NOMOI LAW REVIEW

VOLUME 7, ISSUE 1
MAY 2026

ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

LEGAL PROTECTION POLICY FOR VICTIMS OF ONLINE FRAUD IN LANGSA CITY

Azmi Saputra[1], Azmiati Zuliah[2], Andi Maysarah[3]
[123] Universitas Dharmawangsa Medan
e-mail: Azmisaputra87@gmail.com.

ABSTRACT

The rapid advancement of digital technology has precipitated a surge in online fraud, necessitating robust legal mechanisms to protect vulnerable consumers. This research aims to analyze the regulatory framework governing legal protection for fraud victims in Indonesia and evaluate its implementation by law enforcement in Langsa City. Employing an empirical juridical method, this study utilizes data from interviews with police officials and victims to assess the discrepancy between normative laws and empirical reality. The discussion reveals that while the Criminal Code and ITE Law provide a normative foundation, practical application is obstructed by structural barriers, including inadequate digital forensic infrastructure, limited human resource capacity, and the cross-jurisdictional nature of cybercrime. Consequently, the restitution of victims' financial losses remains difficult to achieve despite the use of restorative justice mechanisms. The study concludes that legal protection in Langsa City is currently suboptimal due to these technical and resource limitations. It is suggested that law enforcement agencies enhance their technical capacity and cross-sectoral coordination, while simultaneously promoting public digital literacy to create a more resilient and just digital ecosystem.

Keywords: Legal Protection, Online Fraud, Cybercrime, Victimology, Langsa City.

INTRODUCTION

The fast growth of information and communication technology has changed many parts of human existence, especially in the social and economic areas.[1] This digital transition has changed the way people do business, moving it from traditional ways to electronic platforms. This has made things easier and more efficient for everyone. The internet is used by a lot of people, which lets people do business from anywhere in the world. This has led to a globalized digital economy. This trend is good for the economy and makes it easier for people to do business in the community. But using technology in everyday life makes us more vulnerable, which bad people might take advantage of. The duality of technology is like a

[1] Naeem AllahRakha, "Cybercrime and the Legal and Ethical Challenges of Emerging Technologies," *International Journal of Law and Policy* 2, no. 5 (2024): 28–36.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

double-edged sword: it can be useful, but it can also lead to new types of crime called cybercrime.[2]

Cybercrime includes a lot of different criminal things that people do via computer networks.[3] Online fraud is one of the most common crimes in the digital era.[4] Online fraud is when someone uses electronic means to trick someone else into giving them money or stealing their money. The people who do these things often do them in secret, using advanced techniques that make it harder for the police to find and arrest them.[5] This kind of crime takes advantage of the confidence that comes with online transactions and the fact that people don't have to meet in person.[6] The growing number of these events shows that we need strong legal tools to stop people from doing bad things and protect the public's interests in the digital world.

People who are victims of online fraud usually lose a lot of money and feel bad about themselves, but they generally don't have much power in the criminal justice system. In many places, the law right now is mostly about punishing the criminal instead of making things right for the victim or keeping them safe. This unfairness makes digital customers who depend on electronic systems for their jobs feel unsafe and like things aren't fair. The state has a fundamental duty to protect all citizens, especially from digital crimes, and to ensure security and legal clarity. Legal protection for victims is not only a matter of following the rules; it is a basic human right that guarantees equal treatment under the law and access to justice. Research suggests that victims of digital extortion, for example, often experience a high level of "double victimization".

Satjipto Rahardjo, in his opinion, stated that legal protection is providing protection for human rights that are harmed by others and that protection is given to the community so that they can enjoy all the rights granted by law. Furthermore, Satjipto Rahardjo quoted Fitzgerald's opinion which stated that the law aims to integrate and coordinate various

---

[2] Aleksandra Kuzior et al., "Cybersecurity and Cybercrime: Current Trends and Threats.," *Journal of International Studies (2071-8330)* 17, no. 2 (2024).

[3] Shuai Chen et al., "Exploring the Global Geography of Cybercrime and Its Driving Forces," *Humanities and Social Sciences Communications* 10, no. 1 (2023): 1–10.

[4] Mohammad Ali Bani Younes, "Internet Fraud To Deceive Email By Using Different Technologies," *International Journal of Advanced Research in Computer Science* 10, no. 1 (2019).

[5] Quentin Rossy and Olivier Ribaux, "Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms," *European Journal on Criminal Policy and Research* 26, no. 3 (2020): 335–356.

[6] Katalin Parti, "What Is a Capable Guardian to Older Fraud Victims? Comparison of Younger and Older Victims' Characteristics of Online Fraud Utilizing Routine Activity Theory," *Frontiers in Psychology* 14 (2023): 1118741.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

interests in society because in a traffic of interests, protection of certain interests can be done by limiting various interests on the other side.[7]

Theoretical research on legal protection usually divides it into two types: preventative and repressive. Both are important for fighting online fraud. Preventive legal protection seeks to avert disagreements or criminal activities by instituting explicit laws and standards that govern behavior in the digital domain. Repressive legal protection, on the other hand, works to settle disagreements and punish people who break the law.[8] When these ideas are used in the context of cybercrime, they show that effective protection needs a full approach that includes stringent rules and responsive law enforcement. Legal academics stress that the law's substance must be backed by a legal culture that puts the rights of the victim first and the punishment of the perpetrator second.

