the protection of the public's right to privacy.[23] Hakim argues that banks are legally liable for losses suffered by customers in connection with the use of the services they provide. [24] Nurmansyah et al. argue that enacting robust and comprehensive personal data protection legislation is essential to combating artificial intelligence enabled phishing offenses.[25] Rusli et al. observe, however, that advances in information technology have created new opportunities for criminal activity. These developments have also made it more difficult for law enforcement authorities to investigate and prosecute criminal offenses.[26] Based on the foregoing analysis, victims of triangle fraud in digital transactions have constitutional rights to protection, legal certainty, and redress for the losses they suffer. The fulfillment of these rights requires the state to discharge its positive obligations by strengthening the regulatory framework, enhancing the capacity of law enforcement authorities, and exercising oversight over electronic system operators and banking institutions, thereby ensuring that victim protection extends beyond mere normative recognition.

As demonstrated in the Introduction, triangle fraud in digital transactions cannot be adequately understood merely as conduct by an offender seeking to obtain gain through deception, because the structure of the offense places victims within transactional relationships shaped by the manipulation of identity, communication, and payment information. Dror-Shpoliansky and Shany argue that the rights enjoyed by individuals in the physical world must likewise be protected in cyberspace.[27] The migration of

---

[23] Gunsu Nurmansyah, Rudi Natamiharja, dan Ikhsan Setiawan, "Legal Protection of Personal Data Against Phishing in Indonesia: A Pancasila-Based Approach," *Pancasila and Law Review* 6, no. 1 (2025): 16, https://doi.org/10.25041/plr.v6i1.4138

[24] Lukmanul Hakim, "Pertanggungjawaban Lembaga Perbankan terhadap Pencurian Data Nasabah," *Dialogia Iuridica: Jurnal Hukum Bisnis dan Investasi* 10, no. 1 (2018): 6, https://doi.org/10.28932/di.v10i1.918.

[25] Gunsu Nurmansyah, I Gede Arya Bagus Wiranata, A. Irzal Fardiansyah, dan Stanislav Vladimirov Mladenov, "Preventing AI-Based Phishing Crimes across National Borders through the Reconstruction of Personal Data Protection Laws," *Jurnal Hukum Novelty* 15, no. 2 (2024): 286, https://doi.org/10.26555/jhn.v15i2.27558.

[26] Tami Rusli, Zainab Ompu Jainah, dan Erlina B, "Protection and Legal Security System for Digital Signature Users as Consumers in the Indonesian Legal System," *Pena Justisia: Media Komunikasi dan Kajian Hukum* 23, no. 2 (2024): 8727, https://doi.org/10.31941/pj.v23i2.4751

[27] Doron Dror-Shpoliansky dan Yuval Shany, "It's the End of the (Offline) World as We Know It: From Human Rights to Digital Human Rights A Proposed Typology," *European Journal of International Law*, 32(4) (2021), p. 1253. https://doi.org/10.1093/ejil/chab087

individual activities to the digital sphere does not extinguish the rights inherent in each person. The state therefore remains obliged to protect those rights as both activities and associated risks move online. Shany explains that the obligation to protect may encompass active measures to safeguard individuals against conduct by private actors that impedes the fulfillment and enjoyment of their rights.[28] This proposition demonstrates that the protection of rights cannot always be secured merely by limiting state action. In certain circumstances, it requires active measures to safeguard individuals against conduct by private actors that interferes with the enjoyment of their rights. Under Indonesian law, Kusnadi and Putri emphasize that every citizen has a constitutional right to privacy.[29] An individual's interests in their data and private sphere are linked to constitutional guarantees. Accordingly, the misuse of technology that infringes upon those interests cannot be reduced to a purely technical issue.

The protection of victims of digital triangle fraud is constitutionally grounded in Article 28D(1), Article 28G(1), and Article 28I(4) of the 1945 Constitution of the Republic of Indonesia. Although the Constitution does not expressly use the term "digital rights," funds held in bank accounts, personal data, personal security, and property remain legally protected interests. The use of digital media merely changes the means by which violations occur; it does not diminish the constitutional character of victims' rights. Agus Setyo Wawan explains that citizens possess constitutional rights to the protection of their person, personal security, personal data, and property from threats posed by cybercrime. Such protection not only entitles victims to report criminal offenses but also imposes positive obligations on the state to prevent cybercrime, enforce the law, and ensure redress for victims' losses.[30] Aldi Prayoga explains that the protection of victims of digital triangle fraud is grounded in the 1945 Constitution of the Republic of Indonesia, the Electronic Information and Transactions Law, and the Personal Data Protection Law. Preventive protection is pursued through education and measures designed to prevent suspicious transactions, whereas responsive protection involves receiving reports, conducting inquiries and investigations, and coordinating efforts to freeze bank accounts used by offenders.[31]

---

[28] Yuval Shany, "Digital Rights and the Outer Limits of International Human Rights Law," *German Law Journal*, 24(3) (2023), p. 468. https://doi.org/10.1017/glj.2023.35

[29] Sekaring Ayumeida Kusnadi dan Dwi Wahyuniarti Prabowo Putri, "Perlindungan Hak Privasi dalam Penyalahgunaan Teknologi Deepfake di Indonesia," *Jurnal Rechts Vinding*, 14(2) (2025), p. 201. https://doi.org/10.33331/rechtsvinding.v14i2.2135

[30] Agus Setyo Wawan, Banit II Satreskrim Polres Ogan Komering Ulu Selatan, wawancara oleh penulis pada tahun 20206.

