TATOHI: Jurnal Ilmu Hukum
Volume 6 Issue 4 June, 2026: p. 176 - 180
E-ISSN: 2775-619X
https://fhukum.unpatti.ac.id/jurnal/tatohi/index
TATOHI: Jurnal Ilmu Hukum
doi: 10.47268/tatohi.v6i4.3875

Legal Protection for Victims of Cyber-Fraud

Glorianus Wau[1*], Mompang Lycurgus Panggabean[2]

[1,2] Faculty of Law, Universitas Kristen Indonesia, Jakarta, Indonesia.
: rianwau406@gmail.com
Corresponding Author*

Abstract

Introduction: *Online fraud cases are increasingly prevalent and represent a significant societal challenge. The diversity of these fraudulent activities indicates a lack of public vigilance and a high level of trust in information circulating on social media. This issue necessitates a robust legal framework to effectively safeguard victims within the rapidly evolving digital landscape.*

Purposes of the Research: *he purpose of this study is to examine the legal protection mechanisms for victims of online fraud. It evaluates the limitations of the current legal system, which often prioritizes punishing perpetrators without an adequate focus on victim rehabilitation or the recovery of material losses caused by the various fraudulent activities in Indonesia.*

Methods of the Research: *This research utilizes a normative legal research method, commonly referred to as doctrinal research, focusing on the analysis of online fraud cases. This approach is chosen because current criminal enforcement often lacks optimization in addressing victim needs, emphasizing punitive sanctions rather than comprehensive restitution for the actual harm and trauma suffered.*

Findings of the Research: *The findings reveal that legal protection for victims is categorized into preventive and repressive measures. Repressive protection is essential, particularly through restitution to compensate for material losses. This study also confirms that current countermeasures align with Article 28 and Article 45A of Law Number 1 of 2024 regarding Electronic Information and Transactions.*

Keywords: : Legal Protection; Criminal Offense; Online Fraud.

Submitted: 2026-04-28 *Revised: 2026-06-28* *Accepted: 2026-06-29* *Published: 2026-06-30*

How To Cite: Glorianus Wau, and Mompang Lycurgus Panggabean. "Legal Protection for Victims of Cyber-Fraud." *TATOHI: Jurnal Ilmu Hukum* 6 no. 4 (2026): 176-180. https://doi.org/10.47268/tatohi.v6i4.3875

INTRODUCTION

The regulation of fraud as a criminal offense in Indonesia is explicitly governed under Article 492 of Law Number 1 of 2023 concerning the Criminal Code. Fraud refers to unlawful acts committed with the intent to benefit oneself or others through deception, false identities, or misleading information that causes harm to another party. Along with the rapid development of digital technology, fraudulent practices have increasingly shifted to online platforms, particularly social media and chat-based applications. These schemes often involve impersonation, fake prize notifications, and deceptive financial requests designed to manipulate victims.[1]

Empirically, online fraud cases continue to increase and have become a serious societal issue. This trend reflects the low level of public awareness and vulnerability to misleading information circulating in digital environments. From a legal standpoint, Indonesia has established a regulatory framework through Law Number 1 of 2024 concerning Electronic Information and Transactions, which prohibits the dissemination of false or misleading

[1] Agus Rusmana, "Penipuan Dalam Interaksi Melalui Media Sosial (Kasus Peristiwa Penipuan Melalui Media Sosial Dalam Masyarakat Berjejaring)." *Jurnal Kajian Informasi & Perpustakaan* 3, no. 2 (2015): 187-194. Doi: https://doi.org/10.24198/jkip.v3i2.9994

information that harms consumers in electronic transactions. However, despite the existence of these legal provisions, there remains a gap between normative regulations and their implementation in practice. Law enforcement faces several challenges, including difficulties in identifying perpetrators who use anonymous identities, complexities in digital evidence, and limited institutional capacity in handling cybercrime.[2]

One example is a case involving SMS-based fraud, where perpetrators used illegal Base Transceiver Station (BTS) devices to send phishing messages to thousands of victims simultaneously. In this case, the South Jakarta District Court convicted two foreign nationals and sentenced them to imprisonment and fines, demonstrating the seriousness of such cybercrimes.[3] Based on previous studies, most research has focused primarily on the development of legal regulations. However, this study differs by not only examining legal norms but also analyzing their practical implementation in society. Therefore, this research addresses the following questions: (1) How is legal protection provided to victims of online fraud; (2) How effective are legal policies in addressing online fraud in Indonesia.