Indonesia has passed a number of laws to deal with cybercrime, the most important of which being the Law on Electronic Information and Transactions and the Criminal Code.[9] These laws set the standard for pursuing online fraud and establishing what makes it a crime. The rules say that anybody who willfully transmits misleading information or changes electronic data to make consumers lose money will face criminal charges. The fact that these rules are in place shows that the administration is serious about making the national legal system work better in the digital age. Nonetheless, the efficacy of these restrictions in reality continues to be a topic of persistent scholarly and practical discourse. The difference between what the law says and how it is carried out in the actual world often makes it hard for victims to get true justice.[10]

Victimology is an important way to think about how online fraud works and what people who are targeted by hackers need.[11] This discipline investigates the victim's role in the commission of a crime and their subsequent treatment within the criminal justice system.[12] Theoretical viewpoints in victimology contend that victims of non-violent crimes, such as fraud, are often ignored and seen only as witnesses rather than as individuals

[7] Satjipto Rahardjo, *Ilmu Hukum*, (Bangdung: Citra Aditya Bakti, 2012), hlm. 53.

[8] Loso Judijanto et al., "The Role of Anonymous Data in Promoting Consumer Loyalty on E-Commerce Platforms in Indonesia," *The Eastasouth Journal of Information System and Computer Science* 2, no. 02 (2024): 105–114.

[9] Agus Nugroho and An An Chandrawulan, "Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries," *Security Journal* (2022): 1.

[10] Muhammad Noval, Ramon Nofrial, and Siti Nurkhotijah, "Analisis Yuridis Proses Penyelesaian Tindak Pidana Terhadap Pelaku Penipuan Melalui Pembayaran Elektronik Untuk Mewujudkan Perlindungan Hukum," *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 2, no. 1 (2022): 29–37.

[11] Eileen M Ahlin and Maria João Lobo Antunes, "Theoretical Approaches in Victimology Research," *Victims & Offenders* (Taylor & Francis, 2025).

[12] Zico Junius Fernando, Anis Widyawati, and Kasmanto Rinaldi, "Cyber Victimology and Legal Gaps in Southeast Asia," *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 1–39.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

necessitating targeted rehabilitation and recompense. The complexity of internet fraud proceedings, in which the culprit and victim may reside in disparate jurisdictions, intensifies this marginalization.[13] So, a good legal strategy must include victimological concepts to make sure that restoring the victim's rights is a top priority for law enforcement.

In other places, like Langsa City, it is harder to put legal protections in place for internet fraud victims because of the way the law and society work together. Langsa City is a growing city where more and more people are using the internet and buying things online. As more people use the internet, more reports of online fraud instances have been submitted with local authorities. The real-life situation in Langsa City is a good example of how to look at how national rules are understood and enforced at the local level. The connection between local police and the community is a very important part of making sure that legal protections work. Challenges in implementing cybercrime laws and protecting victims are common in Southeast Asian regions, often due to ineffective cross-border law enforcement cooperation, local political challenges, and a lack of policing capability against cybercrimes.[14] Law enforcement agencies frequently lack specialized training in digital forensic science and cyber-investigative methodologies.

The police in Langsa City are the first line of defense against cybercrime and the main place for victims to go to get justice.[15] Police and other relevant agencies are responsible for taking complaints, looking into them, and collecting digital evidence to create a case against the people who did it. These agencies can only deal with complicated cybercrimes if they have the right technical tools, trained staff, and knowledge of digital forensics. The fact that internet fraud can happen anywhere in the world makes it hard for them to do their jobs. The person who does it may be in a different region or even a different country. The level of public trust in the legal system is directly affected by how quickly the local system responds.

The main question this research seeks to answer is how the regulatory system works in practice and what problems it faces in certain areas. This research examines the regulation of the legal protection policy for victims of internet fraud under current Indonesian law. The research further investigates the implementation of these protective rules by law enforcement authorities in Langsa City. The study aims to pinpoint the particular challenges faced during

[13] Ridwan Arifin, Hartini Atikasari, and Waspiah Waspiah, "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud," *Jurnal Hukum Novelty* 11, no. 2 (2020): 235–246.

[14] Jin Sun, Shiyu Gu, and Ruotong Su, "AI-Empowered Responsive Regulation for Preventing Future Crimes: An Empirical Inquiry into the Regulatory Pyramid to Combat Future Crimes in China and Southeast Asia," *Asian Journal of Criminology* 21, no. 1 (2026): 8.

[15] Rizky Karo Karo and Agnes Sebastian, "Juridical Analysis on the Criminal Act of Online Shop Fraud in Indonesia," *Lentera Hukum* 6 (2019): 1.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

the enforcement process and suggests strategic initiatives to surmount these impediments. This narrative formulation acts as the framework for examining the gap between what the law says should happen and what really happens in law enforcement.

The goals of this study are to give a thorough look at the laws that protect victims of internet fraud and the legal landscape that surrounds it. The main goal is to find and study the specific laws in Indonesia that protect victims of internet fraud. The second goal is to see how well the police in Langsa City are following these rules and how well they are working. The third goal is to find the structural, substantive, and cultural barriers that make it hard to provide the best legal protection. The study aims to develop specific ideas and recommendations that can improve the enforcement system and guarantee superior outcomes for victims.

The importance of this study is that it could add to the body of knowledge in criminal law and cyber law in both theory and practice. Theoretically, the results will enhance the scholarly discourse on legal protection and victimology within the realm of digital crimes. In practice, the results should help law enforcement in Langsa City and legislators come up with better ways to fight online fraud. The study also wants to make people more aware of their rights as digital consumers and the legal options they have. A strong awareness of these issues will help make the digital world safer and fairer for everyone in the long run.