[31] Aldi Prayoga, Banit II Satreskrim Polres Ogan Komering Ulu Selatan, wawancara oleh penulis pada tahun 2026.

Although Kharisma and Diakanza examine personal data in the context of healthcare services, their study provides a relevant illustration by affirming that the protection of patients' personal data constitutes an integral aspect of human rights and must therefore be safeguarded.[32] This analysis demonstrates that personal data can be situated within a human rights protection framework rather than being treated solely as a commodity or an administrative element. Sitabuana et al. emphasize that the law must be capable of providing adequate protection in response to technological developments and the various risks they generate.[33] Technological advancement must therefore be accompanied by the law's capacity to provide effective protection against the risks arising from the use of technology. Hariansah and Qhistina maintain that public authority must be exercised through reasoned decisions that are reviewable and open to contestation or legal challenge.[34]

The active dimension of the state's obligations becomes more apparent when victim protection is linked to the response stage after suspected fraud has come to light. As cited in the OSCE Guidelines, the ECtHR held in *K.U. v. Finland* (2 December 2008, Application No. 2872/02) that states are under positive obligations to conduct effective criminal investigations and enact appropriate legislation.[35] Within the human rights framework, the state's positive obligations may encompass the enactment of adequate legislation and the effective conduct of inquiries or criminal investigations into offenses. The United Nations Convention against Cybercrime calls upon states to provide assistance and protection to victims.[36] Within the evolving framework of international law, responses to cybercrime focus not only on cooperation and law enforcement action against offenders but also on victim assistance and protection as components of the broader framework for

---

[32] Dona Budi Kharisma dan Adinda Diakanza, "Patient Personal Data Protection: Comparing the Health-Care Regulations in Indonesia, Singapore and the European Union," *International Journal of Human Rights in Healthcare*, 17(2) (2024), p. 157. https://doi.org/10.1108/IJHRH-04-2022-0035

[33] Tundjung Herning Sitabuana et al., "Measuring the Effectiveness of Private Electronic System Organizers Regulations in Developing Social Media Equilibrium," *LAW REFORM*, 19(2), p. 347. https://doi.org/10.14710/lr.v19i2.56534

[34] Syamsul Hariansah dan Livia Qhistina, "Toward Algorithmic Due Process: Constitutional Challenges and Human Rights Risks in Indonesia's Digital State," *Jurnal Pembangunan Hukum Indonesia*, 8(1) (2026), p. 30. https://doi.org/10.14710/jphi.v8i1.25-25

[35] OSCE. Organization for Security and Co-operation in Europe, *Ensuring Human Rights Compliance in Cybercrime Investigations: OSCE Training Guide for Criminal Justice Practitioners* (2023), p. 28. https://cdn.osce.org/sites/default/files/f/documents/e/3/554901.pdf

[36] United Nations, *United Nations Convention against Cybercrime* (2024), Article 34. Link teks resmi UNODC: https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

combating crime. The same Article also calls for appropriate procedures for providing compensation and restitution to victims.

Taken together, the foregoing legal norms and scholarly views establish a framework for protecting victims of digital triangle fraud through a systematic interpretation of Article 28D(1), Article 28G(1), Article 28H(4), and Article 28I(4) of the 1945 Constitution of the Republic of Indonesia. These provisions guarantee legal certainty, protection of the person, personal security, property rights, and the state's responsibility to ensure the fulfillment of human rights. Accordingly, funds held in bank accounts, personal data, digital identities, and transactional security constitute interests protected under the Constitution.

Digital media merely alter the manner in which violations are committed; they do not extinguish the rights vested in victims. Triangle fraud results in multiple and overlapping violations because offenders manipulate identities, communications, transactional relationships, and payment information. Consequently, victims suffer not only property losses but also a diminished sense of security and difficulties in obtaining legal certainty. The accounts provided by Agus Setyo Wawan and Aldi Prayoga demonstrate that victims are not merely persons who report criminal offenses but rights holders entitled to preventive and responsive protection, as well as effective remedies. The state must educate the public, prevent suspicious transactions, receive and act upon reports, secure electronic evidence, freeze implicated bank accounts, and trace the flow of funds. Banks and electronic system providers also bear responsibility in accordance with their respective functions, duties of care, and degrees of fault.

Based on this analysis, the legal construction of victims' constitutional rights encompasses protection of the person, personal data and digital identity, personal security, property, and legal certainty. These rights are to be fulfilled through three interrelated stages: prevention before fraud occurs, law enforcement after a report is received, and redress through asset recovery, restitution, compensation, or other mechanisms provided by law. Constitutional protection for victims of digital triangle fraud therefore cannot end with the normative recognition of rights or the mere receipt of a report. It must be realized through prompt action; coordination among law enforcement authorities, banks, and electronic system providers; accountable decision-making; and accessible redress mechanisms.