METHODS OF THE RESEARCH

The This study employs a normative legal research method, focusing on the analysis of legal norms and doctrines related to online fraud. This method is appropriate because existing regulations tend to emphasize punishment for perpetrators without sufficiently addressing victim recovery and protection.[4] The research adopts three main approaches. First, the conceptual approach is used to examine fundamental legal theories, including legal protection, procedural justice, and substantive justice. Second, the statutory approach involves a comprehensive review of relevant laws and regulations, such as the Criminal Code, the Criminal Procedure Code, the Law on Witness and Victim Protection, the Personal Data Protection Law, and the Electronic Information and Transactions Law. Third, the analytical approach is applied to evaluate the effectiveness of these legal frameworks in practice. Legal materials are collected through document study techniques and analyzed qualitatively to provide prescriptive recommendations for improving legal protection for victims of online fraud.

RESULTS AND DISCUSSION

A. Forms of Legal Protection for Victims of Online Fraud

The rapid development of digital technology has significantly transformed social interactions, particularly through the widespread use of social media as a medium not only for communication but also for economic activities such as online transactions. However, this transformation has also created new opportunities for cybercrime, especially online fraud, which continues to evolve in both form and complexity.[5]

From a legal perspective, online fraud in Indonesia is regulated under both the Criminal Code and Law Number 1 of 2024 concerning Electronic Information and Transactions (Electronic Information and Transactions Act). The Electronic Information and Transactions Act specifically prohibits the dissemination of false or misleading information that causes losses in electronic transactions. However, despite this dual regulatory framework, legal

[2] Lilik Mulyadi, *Hukum Acara Pidana: Normatif, Teoritis, Praktik, dan Permasalahannya* (Bandung: Alumni, 2007).
[3] Aditya Yudi, "Sebar Ribuan SMS Palsu dari BCA dan UOB, 2 WN China Dipenjara 5 Tahun,", https://dandapala.com/article/detail/sebar-ribuan-sms-palsu-dari-bca-dan-uob-2-wn-china-dipenjara-5-tahun/
[4] Peter Mahmud Marzuki, *Penelitian Hukum* (Jakarta: Kencana, 2007), p. 56.
[5] Andi Sofyan and Abdul Azis, *Hukum Acara Pidana Suatu Pengantar* (Jakarta: Kencana, 2014).

protection for victims remains inadequate in practice. One fundamental issue lies in the imbalance between the punishment of perpetrators and the recovery of victims. The current legal framework primarily focuses on criminal sanctions, while mechanisms for restitution and compensation for victims are not effectively implemented.[6] This creates a situation where justice is formally achieved through punishment, but materially fails to restore the victim's losses.

In the context of legal protection theory, as proposed by Philipus M. Hadjon, legal protection can be divided into preventive and repressive forms. Preventive protection aims to prevent violations before they occur, while repressive protection focuses on resolving disputes and providing remedies after harm has occurred.[7] In cases of online fraud, legal protection is predominantly repressive, as actions are taken only after victims have suffered losses.

Victims of online fraud are entitled to restitution, which may include compensation for financial loss, psychological suffering, and other damages directly caused by the crime. However, in practice, obtaining such restitution is often difficult. Victims are frequently required to pursue separate civil litigation to recover their losses, which imposes additional burdens and costs. This raises a critical question: whether the current legal system truly provides comprehensive protection or merely symbolic justice.