METHOD

This study utilizes an empirical juridical methodology, referred to as socio-legal research, to examine the implementation of legal provisions within a practical framework.[16] This approach often combines normative/doctrinal legal research with empirical field studies.[17] The main sources of data are in-depth interviews with police officers from the Langsa City Police Department and people who have been victims of internet fraud in the area. Secondary data are obtained from primary legal sources, including the Criminal Code, the Electronic Information and Transactions Law, and pertinent scholarly literature.[18] To get qualitative evidence, data collecting methods include observation, structured interviews, and in-depth document studies.[19] The investigation employs a qualitative descriptive

[16] Siti Zahratul Azizah, Zainal Asikin, and Lalu Parman, "Implementation of E-Commerce Crime Law Enforcement at the West Nusa Tenggara Regional Police," *International Journal of Multicultural and Multireligious Understanding* 8, no. 2 (2021): 7.

[17] Sultan Fauzan Hanif and Rully Faradhila Ariani, "Fair Legal Certainty In The Implementation Of International Arbitration Awards (A Socio Legal Study)," *Pattimura Law Journal* 6, no. 2 (2022): 16–37.

[18] Milla Mudzalifah and Pujiyono Pujiyono, "The Politics of Criminal Law in Cybercrime: An Efforts to Combat Information Technology Crimes in Indonesia," *Jurnal Pembaharuan Hukum* 10, no. 1 (2023): 77–89.

[19] Teuku Muttaqin Mansur, Sulaiman Sulaiman, and Hasbi Ali, "Adat Court in Aceh, Indonesia: A Review of Law," *Jurnal Ilmiah Peuradeun* 8, no. 2 (2020): 423–442.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

methodology, wherein collected data is condensed, presented, and validated to ascertain findings about the efficacy of legal protection for fraud victims.

DISCUSSION

Regulatory Framework of Legal Protection for Online Fraud Victims in Indonesia

The legal foundation for protecting victims of online fraud in Indonesia is anchored in a dual-layer framework consisting of the Criminal Code and special legislation governing electronic transactions. The Criminal Code serves as the *lex generalis*, specifically Article 378, which defines fraud as an act of deception used to benefit oneself or others unlawfully.[20] This article provides the fundamental definition of fraud, emphasizing elements such as the use of false names, false capacities, or deceitful words.[21] The application of the Criminal Code in the digital era, however, required expansion to cover intangible electronic mediums. Indonesia addressed this need by enacting Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016.

The Law on Electronic Information and Transactions functions as the *lex specialis*, providing detailed provisions for crimes committed via the internet.[22] Article 28 paragraph of the ITE Law specifically prohibits the intentional and unauthorized dissemination of false and misleading news resulting in consumer losses in electronic transactions. This provision directly addresses the nature of online fraud, where perpetrators often manipulate data, use fake identities, or create fake online storefronts to deceive victims, by prohibiting the spread of false and misleading information in electronic transactions.[23] The existence of this specific article allows prosecutors to charge offenders with stricter penalties compared to the general fraud provisions in the Criminal Code. The regulation acknowledges the unique characteristics of cybercrime, such as speed, anonymity, and the potential for widespread damage.

Legal protection for victims is not solely defined by the criminalization of the offender but also by the mechanisms available for restitution and rights recovery. The Indonesian criminal justice system has traditionally focused on retributive justice, often leaving the victim with little recourse for financial recovery unless they pursue a separate

[20] Didi Sukardi et al., "Solving Cyber Crime in Online Buying and Selling in Cirebon City in Review of ITE Law and Islamic Law," *Al-Mustashfa: Jurnal Penelitian Hukum Ekonomi Syariah* 8, no. 2 (2023): 237–250.

[21] Yaris Adhial Fajrin et al., "Illegal Electronic Investments in Trade Robot Missions According to the Criminal Law in Indonesia," *KnE Social Sciences* (2024): 384–393.

[22] Farris Nur Sanjaya, "Application of Law Information and Electronic Transactions in Crime Investigation of Online Gambling," *Jurnal Daulat Hukum* 1, no. 2 (2018): 537–542.

[23] Juneidi Hasibuan and Syafrudin Syam, "A Legal Analysis on Online Fraud Using Fake Identity," *Indonesian Journal of Multidisciplinary Science* 2, no. 10 (2023): 3308–3317.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

civil lawsuit.[24] The Law on Witness and Victim Protection (Law No. 31 of 2014) attempts to bridge this gap by offering protection and assistance to victims of crimes.[25] This law mandates that victims are entitled to obtain medical assistance and psychosocial rehabilitation, and in certain cases, to apply for restitution from the perpetrator.[26] The integration of these protective measures into the handling of online fraud cases is vital for achieving comprehensive justice.

The concept of legal protection also encompasses procedural rights during the investigation and trial processes. The Criminal Procedure Code regulates the status of the victim primarily as a witness who assists the state in proving the guilt of the defendant.[27] This procedural stance often limits the victim's active participation in the judicial process, relegating them to a passive role. Recent legal developments and circulars from the Chief of Police have begun to encourage a more restorative justice approach, particularly for crimes involving property loss like fraud.[28] Restorative justice mechanisms allow for mediation between the victim and the perpetrator, focusing on the return of assets rather than solely on incarceration.[29]

Academic analysis of these regulations suggests that while the normative framework is robust in defining the crime, it remains deficient in enforcing automatic compensation mechanisms. The burden of proof to claim damages often falls heavily on the victim, who must navigate complex bureaucratic procedures. The separation of criminal and civil liability in the Indonesian legal system means that a criminal conviction does not automatically result in the return of stolen funds. This dichotomy presents a significant hurdle for victims of online fraud, who are primarily interested in the recovery of their financial losses. Legal experts argue for an integrated system where criminal restitution can be enforced directly within the criminal sentencing phase.