1. The Effectiveness of Law Enforcement and Triangle Fraud Mitigation within the Jurisdiction of the South Ogan Komering Ulu Resort Police: An Assessment of Legal Substance, Legal Structure, and Legal Culture

Online fraud is one of the many forms of fraud not specifically regulated under Indonesia's Electronic Information and Transactions Law.[37] Hartono and Hapsari argue that extradition and mutual legal assistance should be treated as complementary mechanisms rather than viewed in isolation.[38] Drawing on these two perspectives, the gaps in the legal framework for mitigating triangle fraud in digital transactions lie not only in the absence of provisions specifically addressing this scheme but also in the failure to integrate rules for determining the respective roles of the offender, legitimate seller, and buyer or victim with mechanisms for collecting electronic evidence, tracing the flow of funds, freezing bank accounts, requesting data from digital platforms, recovering victims' losses, and facilitating cross-jurisdictional cooperation. The resulting fragmentation may lead to the misidentification of offenders and victims, delays in securing electronic evidence, and weaknesses in efforts to recover victims' funds. The framework for mitigating triangle fraud should therefore integrate criminal law, electronic transactions law, consumer protection, payment systems, digital platform liability, and mechanisms for cross jurisdictional law enforcement cooperation into a single coordinated response procedure.

Aldi Prayoga explains that triangle fraud involves a legitimate seller, a buyer, and an offender posing as an intermediary. The offender copies photographs of the seller's goods, relists the goods through digital platforms, and provides the seller and the buyer with different information. The buyer is instructed to transfer funds, while the seller is led to believe that the transaction has been arranged by the offender. The complexity of this three-party relationship makes the fraud difficult to detect at the outset of the transaction.[39] Agus Setyo Wawan menyatakan bahwa penjual dan pembeli sama-sama berpotensi menjadi korban, sedangkan pelaku merupakan pihak ketiga yang memanipulasi komunikasi kedua pihak. Penanganan perkara menghadapi kesulitan karena pelaku menggunakan identitas, nomor telepon, rekening, dan akun media sosial yang berbeda. Pelacakan juga membutuhkan pengamanan bukti percakapan, mutasi rekening, identitas akun, dan keterangan para pihak yang terlibat.[40]

---

[37] Dheny Rusdiyanto, Dwi Raka Siwi, Galuh Fitriana, Astria Fitri, dan Zainab Ompu Jainah, "Penipuan Menggunakan Media Internet Berupa Jual-Beli Online," *Iqtishaduna: Jurnal Ilmiah Mahasiswa Jurusan Hukum Ekonomi Syariah* 5, no. 2 (2024): 280, https://doi.org/10.24252/iqtishaduna.vi.43808.

[38] Bambang Hartono dan Recca Ayu Hapsari, "Mutual Legal Assistance pada Pemberantasan Cyber Crime Lintas Yurisdiksi di Indonesia," *SASI* 25, no. 1 (2019): 61, https://doi.org/10.47268/sasi.v25i1.136

[39] Aldi Prayoga, Banit II Satreskrim Polres Ogan Komering Ulu Selatan, wawancara oleh penulis pada tahun 2026.

[40] Agus Setyo Wawan, Banit II Satreskrim Polres Ogan Komering Ulu Selatan, wawancara oleh penulis pada tahun 2026.

Eryadi Yuswanto explains that effective law enforcement against digital fraud requires an understanding of digital transaction patterns, offender characteristics, and the forms of psychological manipulation employed in such schemes. In his view, cooperation among the police, financial institutions, government agencies, and digital platform operators is necessary to prevent similar cases from recurring. These observations indicate that effective mitigation depends not only on the availability of regulations but also on interagency coordination and the public's ability to recognize transaction-related risks.[41] Nugroho and Chandrawulan observe that, despite active efforts by many states to curb cybercrime, the problem persists.[42] Efforts by states to curb cybercrime have not, in themselves, resolved the problem because cybercrime continues to evolve in response to changing technological and social conditions. Matsaung and Masiloane explain that the use of technology to obtain and manipulate information provides fertile ground for cybercriminals.[43] The use of technology to obtain and manipulate information creates opportunities that can be exploited by cybercriminals. In examining the implementation of Indonesia's Electronic Information and Transactions Law, Mahrina et al. conclude that the Law has yet to be implemented effectively.[44]

Whelan et al. identified core organizational challenges that affect the capacity of police cybercrime units to make optimal use of civilian expertise.[45]. Zamroni and Basri emphasize that every stage of the investigation, trial, and post-trial process should incorporate both virtual and in-person support for victims of cybercrime.[46] Support for victims of cybercrime should be provided continuously, beginning at the preliminary inquiry or investigation stage, continuing throughout the trial, and extending beyond the conclusion of judicial proceedings. Ayiliani and Farida explain that, in the context of personal data protection, key responsibilities include performing oversight functions and

[41] Eryadi Yuswanto, masyarakat Kabupaten Ogan Komering Ulu Selatan, wawancara oleh penulis di Ulu Selatan Tahun 2026.
[42] Andri Nugroho dan An An Chandrawulan, "Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries," *Security Journal*, 36 (2023), p. 651. https://doi.org/10.1057/s41284-022-00357-y
[43] Palesa Matsaung dan David T. Masiloane, "The Role of Cyber Intelligence in Policing Cybercrime in South Africa: Insights from Law Enforcement Officers," *African Security Review*, 34(2) (2025), p. 152. https://doi.org/10.1080/10246029.2024.2421225
[44] Mahrina, Joko Sasmito, dan Candra Zonyfar, "The Electronic and Transactions Law (EIT Law) as the First Cybercrime Law in Indonesia: An Introduction and Its Implementation," *Pena Justisia: Media Komunikasi dan Kajian Hukum*, 21(2) (2022), p. 345. https://doi.org/10.31941/pj.v21i2.2680
[45] Chad Whelan et al., "Expertise Integration in Cybercrime Policing: Exploring Civilian Career Lifecycles," *Deviant Behavior*, 46(9) (2025), p. 1213. https://doi.org/10.1080/01639625.2024.2357810
[46] Zamroni dan Basri, "Legal Protection for Victims of Cybercrime as a Form of Transnational Crime," *Jurnal Ius Constituendum*, 9(1) (2024), p. 130. https://doi.org/10.26623/jic.v9i1.8288

facilitating the submission of complaints.[47] Effective personal data protection therefore requires both institutional oversight and an accessible mechanism through which members of the public can lodge complaints.