Furthermore, the nature of online fraud presents unique challenges. Perpetrators often use anonymous identities, fake accounts, and sophisticated digital manipulation techniques, making detection and prosecution more difficult.[8] This indicates that existing legal instruments, while normatively sufficient, are not yet fully effective in addressing the realities of cybercrime. Therefore, legal protection for victims of online fraud must be strengthened not only through stricter enforcement but also through the development of integrated mechanisms that ensure victim recovery. Without such improvements, the legal system risks failing to deliver substantive justice.

B. Efforts to Overcome Online Fraud Crimes.

This Law enforcement against online fraud, particularly through social media and chat-based platforms, faces significant challenges. One of the primary obstacles is the difficulty in identifying perpetrators, who often use fake identities, anonymous accounts, and even third-party bank accounts to conceal their activities.[9] In addition, limitations in technological resources and human capacity among law enforcement agencies further hinder effective investigation and prosecution of cybercrime cases.[10] This suggests that the issue is not solely regulatory but also institutional and structural.

From a legal standpoint, the imposition of criminal liability for online fraud is based on the fulfillment of both objective and subjective elements. Objectively, the act involves the dissemination of false or misleading information causing harm, while subjectively, it requires intent and unlawful purpose. These elements are regulated under Article 28 of the Electronic Information and Transactions Act as well as Article 492 of the Criminal Code.

---

[6] Ruslan Renggong, *Hukum Pidana Khusus* (Jakarta: Prenada Media Group, 2016).

[7] Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia* (Surabaya: Peradaban, 2007).

[8] Yusran Radyamal Al Miski, Satria Manggala Putra, Muhammad Iqbal Purwanto, Syadza Luthfiyyah., "Eksistensi Tindak Pidana Penipuan (Bedrog) dalam Pasal 378 KUHP di Era Digital," *Journal Equitable* 10, no. 2 (2025): 369-389. Doi: https://doi.org/10.37859/jeq.v10i2.9072

[9] Ihsan M. and Burhayan, *Hambatan dalam Menangani Tindak Pidana Penipuan melalui Media Sosial* (Jakarta: Gramedia, 2022)

[10] Anisa Sahara and Kuswandi, "Penipuan Online sebagai Bentuk Kejahatan Siber dalam Perspektif Kriminologi," *Parlementer* 2, no. 4 (2025): 91-105. Doi: https://doi.org/10.62383/parlementer.v2i4.1425

However, a critical issue arises from the overlapping application of these provisions. In practice, law enforcement officers must carefully determine whether a case falls under general fraud provisions or electronic information regulations. This inconsistency may lead to legal uncertainty and weaken the effectiveness of prosecution. According to Soerjono Soekanto's theory of law enforcement, the effectiveness of legal enforcement depends on five key factors: legal substance, law enforcement officials, facilities and infrastructure, society, and legal culture.[11] Applying this framework to online fraud cases reveals several weaknesses.

First, in terms of legal substance, although regulations exist, they have not fully adapted to the rapid evolution of cybercrime. Second, law enforcement officials often lack sufficient expertise in digital forensics and cyber investigations. Third, technological infrastructure remains limited, particularly in tracing digital evidence. Fourth, public awareness is relatively low, making individuals more vulnerable to fraud. Finally, legal culture, including attitudes toward digital security and reporting crimes, also affects enforcement outcomes. Moreover, empirical studies show that victims do not always receive adequate compensation, even when perpetrators are successfully prosecuted.[12] This highlights a gap between the goals of criminal law - punishment and deterrence - and the needs of victims—recovery and justice.

From a critical perspective, relying solely on criminal sanctions is insufficient to address online fraud. A more comprehensive approach is required, including: a) strengthening victim restitution mechanisms, b) improving digital literacy among the public, c) enhancing technological capabilities of law enforcement, and d) harmonizing legal regulations to avoid overlap and inconsistency. Thus, while current legal efforts are formally aligned with existing regulations, their practical effectiveness remains limited. Without systemic improvements, online fraud will continue to pose a significant threat in the digital era.