---

[24] Peter Jeremiah Setiawan and Hansel Ardison, "Criminal Victimization on Large-Scale Investment Scam in Indonesia," *Veritas et Justitia* 7, no. 1 (2021): 1–30.

[25] Angkasa Angkasa et al., "Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim," *Lex Scientia Law Review* 7, no. 1 (2023): 119–178.

[26] Mahfud Mahfud, "Crime Victims Protection in Indonesia: An Analysis of the Recent Victim Protection Acts," *Kertha Patrika* 42 (2020): 115–131.

[27] Oheo K Haris and Ali Risky, "Victim's Involvement Model in Children Legal Process Based on Law No. 11/2012 on Children Criminal Justice System," *Yuridika* 34, no. 1 (2019): 105.

[28] Arnott Ferels and Hery Firmansyah, "Analisis Rechtsvacuum Dalam Hukum Acara Pidana Indonesia: Penerapan Penghentian Penuntutan Berdasarkan Keadilan Restoratif," *Syntax Literate; Jurnal Ilmiah Indonesia* 8, no. 11 (2023): 6215–6228.

[29] Emmanuel Arianto Waluyo Adi, "Penal Mediation as the Concept of Restorative Justice in the Draft Criminal Procedure Code," *Lex Scientia Law Review* 5, no. 1 (2021): 139–164.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

The dynamic nature of technology necessitates that these regulations be interpreted flexibly by the judiciary to cover evolving modes of fraud.[30] Perpetrators constantly develop new techniques, such as phishing, social engineering, and marketplace manipulation, which may not be explicitly described in older statutory texts.[31] The inherent flexibility in applying the ITE Law allows for its adaptation to new technological advancements and novel fraud schemes. This judicial adaptability ensures that victims of novel fraud schemes are not left without legal remedy due to technicalities. The responsiveness of the regulatory framework is tested by its ability to adapt to these new variations of cybercrime.

The ultimate goal of these regulations is to create a deterrent effect for criminals and a safety net for the public. The harmonization between the Criminal Code, the ITE Law, and the Witness and Victim Protection Law creates a comprehensive, albeit complex, web of protection. The state has provided the necessary tools to combat online fraud, but the efficacy of these tools depends heavily on the consistency of their application. A robust regulatory framework serves as the starting point, but it must be complemented by proactive enforcement and a judiciary sensitive to the losses suffered by victims. The current laws provide a solid foundation, yet continuous amendments and policy adjustments are required to close existing loopholes regarding victim compensation.

Implementation of Legal Protection by Law Enforcement in Langsa City

The execution of legal protection policies for online fraud victims in Langsa City is primarily the responsibility of the Resort Police of Langsa. The police serve as the initial gatekeepers of the criminal justice system, receiving reports and determining the course of legal action. The standard operating procedure usually begins with the victim filing a formal report at the Integrated Police Service Center. The police in Indonesia, including local units, have established specific desks or units to handle cyber-related crimes, reflecting an awareness of the growing trend of digital offenses.[32] This initial intake process is critical, as it determines whether the case is classified as a criminal act worthy of investigation or a civil dispute.

[30] Wojciech Filipkowski and Lorenzo Picarella, "Criminalizing Cybercrimes: Italian and Polish Experiences," *Bialostockie Studia Prawnicze* 26 (2021): 171.

[31] Vishnu Laxman et al., "Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review," *Journal of Digital Economy* 3 (2024): 205–222.

[32] Mochammad Fahlevi et al., "Cybercrime Business Digital in Indonesia," in *E3S Web of Conferences*, vol. 125 (EDP Sciences, 2019), 21001.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

The investigation process involves the collection of digital evidence, which presents unique challenges compared to physical crimes.[33] Investigators in Langsa City are tasked with tracing IP addresses, bank account transaction histories, and chat logs to identify the perpetrator. The police often collaborate with bank authorities to freeze accounts used by fraudsters, a crucial step in preventing the dissipation of stolen assets. This collaboration, however, requires adherence to strict banking secrecy laws, which can be a significant obstacle, as banks are often restricted from providing customer identity without consent or a formal legal process. The speed at which law enforcement can act often determines the likelihood of asset recovery for the victim, and delays can hinder this process.

Law enforcement officials in Langsa City increasingly utilize a restorative justice approach in handling online fraud cases where the loss amount is relatively small or where the parties are willing to settle. The police, empowered by discretion under Indonesian law, facilitate mediation sessions between the victim and the perpetrator, provided the perpetrator is identified and apprehended. The priority in these sessions is often the return of the victim's funds, which is frequently the primary desire of victims of online fraud.[34] This approach offers immediate relief and can be a practical form of legal protection, avoiding the lengthy and costly trial process. The implementation of this discretion relies heavily on the judgment and integrity of the individual investigators.[35]

Based on the results of interviews with investigators from the Langsa Police Criminal Investigation Unit (initial A), it is known that in handling online fraud cases, officers normatively use Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law, but in practice they face obstacles because the perpetrators are often outside the Langsa area or even outside the province so that the process of tracking accounts and collecting digital evidence takes a long time; this condition shows that legal norms formally work in the aspect of criminalization, but their effectiveness is empirically limited due to technical and jurisdictional obstacles. This situation is in line with research findings regarding the implementation of digital forensics which confirms that electronic evidence has been recognized as valid evidence, but still faces challenges of competence and infrastructure, [36]

[33] Isdian Anggraeny et al., "The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department," *KnE Social Sciences* (2022): 349–359.

[34] Silvony Kakoe, Masruchin Ruba'i, and Abdul Madjid, "Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi Sebagai Pidana Tambahan," *Jurnal Legalitas* 13, no. 02 (2020): 118–131.