Recent regulatory developments have strengthened several components of the protection chain. Nevertheless, these sector-specific advances must still be assessed in light of the distinctive characteristics of triangle fraud schemes. Law of the Republic of Indonesia No. 3 of 2026 assigns the Witness and Victim Protection Agency the responsibility for providing protection and ensuring the fulfillment of the rights of witnesses and victims within the scope prescribed by law (Law of the Republic of Indonesia No. 3 of 2026, Article 26).[48] Accordingly, the witness and victim protection regime affirms an institutional mandate to provide protection and ensure the fulfillment of victims' rights in accordance with legally prescribed requirements and mechanisms. In the financial services sector, the Financial Services Authority stipulates that "Financial Services Business Actors (Pelaku Usaha Jasa Keuangan) are required to maintain the confidentiality and security of consumers' data and information" (OJK, 2023, Article 19(1)).[49] Financial Services Business Actors (Pelaku Usaha Jasa Keuangan) are required to safeguard the security and confidentiality of consumer information, while the same regulation further requires them to respond to consumer complaints.

From the perspective of legal substance, the handling of digital triangle fraud is grounded in criminal law, the Electronic Information and Transactions Law, consumer protection legislation, and financial services regulations. However, no provision specifically integrates the identification of the parties involved, the preservation of electronic evidence, the freezing of bank accounts, requests for data from digital platforms, and redress for victims' losses. This fragmentation indicates that the existing legal framework does not yet fully support the rapid and coordinated handling of triangle fraud.

---

[47] Fitria Maulida Ayiliani dan Elfia Farida, "Urgensi Pembentukan Lembaga Pengawas Data Pribadi sebagai Upaya Pelindungan Hukum terhadap Transfer Data Pribadi Lintas Negara," *Jurnal Pembangunan Hukum Indonesia*, 6(3) (2024), p. 431. https://doi.org/10.14710/jphi.v6i3.431-455

[48] Republik Indonesia, *Undang-Undang Republik Indonesia Nomor 3 Tahun 2026 tentang Pelindungan Saksi dan Korban*, Pasal 26. https://peraturan.bpk.go.id/Details/349942/uu-no-3-tahun-2026

[49] Otoritas Jasa Keuangan, *Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*, Pasal 19 ayat (1). https://www.ojk.go.id/id/regulasi/Documents/Pages/Pelindungan-Konsumen-dan-Masyarakat-di-Sektor-Jasa-Keuangan/POJK%2022%20Tahun%202023%20Pelindungan%20Konsumen%20dan%20Masyarakat%20di%20Sektor%20Jasa%20Keuangan.pdf

From the perspective of legal structure, the accounts provided by Aldi Prayoga, Agus Setyo Wawan, and Eryadi Yuswanto indicate that effective case handling depends heavily on investigators' ability to understand transaction patterns and coordinate with banks, government agencies, and digital platform operators. The use of different identities, telephone numbers, bank accounts, and user accounts means that tracing activities require considerable time and access to data held by multiple institutions. Thus, the legal structure within the jurisdiction of the South Ogan Komering Ulu Resort Police has performed its law enforcement functions, but its effectiveness remains constrained by technical capacity and interagency coordination. From the perspective of legal culture, the proliferation of fraud is influenced by offenders' ability to exploit trust and insufficient public vigilance in digital transactions. Individuals who are unfamiliar with triangle fraud may follow payment instructions without verifying the identities and transactional relationships of the parties involved. A legal culture conducive to effective mitigation must therefore be cultivated through public education, routine verification of transaction information, preservation of communication records, and prompt reporting once fraud is detected.

Taken together, these three elements indicate that law enforcement and triangle fraud mitigation within the jurisdiction of the South Ogan Komering Ulu Resort Police cannot yet be regarded as fully effective. The relevant legal substance is available but remains sectoral; the legal structure is functioning but faces constraints in interagency coordination and digital tracing; and public legal culture does not yet provide adequate protection against transactional manipulation. Improving effectiveness requires an integrated case-handling procedure connecting the police, financial institutions, the Witness and Victim Protection Agency (LPSK), government agencies, and digital platform operators. This procedure should be supported by enhanced investigative capacity, expedited data exchange and account freezing, victim assistance, and public education on safe transaction practices. Such measures would ensure that law enforcement focuses not only on taking action against offenders but also on preventing fraud and providing redress for victims' losses.