CONCLUSION

Legal protection for victims of online fraud in Indonesia formally exists through both the Criminal Code and the Electronic Information and Transactions Law. However, this research demonstrates that such protection remains predominantly punitive in nature, focusing more on sanctioning perpetrators than restoring victims' losses. As a result, there is a significant imbalance between legal certainty and substantive justice. From a theoretical perspective, legal protection should encompass both preventive and repressive measures. In practice, however, protection is largely reactive, with limited mechanisms to ensure restitution or compensation for victims. This indicates that the current legal framework has not fully accommodated the rights and needs of victims in the digital era. Furthermore, the effectiveness of law enforcement is constrained by multiple factors, including the complexity of cybercrime, limitations in digital forensic capabilities, overlapping legal provisions, and low public awareness. These challenges highlight that the issue is not merely regulatory but also institutional and societal. Therefore, strengthening legal protection for victims of online fraud requires a more comprehensive approach. This includes harmonizing relevant regulations, enhancing the capacity of law enforcement agencies, improving digital literacy among the public, and, most importantly, establishing

[11] Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum* (Jakarta: Rajawali Pers, 2008).
[12] Aziz Suharto, "Upaya Perlindungan terhadap Tindak Pidana Penipuan Jual Beli Online," *Iblam Law Review* 4, no. 3 (2024): 23-33. Doi: https://doi.org/10.52249/ilr.v4i3.449

effective mechanisms for victim restitution. Without such reforms, the legal system risks failing to provide meaningful justice in the face of increasingly sophisticated cybercrime.

REFERENCES

Aditya Yudi, "Sebar Ribuan SMS Palsu dari BCA dan UOB, 2 WN China Dipenjara 5 Tahun,", https://dandapala.com/article/detail/sebar-ribuan-sms-palsu-dari-bca-dan-uob-2-wn-china-dipenjara-5-tahun/.

Andi Sofyan and Abdul Azis, *Hukum Acara Pidana Suatu Pengantar*, Jakarta: Kencana, 2014.

Anisa Sahara and Kuswandi, "Penipuan Online sebagai Bentuk Kejahatan Siber dalam Perspektif Kriminologi," *Parlementer* 2, no. 4 (2025): 91-105. Doi: https://doi.org/10.62383/parlementer.v2i4.1425.

Agus Rusmana, "Penipuan Dalam Interaksi Melalui Media Sosial (Kasus Peristiwa Penipuan Melalui Media Sosial Dalam Masyarakat Berjejaring)." *Jurnal Kajian Informasi & Perpustakaan* 3, no. 2 (2015): 187-194. Doi: https://doi.org/10.24198/jkip.v3i2.9994.

Aziz Suharto, "Upaya Perlindungan terhadap Tindak Pidana Penipuan Jual Beli Online," *Iblam Law Review* 4, no. 3 (2024): 23-33. Doi: https://doi.org/10.52249/ilr.v4i3.449.

Ihsan M. and Burhayan, *Hambatan dalam Menangani Tindak Pidana Penipuan melalui Media Sosial*, Jakarta: Gramedia, 2022.

Lilik Mulyadi, *Hukum Acara Pidana: Normatif, Teoritis, Praktik, dan Permasalahannya*, Bandung: Alumni, 2007.

Peter Mahmud Marzuki, *Penelitian Hukum*, Jakarta: Kencana, 2007.

Philipus M. Hadjon, *Perlindungan Hukum Bagi Rakyat di Indonesia*, Surabaya: Peradaban, 2007.

Ruslan Renggong, *Hukum Pidana Khusus*, Jakarta: Prenada Media Group, 2016.

Soerjono Soekanto, *Faktor-Faktor yang Mempengaruhi Penegakan Hukum*, Jakarta: Rajawali Pers, 2008.

Yusran Radyamal Al Miski, Satria Manggala Putra, Muhammad Iqbal Purwanto, Syadza Luthfiyyah., "Eksistensi Tindak Pidana Penipuan (Bedrog) dalam Pasal 378 KUHP di Era Digital," *Journal Equitable* 10, no. 2 (2025): 369-389. Doi: https://doi.org/10.37859/jeq.v10i2.9072.