[35] Yaris Adhial Fajrin and Ach Faisol Triwijaya, "The Concept Of Penal Mediation For Defamation Delict In The Indonesia Ite Law As A Manifestation Of Restorative Justice," *Yustisia Jurnal Hukum* 9, no. 3 (2020): 363–385.

[36] Irvan Saputra and Andi Maysarah, "Implementasi Digital Forensics Dalam Pembuktian Tindak Pidana Cyber Crime Di Pengadilan Negeri Medan," *Warta Dharmawangsa* 20, no. 1 (2026): 416–430.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

and something similar also occurs in Langsa where the limitations of local digital forensic devices cause dependence on the Regional Police. From the victim's perspective, one of the victims (initials S) stated that even though a report had been made, the loss could not be recovered because the perpetrator's account was empty and the victim did not know the compensation mechanism, which shows that normatively the victim does have the right to protection and recovery as emphasized in the study of victim protection in criminal law, [37] but in practice in Langsa City the victim is still positioned more as a witness than as a subject whose economic rights are prioritized. Thus, through an empirical juridical approach, a gap is seen between das sollen and das sein, where Article 28 paragraph (1) of the ITE Law is effective in ensnaring the perpetrator but has not been effective in guaranteeing the recovery of the victim's losses, restorative justice is only applied in a limited way in certain cases, and structural obstacles (limited forensic laboratories and cross-regional coordination), substantive (lack of automatic restitution mechanisms), and cultural (low digital literacy and victims' reluctance to report) cause the repressive function of the law to be more dominant than the protective function for victims.

The protection of the victim's psychological well-being during the investigation is another aspect of implementation that varies in practice. The police are required to treat victims with dignity and provide them with updates regarding the progress of their case.[38] The reality in Langsa City shows that while officers are generally cooperative, the sheer volume of cases can lead to communication gaps. Victims often feel left in the dark regarding the status of their reports, contributing to a sense of helplessness. While the police administration strives to improve transparency through digital notification systems, full implementation remains a work in progress.

Inter-agency cooperation is a cornerstone of the implementation strategy in Langsa City, involving the police, the prosecutor's office, and local communication offices. The complexity of cybercrime often requires expert testimony to prove the elements of the offense under the ITE Law.[39] Investigators occasionally face difficulties in securing these experts promptly, which can prolong the investigation phase, and law enforcement agencies are not always keen on digital forensic examinations. Effective coordination between the police and the prosecutor's office is vital to ensure that case files are legally sound and robust enough

[37] Abraham Abraham, Kusbianto Kusbianto, and Azmiati Zuliah, "Kedudukan Hukum Tindak Pidana Perdagangan Orang Dalam Memberikan Perlindungan Terhadap Korban Di Indonesia," *Law Jurnal* 6, no. 1 (2025): 118–124.

[38] Petrus Reinhard Golosea, "A Legal Analysis of Crime Victim Protection in Indonesia," *Russian Law Journal* 11, no. 3S (2023): 402–409.

[39] Indriati Amarini et al., "The Legal Position of Digital Forensic Experts in the Settlement of Information Technology Crime Cases," *Lex Scientia Law Review* 8, no. 1 (2024): 355–384.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

for trial, although this coordination process can sometimes be delayed. This synergy ensures that the legal protection provided during the investigation carries through to the prosecution stage.

The geographical jurisdiction of the Langsa City Police often clashes with the borderless nature of online fraud. Many perpetrators operating against victims in Langsa are located in other regions or even internationally.[40] The implementation of legal protection thus involves coordination with police units in other jurisdictions. This cross-jurisdictional cooperation is frequently slow and bureaucratic, hampering the ability of local police to make arrests due to factors like differing legal systems and difficulties in extradition. The limitations of territorial authority act as a significant constraint on the implementation of repressive protection measures against transnational cybercrime.

The assessment of implementation effectiveness reveals a mixed record, with successful prosecutions coexisting with unresolved cases. The police in Langsa City, like other Indonesian police units, have achieved successes in combating cybercrime, including cracking down on local syndicates. However, a significant number of cases, particularly those involving sophisticated anonymous perpetrators, remain in the investigation stage for extended periods due to the anonymity of criminals and challenges in tracing them. The commitment of the law enforcement apparatus is evident, but their effectiveness is modulated by resource availability and procedural hurdles. These challenges include a shortage of skilled personnel, fragmented inter-agency coordination, and a lack of adequate facilities and infrastructure for cybercrime investigations. The implementation of protection is a continuous effort that requires constant adaptation to the shifting tactics of cybercriminals, who continually exploit new technologies and adapt their methods.[41]

Obstacles and Efforts to Overcome Challenges in Langsa City

The implementation of legal protection for online fraud victims in Langsa City is hindered by a variety of structural and substantial obstacles. The most prominent internal obstacle is the limited availability of advanced digital forensics infrastructure within the Langsa Police Department.[42] Cybercrime investigations require sophisticated hardware and

[40] Gomgom Siregar and Sarman Sinaga, "The Law Globalization in Cybercrime Prevention," *International Journal of Law Reconstruction* 5, no. 2 (2021): 211–227.

[41] Desta Lesmana, Mochammmad Afifuddin, and Agus Adriyanto, "Challenges and Cybersecurity Threats in Digital Economic Transformation," *International Journal Of Humanities Education and Social Sciences (IJHESS)* 2, no. 6 (2023).

[42] Handar Subhandi Bakhtiar et al., "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia," *Egyptian Journal of Forensic Sciences* 15, no. 1 (2025): 39.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

software to retrieve and analyze electronic evidence that is admissible in court. The reliance on provincial-level laboratories for detailed forensic analysis creates bottlenecks that delay case resolution. This technological gap significantly hampers the speed and efficiency of investigations, often allowing perpetrators time to cover their tracks.