2. The Reconstruction of an Ideal Legal Protection Model to Ensure Legal Certainty and Restore the Rights of Victims of Transaction-Related Cybercrime

The findings concerning the three dimensions of the state's positive obligations and the gaps in the integration of protective functions provide the foundation for the reconstruction developed in this study. The first component is protection, which operates before losses occur. Whitty explains that cyber fraud causes both financial and

psychological harm to individuals.[50] This indicates that the consequences of cyber fraud extend beyond monetary loss, as victims may also suffer psychological harm. Nataraj-Hansen and Richards found that victims of online fraud experience substantial victim-blaming from family members, friends, professionals, the wider community, and, frequently, themselves.[51] Victims of online fraud are frequently blamed by those around them, professionals, the wider public, and even themselves. Makarim emphasizes that cybersecurity cannot be understood solely as a technical issue.[52] Cybersecurity must therefore be situated within a broader framework that extends beyond the protection of devices and networks, as it also encompasses legal awareness and public behavior.

Agus Setyo Wawan explains that victims of cybercrime may experience not only material losses but also psychological and social harm. Legal protection therefore cannot be limited to punishing offenders. Responses should encompass prevention, the rapid interruption of fund transfers, the provision of case-related information to victims, and redress for their losses. He also describes the Digital Awareness Village Program (Program Desa Sadar Digital), which is used to educate local communities about cybercrime and its prevention.[53] Rizki Saputra explains that victim protection continues to face obstacles related to the preservation of electronic evidence, the technical capacity of law enforcement personnel, and the connection between criminal investigations and remedial mechanisms. In his view, harmonization among the Criminal Code, the Criminal Procedure Code, the Electronic Information and Transactions Law, and technical regulations governing digital forensics is necessary to ensure that case resolution is not reduced to disputes over the applicable legal provisions. Case handling should be directed toward both establishing a robust evidentiary basis and securing redress for victims' losses.[54]

Koning et al. observe that fraud targeting individuals is an increasingly serious problem with substantial consequences for both victims and society. For victims, the

---

[50] Monica T. Whitty, "A Systematic Literature Review of Profiling Victims of Cyber Scams: Setting Up a Framework for Future Research," *Cogent Social Sciences*, 11(1) (2025), p. 1. https://doi.org/10.1080/23311886.2025.2563781

[51] Sofie Nataraj-Hansen dan Kelly Richards, "Why Do Fraud Victims Get Blamed? Lerner's Belief in a Just World and Its Application to Victims of Online Fraud," *Journal of Financial Crime*, 30(3) (2023), p. 828. https://doi.org/10.1108/JFC-02-2022-0037

[52] Edmon Makarim, "Membangun Kesadaran Hukum Masyarakat dalam Meningkatkan Keamanan Siber," *Jurnal Rechts Vinding*, 15(1) (2026), p. 77. https://rechtsvinding.bphn.go.id/ejournal/index.php/jrv/issue/view/53/showToc

[53] Agus Setyo Wawan, Banit II Satreskrim Polres Ogan Komering Ulu Selatan, wawancara oleh penulis pada tahun 2026.

[54] Rizki Saputra, masyarakat Kabupaten Ogan Komering Ulu Selatan, wawancara oleh penulis pada tahun 2026.

police represent an important source of assistance. The police can provide support, while reports filed with them constitute a crucial source of information for broader efforts to combat fraud.[55] Sa'diyah et al. develop an analysis aimed at formulating a victim-oriented model of digital justice.[56] Developments in Indonesian digital law scholarship demonstrate the need to construct a model of justice that places victims' interests at the center of legal analysis.

The European Commission identifies effective communication with victims and the creation of a safe environment in which they can report crimes as integral components of a broader victim-empowerment strategy.[57] Providing redress that recognizes victims' circumstances following the initial response and law enforcement process as an integral measure of effective protection. Ubwarin et al. explain that asset confiscation can perform three principal functions: serving as a punitive measure, operating as a means of prevention, and restoring the interests harmed by the offense.[58] Asset confiscation is therefore relevant not only to punishment and prevention but also to the restoration of victims' interests. The United Nations Interregional Crime and Justice Research Institute emphasizes that mechanisms for reporting cybercrime and accessing justice in cybercrime cases should be victim friendly and empowering.[59] Mechanisms intended for victims should be designed in a victim-friendly manner and should enable them to access justice effectively.

The findings of Whitty and Nataraj-Hansen and Richards indicate that victims of transaction-related cybercrime experience financial, psychological, and social harm. Victim-blaming may exacerbate these harms and discourage victims from reporting the offense. Legal protection therefore cannot focus solely on punishing offenders but must place victims' needs and recovery at its center. The accounts provided by Agus Setyo

---

[55] L. Koning, M. Junger, dan B. Veldkamp, "Reporting Fraud Victimization to the Police: Factors That Affect Whether Victims Report," *Psychology, Crime & Law* (2025), p. 1. https://doi.org/10.1080/1068316X.2025.2468347

[56] Nur Khalimatus Sa'diyah, Retno Budi Kartoningrat, dan Umi Enggarsasi, "Toward a Victim-Oriented Digital Justice Model: Legal Protection for Personal Data Misuse Under the Personal Data Protection Law," *Jurnal Hukum*, 42(2) (2026), p. 284. https://doi.org/10.26532/jh.v42i2.48829

[57] European Commission, *EU Strategy on Victims' Rights (2020–2025)* (2020), Priority 1: "Empowering victims of crime" https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0258

[58] Erwin Ubwarin, Febby Mutiara Nelson, R Narendra Jatna, dan Valentino Dinatra Soplantila, "Reconstructing the Role of Confiscation and Seizure in Realizing the Right to Restitution for Victims of Criminal Acts," *LAW REFORM*, 22(1) (2026), p. 295. https://doi.org/10.14710/lr.v22i1.73378

[59] United Nations Interregional Crime and Justice Research Institute, *Access to Justice in the Digital Age: Empowering Victims of Cybercrime in Africa* (2025), p. viii. https://www.unicri.org/sites/default/files/2025-06/Access-Justice-Digital-Age-Empowering-Victims-Africa_0.pdf

Wawan and Rizki Saputra demonstrate that victim protection remains constrained by difficulties in preserving electronic evidence, the technical capacity of law enforcement personnel, the interruption of fund flows, and the connection between criminal investigations and remedial mechanisms. These conditions demonstrate the need to harmonize the Criminal Code, the Criminal Procedure Code, the Electronic Information and Transactions Law, and technical regulations governing digital forensics to ensure clarity regarding procedures, institutional authority, and victims' rights.