Human resource capacity constitutes another significant internal hurdle for law enforcement in the region.[43] The rapid evolution of cybercrime techniques outpaces the training frequency of local police officers. Investigators in Langsa City may possess general knowledge of criminal law but sometimes lack the specialized technical expertise required to navigate complex digital fraud schemes. The shortage of certified cybercrime investigators means that the workload is distributed among a small number of personnel, leading to burnout and slower case turnover. This skill gap affects the quality of evidence collection and the ability to build watertight cases against tech-savvy criminals.

External obstacles are largely driven by the behavior and location of the perpetrators and the community itself. The anonymity provided by the internet allows fraudsters to easily mask their identities and operate from jurisdictions far removed from Langsa City.[44] Pursuing a suspect located in a different province requires substantial operational funds and administrative coordination, which are often limited. The usage of "mule accounts" (rekening penampung) bought from third parties further complicates the tracing of funds, breaking the link between the bank account and the actual criminal.[45]

The legal culture and awareness of the society in Langsa City also present challenges to effective legal protection. Many victims of online fraud do not report the crime due to skepticism about the legal outcome, embarrassment, or a lack of trust in the justice system. When reports are filed, victims often fail to preserve crucial evidence such as chat logs or transfer receipts, having deleted them in frustration, or they lack the knowledge to do so effectively.[46] The lack of digital literacy among the public makes them easy targets for social engineering and hampers the investigative process. This lack of awareness creates a cycle where crimes go unreported, and perpetrators remain emboldened.

Efforts to overcome these obstacles must begin with the strengthening of institutional capacity at the local level. The Langsa City Police need to advocate for increased budget

[43] Muhammad Indra Muliansyah and Irma Rachman, "Transformation of Law Enforcement in Indonesia: Between Hope and Reality," *Estudiante Law Journal* 7, no. 2 (2025): 493–510.

[44] You Zhou et al., "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality," *Asian Journal of Criminology* 19, no. 3 (2024): 419–439.

[45] Muhammad Subtain Raza, Qi Zhan, and Sana Rubab, "Role of Money Mules in Money Laundering and Financial Crimes a Discussion through Case Studies," *Journal of Financial Crime* 27, no. 3 (2020): 911–931.

[46] Misita Anwar et al., "Cyber Capacity Building in Indonesia: A Study of Cyber Security Awareness in Rural Community," in *International Conference on Asian Digital Libraries* (Springer, 2024), 250–259.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

allocations specifically for cybercrime investigation tools and training. Sending officers to specialized training programs on digital forensics and cyber investigation techniques is a critical investment. Improving the technical competence of investigators will reduce reliance on external experts and accelerate the evidence-processing timeline. Upgrading the technological infrastructure at the precinct level is a necessary step to match the sophistication of modern criminals.

Enhancing public education and digital literacy is a vital strategy for overcoming external obstacles. Law enforcement agencies, in collaboration with the local government and educational institutions, should conduct regular socialization programs regarding safe online transaction practices. Educating the public on how to preserve digital evidence and the importance of reporting crimes immediately can significantly improve investigation success rates. Preventive campaigns that highlight common fraud modus operandi can serve as a first line of defense, reducing the number of potential victims.

Strengthening cross-sectoral and cross-jurisdictional cooperation is the final key effort required to improve legal protection. The Langsa Police should establish faster, more direct channels of communication with the banking sector and telecommunication providers to expedite the freezing of accounts and tracking of numbers.[47] At the national level, streamlining the bureaucratic procedures for cross-regional investigations will allow for more agile pursuit of offenders. Building a stronger network with cybercrime units in major cities will facilitate the apprehension of syndicates targeting victims in regions like Langsa. These combined efforts aim to create a more responsive and effective legal protection system.

CONCLUSION

Based on the results of empirical legal research on legal protection for victims of online fraud in Langsa City, it can be concluded that normatively the regulatory framework through Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law has provided an adequate legal basis for ensnaring perpetrators, and theoretically guarantees the rights of protection and recovery of victims as emphasized in the study of victim protection in criminal law. However, in its implementation in Langsa City, this legal protection has not been running optimally because even though law enforcement officers have used electronic evidence-based evidentiary mechanisms in accordance with digital forensics principles, its effectiveness is still hampered by limited digital forensic infrastructure, cross-regional jurisdictional constraints, and the lack of integration of restitution mechanisms in judicial practice, so that protection is more oriented towards punishing perpetrators than recovering

[47] Jin Sun and Shiyu Gu, "Responsive Policing for Cyberfraud Prevention: An Empirical Inquiry into the Regulatory Pyramid to Protect Cyberfraud Victims in China," *Policing and Society* (2025): 1–21.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

victims' losses. therefore, it is necessary to strengthen the technical capacity of officers, standardize procedures for handling electronic evidence, optimize cross-regional coordination, and integrate policies that are more oriented towards recovering victims' rights.

REFERENCES

Adi, Emmanuel Arianto Waluyo. "Penal Mediation as the Concept of Restorative Justice in the Draft Criminal Procedure Code." *Lex Scientia Law Review* 5, no. 1 (2021): 139–164.

Ahlin, Eileen M, and Maria João Lobo Antunes. "Theoretical Approaches in Victimology Research." *Victims & Offenders*. Taylor & Francis, 2025.

AllahRakha, Naeem. "Cybercrime and the Legal and Ethical Challenges of Emerging Technologies." *International Journal of Law and Policy* 2, no. 5 (2024): 28–36.

Amarini, Indriati, Rizky Aulia Cahyadri, Maulida Ayu Fitriani, and Noorfajri Ismail. "The Legal Position of Digital Forensic Experts in the Settlement of Information Technology Crime Cases." *Lex Scientia Law Review* 8, no. 1 (2024): 355–384.

Anggraeny, Isdian, Cindy Monique, Yohana Puspitasari Wardoyo, and Aprilia Bhirini Slamet. "The Urgency of Establishing Guidelines for Handling Cybercrime Cases in the Indonesian National Police Department." *KnE Social Sciences* (2022): 349–359.

Angkasa, Angkasa, Filep Wamafma, Ogiandhafiz Juanda, and Bhanu Prakash Nunna. "Illegal Online Loans in Indonesia: Between the Law Enforcement and Protection of Victim." *Lex Scientia Law Review* 7, no. 1 (2023): 119–178.

Anwar, Misita, Devi Karolita, Intan Sari Areni, Tyanita Puti Marindah Wardhani, Faisal Syafar, and Irfan Syamsuddin. "Cyber Capacity Building in Indonesia: A Study of Cyber Security Awareness in Rural Community." In *International Conference on Asian Digital Libraries*, 250–259. Springer, 2024.

Arifin, Ridwan, Hartini Atikasari, and Waspiah Waspiah. "The Intersection of Criminal Law, Technology and Business Commercial Law on Carding as Cyber Fraud." *Jurnal Hukum Novelty* 11, no. 2 (2020): 235–246.

Azizah, Siti Zahratul, Zainal Asikin, and Lalu Parman. "Implementation of E-Commerce Crime Law Enforcement at the West Nusa Tenggara Regional Police." *International Journal of Multicultural and Multireligious Understanding* 8, no. 2 (2021): 7.

Bakhtiar, Handar Subhandi, Amir Ilyas, Abdul Kholiq, and Handina Sulastrina Bakhtiar. "The Utilisation of Scientific Crime Investigation Methods and Forensic Evidence in the Criminal Investigation Process in Indonesia." *Egyptian Journal of Forensic Sciences* 15, no. 1 (2025): 39.

Chen, Shuai, Mengmeng Hao, Fangyu Ding, Dong Jiang, Jiping Dong, Shize Zhang, Qiquan Guo, and Chundong Gao. "Exploring the Global Geography of Cybercrime and Its Driving Forces." *Humanities and Social Sciences Communications* 10, no. 1 (2023): 1–10.

Fahlevi, Mochammad, Mohamad Saparudin, Sari Maemunah, Dasih Irma, and Muhamad Ekhsan. "Cybercrime Business Digital in Indonesia." In *E3S Web of Conferences*, 125:21001. EDP Sciences, 2019.

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

Fajrin, Yaris Adhial, Fadjar Ramdhani Setyawan, Said Noor Prasetyo, Radhityas Kharisma Nuryasinta, Syariful Alam, Kukuh Dwi Kurniawan, and Wahyudi Kurniawan. "Illegal Electronic Investments in Trade Robot Missions According to the Criminal Law in Indonesia." *KnE Social Sciences* (2024): 384–393.

Fajrin, Yaris Adhial, and Ach Faisol Triwijaya. "The Concept Of Penal Mediation For Defamation Delict In The Indonesia Ite Law As A Manifestation Of Restorative Justice." *Yustisia Jurnal Hukum* 9, no. 3 (2020): 363–385.

Ferels, Arnott, and Hery Firmansyah. "Analisis Rechtsvacuum Dalam Hukum Acara Pidana Indonesia: Penerapan Penghentian Penuntutan Berdasarkan Keadilan Restoratif." *Syntax Literate; Jurnal Ilmiah Indonesia* 8, no. 11 (2023): 6215–6228.

Fernando, Zico Junius, Anis Widyawati, and Kasmanto Rinaldi. "Cyber Victimology and Legal Gaps in Southeast Asia." *International Law Discourse in Southeast Asia* 4, no. 1 (2025): 1–39.

Filipkowski, Wojciech, and Lorenzo Picarella. "Criminalizing Cybercrimes: Italian and Polish Experiences." *Bialostockie Studia Prawnicze* 26 (2021): 171.

Golosea, Petrus Reinhard. "A Legal Analysis of Crime Victim Protection in Indonesia." *Russian Law Journal* 11, no. 3S (2023): 402–409.

Hanif, Sultan Fauzan, and Rully Faradhila Ariani. "Fair Legal Certainty In The Implementation Of International Arbitration Awards (A Socio Legal Study)." *Pattimura Law Journal* 6, no. 2 (2022): 16–37.

Haris, Oheo K, and Ali Risky. "Victim's Involvement Model in Children Legal Process Based on Law No. 11/2012 on Children Criminal Justice System." *Yuridika* 34, no. 1 (2019): 105.

Hasibuan, Juneidi, and Syafrudin Syam. "A Legal Analysis on Online Fraud Using Fake Identity." *Indonesian Journal of Multidisciplinary Science* 2, no. 10 (2023): 3308–3317.

Judijanto, Loso, Sayed Achmady, I Wayan Karang Utama, Femmy Effendy, and Puji Chairu Sabila. "The Role of Anonymous Data in Promoting Consumer Loyalty on E-Commerce Platforms in Indonesia." *The Eastasouth Journal of Information System and Computer Science* 2, no. 02 (2024): 105–114.

Kakoe, Silvony, Masruchin Ruba'i, and Abdul Madjid. "Perlindungan Hukum Korban Penipuan Transaksi Jual Beli Online Melalui Ganti Rugi Sebagai Pidana Tambahan." *Jurnal Legalitas* 13, no. 02 (2020): 118–131.