The findings of Koning et al. position the police as the primary gateway to assistance and a crucial source of information in combating fraud. An ideal protection framework therefore requires secure reporting mechanisms, regular communication regarding case progress, the preservation of evidence, and the tracing and seizure of assets. Asset seizure should support not only evidence gathering and offender accountability but also redress for victims' losses. Based on this analysis, the required reconstruction takes the form of an integrated, victim-centered legal protection model. This model comprises four stages: prevention through education; rapid response through reporting and the interruption of fund transfers; law enforcement through evidence preservation and criminal investigation; and recovery through asset recovery, restitution, information regarding case progress, and psychological support.

Legal certainty is thus realized through clear procedures, defined case handling time limits, an explicit allocation of authority, and interagency coordination. The restoration of rights requires returning victims, as far as possible, to their pre-offense position across financial, psychological, and social dimensions. Under this model, the effectiveness of protection is measured not only by the punishment of offenders but also by the extent to which victims' rights are fulfilled and their circumstances restored.

CONCLUSION

The protection of property, personal data, digital identities, personal security, and legal certainty for victims of digital triangle fraud forms an integral part of citizens' constitutional rights. The fulfillment of these rights imposes positive obligations on the state to prevent fraud, receive and act upon reports, preserve electronic evidence, interrupt fund flows, and provide mechanisms for redressing victims' losses.

Law enforcement and triangle fraud mitigation within the jurisdiction of the South Ogan Komering Ulu Resort Police are not yet fully effective. In terms of legal substance, the relevant provisions remain dispersed across several legal regimes. In terms of legal structure, case handling is constrained by technical capacity, data exchange, and

interagency coordination. In terms of legal culture, low transaction literacy and delayed reporting increase the risk and extent of victims' losses.

An ideal protection model must integrate prevention, rapid response, law enforcement, and victim recovery. Its implementation requires education on safe transaction practices, an integrated reporting mechanism, the rapid interruption of fund transfers, electronic evidence preservation, asset tracing and seizure, restitution, regular case updates, and psychological and social support. The effectiveness of protection should be measured not only by the punishment of offenders but also by the restoration of victims' rights and well-being.

REFERENCES

Akinbowale, O. E., Mashigo, M. P., & Zerihun, M. F. (2024). *Understanding and mitigating cyberfraud in Africa*. AVARSITY Books. https://doi.org/10.4102/aosis.2024.BK485

Ayiliani, F. M., & Farida, E. (2024). Urgensi pembentukan lembaga pengawas data pribadi sebagai upaya pelindungan hukum terhadap transfer data pribadi lintas negara. *Jurnal Pembangunan Hukum Indonesia, 6*(3), 431–455. https://doi.org/10.14710/jphi.v6i3.431-455

Cross, C. (2020). 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice, 20*(3), 358–375. https://doi.org/10.1177/1748895819835910

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal: Theory, Practice and Principles, 96*(4), 573–592. https://doi.org/10.1177/0032258X221107584

Dewan Perwakilan Rakyat Republik Indonesia. (n.d.). *Undang-Undang Dasar Negara Republik Indonesia Tahun 1945*. https://www.dpr.go.id/dokumen/jdih/undang-undang-dasar

Dror-Shpoliansky, D., & Shany, Y. (2021). It's the end of the (offline) world as we know it: From human rights to digital human rights—A proposed typology. *European Journal of International Law, 32*(4), 1249–1282. https://doi.org/10.1093/ejil/chab087

European Commission. (2020). *EU strategy on victims' rights (2020–2025)*. EUR-Lex. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52020DC0258

Gunardi. (2022). *Buku ajar metode penelitian hukum*. Damera Press. https://lintar.untar.ac.id/repository/penelitian/buktipenelitian_10287001_11B030924141233.pdf

Halder, D. (2022). *Cyber victimology: Decoding cyber-crime victimisation*. Routledge. https://doi.org/10.4324/9781315155685

Hariansah, S., & Qhistina, L. (2026). Toward algorithmic due process: Constitutional challenges and human rights risks in Indonesia's digital state. *Jurnal Pembangunan Hukum Indonesia, 8*(1), 25–45. https://doi.org/10.14710/jphi.v8i1.25-25

Hermanto, B., Nur, A. I., & Zulfa, I. (2025). Dinamika pengaturan hukum siber Indonesia: Refleksi Putusan Mahkamah Konstitusi dalam *ius constituendum*. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 14*(2), 315–335. https://doi.org/10.33331/rechtsvinding.v14i2.2045

Irawan, B., Mulyanti, D., Budiaman, H., Rahman, Y. M., & Taufiqurrohman, A. (2025). Perspective of state sovereignty in law enforcement related to cyberlaw jurisdiction. *LAW REFORM, 21*(1), 120–134. https://doi.org/10.14710/lr.v21i1.68760

Kharisma, D. B., & Diakanza, A. (2024). Patient personal data protection: Comparing the health-care regulations in Indonesia, Singapore and the European Union. *International Journal of Human Rights in Healthcare, 17*(2), 157–169. https://doi.org/10.1108/IJHRH-04-2022-0035

Komisi Nasional Hak Asasi Manusia Republik Indonesia. (2021, November 8). *Bergerak bersama demi pemenuhan hak bagi penyandang disabilitas*. https://www.komnasham.go.id/komnas-ham-bergerak-bersama-demi-pemenuhan-hak-bagi-penyandang-disabilitas

Koning, L., Junger, M., & Veldkamp, B. (2025). Reporting fraud victimization to the police: Factors that affect whether victims report. *Psychology, Crime & Law*, 1–29. https://doi.org/10.1080/1068316X.2025.2468347

Kusnadi, S. A., & Putri, D. W. S. (2025). Perlindungan hak privasi dalam penyalahgunaan teknologi deepfake di Indonesia. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 14*(2), 195–210. https://doi.org/10.33331/rechtsvinding.v14i2.2135

Luong, H. T., & Ngo, H. M. (2024). Understanding the nature of the transnational scam-related fraud: Challenges and solutions from Vietnam's perspective. *Laws, 13*(6), Article 70. https://doi.org/10.3390/laws13060070

Mahkamah Konstitusi Republik Indonesia. (2026, May 5). *Pemohon tambah alat bukti penyalahgunaan data pribadi*. https://www.mkri.id/berita/pemohon-tambah-alat-bukti-penyalahgunaan-data-pribadi-24987

Mahrina, Sasmito, J., & Zonyfar, C. (2022). The Electronic and Transactions Law (EIT Law) as the first cybercrime law in Indonesia: An introduction and its implementation. *Pena Justisia: Media Komunikasi dan Kajian Hukum, 21*(2), 345–362. https://doi.org/10.31941/pj.v21i2.2680

Makarim, E. (2026). Membangun kesadaran hukum masyarakat dalam meningkatkan keamanan siber. *Jurnal Rechts Vinding: Media Pembinaan Hukum Nasional, 15*(1), 77–

96.
https://rechtsvinding.bphn.go.id/ejournal/index.php/jrv/issue/view/53/showToc

Matsaung, P., & Masiloane, D. T. (2025). The role of cyber intelligence in policing cybercrime in South Africa: Insights from law enforcement officers. *African Security Review, 34*(2), 152–167. https://doi.org/10.1080/10246029.2024.2421225

Nataraj-Hansen, S., & Richards, K. (2023). Why do fraud victims get blamed? Lerner's belief in a just world and its application to victims of online fraud. *Journal of Financial Crime, 30*(3), 828–839. https://doi.org/10.1108/JFC-02-2022-0037

Nugroho, A., & Chandrawulan, A. A. (2023). Research synthesis of cybercrime laws and COVID-19 in Indonesia: Lessons for developed and developing countries. *Security Journal, 36*, 651–670. https://doi.org/10.1057/s41284-022-00357-y

Nugroho, S. S., Haryani, A. T., & Farkhani. (2020). *Metodologi riset hukum*. Oase Pustaka. https://unmermadiun.ac.id/repository_jurnal_penelitian/Sigit%20Sapto%20Nugroho/URL%20Buku%20Ajar/BUKU%20METODOLOGI%20RISET%20HUKUM.pdf

Organization for Security and Co-operation in Europe. (2023). *Ensuring human rights compliance in cybercrime investigations: OSCE training guide for criminal justice practitioners*.
https://cdn.osce.org/sites/default/files/f/documents/e/3/554901.pdf

Otoritas Jasa Keuangan. (2023). *Peraturan Otoritas Jasa Keuangan Republik Indonesia Nomor 22 Tahun 2023 tentang Pelindungan Konsumen dan Masyarakat di Sektor Jasa Keuangan*.https://www.ojk.go.id/id/regulasi/Documents/Pages/Pelindungan-Konsumen-dan-Masyarakat-di-Sektor-Jasa-Keuangan/POJK%2022%20Tahun%202023%20Pelindungan%20Konsumen%20dan%20Masyarakat%20di%20Sektor%20Jasa%20Keuangan.pdf

Prayoga, A. Banit II Satreskrim Polres Ogan Komering Ulu Selatan. Wawancara oleh penulis di Polres Ogan Komering Ulu Selatan, Muaradua, pada tahun 2026.