Karo, Rizky Karo, and Agnes Sebastian. "Juridical Analysis on the Criminal Act of Online Shop Fraud in Indonesia." *Lentera Hukum* 6 (2019): 1.

Kuzior, Aleksandra, Inna Tiutiunyk, Anetta Zielińska, and Roland Kelemen. "Cybersecurity and Cybercrime: Current Trends and Threats." *Journal of International Studies (2071-8330)* 17, no. 2 (2024).

Laxman, Vishnu, Nithyashree Ramesh, Senthil Kumar Jaya Prakash, and Ravi Aluvala. "Emerging Threats in Digital Payment and Financial Crime: A Bibliometric Review." *Journal of Digital Economy* 3 (2024): 205–222.

Lesmana, Desta, Mochammmad Afifuddin, and Agus Adriyanto. "Challenges and

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

Cybersecurity Threats in Digital Economic Transformation." *International Journal Of Humanities Education and Social Sciences (IJHESS)* 2, no. 6 (2023).

Mahfud, Mahfud. "Crime Victims Protection in Indonesia: An Analysis of the Recent Victim Protection Acts." *Kertha Patrika* 42 (2020): 115–131.

Mansur, Teuku Muttaqin, Sulaiman Sulaiman, and Hasbi Ali. "Adat Court in Aceh, Indonesia: A Review of Law." *Jurnal Ilmiah Peuradeun* 8, no. 2 (2020): 423–442.

Mudzalifah, Milla, and Pujiyono Pujiyono. "The Politics of Criminal Law in Cybercrime: An Efforts to Combat Information Technology Crimes in Indonesia." *Jurnal Pembaharuan Hukum* 10, no. 1 (2023): 77–89.

Muliansyah, Muhammad Indra, and Irma Rachman. "Transformation of Law Enforcement in Indonesia: Between Hope and Reality." *Estudiante Law Journal* 7, no. 2 (2025): 493–510.

Noval, Muhammad, Ramon Nofrial, and Siti Nurkhotijah. "Analisis Yuridis Proses Penyelesaian Tindak Pidana Terhadap Pelaku Penipuan Melalui Pembayaran Elektronik Untuk Mewujudkan Perlindungan Hukum." *Jurnal Ilmiah Hukum Dan Hak Asasi Manusia* 2, no. 1 (2022): 29–37.

Nugroho, Agus, and An An Chandrawulan. "Research Synthesis of Cybercrime Laws and COVID-19 in Indonesia: Lessons for Developed and Developing Countries." *Security Journal* (2022): 1.

Parti, Katalin. "What Is a Capable Guardian to Older Fraud Victims? Comparison of Younger and Older Victims' Characteristics of Online Fraud Utilizing Routine Activity Theory." *Frontiers in Psychology* 14 (2023): 1118741.

Rahardjo Satjipto, *Ilmu Hukum*, Bangdung: Citra Aditya Bakti, 2012.

Raza, Muhammad Subtain, Qi Zhan, and Sana Rubab. "Role of Money Mules in Money Laundering and Financial Crimes a Discussion through Case Studies." *Journal of Financial Crime* 27, no. 3 (2020): 911–931.

Rossy, Quentin, and Olivier Ribaux. "Orienting the Development of Crime Analysis Processes in Police Organisations Covering the Digital Transformations of Fraud Mechanisms." *European Journal on Criminal Policy and Research* 26, no. 3 (2020): 335–356.

Sanjaya, Farris Nur. "Application of Law Information and Electronic Transactions in Crime Investigation of Online Gambling." *Jurnal Daulat Hukum* 1, no. 2 (2018): 537–542.

Setiawan, Peter Jeremiah, and Hansel Ardison. "Criminal Victimization on Large-Scale Investment Scam in Indonesia." *Veritas et Justitia* 7, no. 1 (2021): 1–30.

Siregar, Gomgom, and Sarman Sinaga. "The Law Globalization in Cybercrime Prevention." *International Journal of Law Reconstruction* 5, no. 2 (2021): 211–227.

Sukardi, Didi, Farha Bayu Nugraha, Ubaidillah Ubaidillah, Abdul Fatakh, Leliya Leliya, and Muhammad Fadel Arrizky. "Solving Cyber Crime in Online Buying and Selling in Cirebon City in Review of ITE Law and Islamic Law." *Al-Mustashfa: Jurnal Penelitian Hukum Ekonomi Syariah* 8, no. 2 (2023): 237–250.

Sun, Jin, and Shiyu Gu. "Responsive Policing for Cyberfraud Prevention: An Empirical

NOMOI LAW REVIEW
VOLUME 7, ISSUE 1
MAY 2026
ISSN (Print) 2723-3413 - ISSN (Online) 2722-3663
DOI: https://doi.org/10.30596/nomoi.v7i1.31050

Inquiry into the Regulatory Pyramid to Protect Cyberfraud Victims in China." *Policing and Society* (2025): 1–21.

Sun, Jin, Shiyu Gu, and Ruotong Su. "AI-Empowered Responsive Regulation for Preventing Future Crimes: An Empirical Inquiry into the Regulatory Pyramid to Combat Future Crimes in China and Southeast Asia." *Asian Journal of Criminology* 21, no. 1 (2026): 8.

Younes, Mohammad Ali Bani. "Internet Fraud To Deceive Email By Using Different Technologies." *International Journal of Advanced Research in Computer Science* 10, no. 1 (2019).

Zhou, You, Milind Tiwari, Ausma Bernot, and Kai Lin. "Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality." *Asian Journal of Criminology* 19, no. 3 (2024): 419–439.