Republik Indonesia. (2022). *Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi*. Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196, Tambahan Lembaran Negara Republik Indonesia Nomor 6820. https://peraturan.bpk.go.id/Details/229798/uu-no-27-tahun-2022

Republik Indonesia. (2023). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana*. Lembaran Negara Republik Indonesia Tahun 2023 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6842. https://peraturan.bpk.go.id/Details/234935/uu-no-1-tahun-2023

Republik Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun

2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905. https://jdih.komdigi.go.id/produk_hukum/view/id/884/t/undangundang%2Bnomor%2B1%2Btahun%2B2024

Republik Indonesia. (2024). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara Republik Indonesia Tahun 2024 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 6905. https://peraturan.bpk.go.id/Details/274494/uu-no-1-tahun-2024

Republik Indonesia. (2025). *Undang-Undang Republik Indonesia Nomor 20 Tahun 2025 tentang Kitab Undang-Undang Hukum Acara Pidana*. Lembaran Negara Republik Indonesia Tahun 2025 Nomor 188, Tambahan Lembaran Negara Republik Indonesia Nomor 7149. https://peraturan.bpk.go.id/Details/337302/uu-no-20-tahun-2025

Republik Indonesia. (2026). *Undang-Undang Republik Indonesia Nomor 1 Tahun 2026 tentang Penyesuaian Pidana*. Lembaran Negara Republik Indonesia Tahun 2026 Nomor 1, Tambahan Lembaran Negara Republik Indonesia Nomor 7153. https://peraturan.bpk.go.id/Details/337869/uu-no-1-tahun-2026

Republik Indonesia. (2026). *Undang-Undang Republik Indonesia Nomor 3 Tahun 2026 tentang Pelindungan Saksi dan Korban*. Database Peraturan BPK. https://peraturan.bpk.go.id/Details/349942/uu-no-3-tahun-2026

Sa'diyah, N. K., Kartoningrat, R. B., & Enggarsasi, U. (2026). Toward a victim-oriented digital justice model: Legal protection for personal data misuse under the Personal Data Protection Law. *Jurnal Hukum, 42*(2), 284–313. https://doi.org/10.26532/jh.v42i2.48829

Saputra, R. Masyarakat Kabupaten Ogan Komering Ulu Selatan. Wawancara oleh penulis di di Ulu Selatan Tahun 2026.

Shany, Y. (2023). Digital rights and the outer limits of international human rights law. *German Law Journal, 24*(3), 461–472. https://doi.org/10.1017/glj.2023.35

Sitabuana, T. H., Adhari, A., Suryani, L. S., Sanjaya, D., & Amri, I. F. (2024). Measuring the effectiveness of private electronic system organizers regulations in developing social media equilibrium. *LAW REFORM, 19*(2), 344–371. https://doi.org/10.14710/lr.v19i2.56534

Sun, J., & Gu, S. (2025). Responsive policing for cyberfraud prevention: An empirical inquiry into the regulatory pyramid to protect cyberfraud victims in China. *Policing and Society, 36*(2), 232–252. https://doi.org/10.1080/10439463.2025.2548237

Suseno, S., Ramli, A. M., Mayana, R. F., Safiranita, T., & Tiarma, B. A. N. (2025). Cybercrime in the new criminal code in Indonesia. *Cogent Social Sciences, 11*(1), Article 2439543. https://doi.org/10.1080/23311886.2024.2439543

Syarif, M., Ramadhani, R., Graha, M. A. W., Yanuaria, T., Muhtar, M. H., Asmah, N., Syahril, M. A. F., Utami, R. D., Rustan, A., Nasution, H. S., Putera, A., Wilhelmus, K., & Jannah, M. (2024). *Metode penelitian hukum*. Get Press Indonesia. https://www.researchgate.net/profile/Mohamad-Hidayat-Muhtar/publication/381460823_METODE_PENELITIAN_HUKUM/links/666e76f8de777205a32ff37b/METODE-PENELITIAN-HUKUM.pdf

Ubwarin, E., Nelson, F. M., Jatna, R. N., & Soplantila, V. D. (2026). Reconstructing the role of confiscation and seizure in realizing the right to restitution for victims of criminal acts. *LAW REFORM, 22*(1), 294–314. https://doi.org/10.14710/lr.v22i1.73378

United Nations Interregional Crime and Justice Research Institute. (2025). *Access to justice in the digital age: Empowering victims of cybercrime in Africa*. https://www.unicri.org/sites/default/files/2025-06/Access-Justice-Digital-Age-Empowering-Victims-Africa_0.pdf

United Nations. (2024). *United Nations Convention against Cybercrime*. United Nations Office on Drugs and Crime. https://www.unodc.org/unodc/en/cybercrime/convention/text/convention-full-text.html

Utami, P. D. Y., & Purwanti, N. P. (2025). Strengthening legal protections against social engineering in digital banking: Challenges, gaps, and recommendations. *Masalah-Masalah Hukum, 54*(2), 214–226. https://doi.org/10.14710/mmh.54.2.2025.214-226

Wawan, A. S. Banit II Satreskrim Polres Ogan Komering Ulu Selatan. Wawancara oleh penulis di Polres Ogan Komering Ulu Selatan, Muaradua, pada tahu 2026.

Whelan, C., Harkin, D., Martin, J., Miccelli, M., & Villeneuve-Dubuc, M.-P. (2025). Expertise integration in cybercrime policing: Exploring civilian career lifecycles. *Deviant Behavior, 46*(9), 1213–1230. https://doi.org/10.1080/01639625.2024.2357810

Whitty, M. T. (2025). A systematic literature review of profiling victims of cyber scams: Setting up a framework for future research. *Cogent Social Sciences, 11*(1), Article 2563781. https://doi.org/10.1080/23311886.2025.2563781

Yuswanto, E. Masyarakat Kabupaten Ogan Komering Ulu Selatan. Wawancara oleh penulis di Ulu Selatan Tahun 2026.

Zamroni, Z., & Basri, B. (2024). Legal protection for victims of cybercrime as a form of transnational crime. *Jurnal Ius Constituendum, 9*(1), 130–149. https://doi.org/10.26623/jic.v9i1.8288