Jurnal Legalitas
Volume 19 Issue 1, 2026
P-ISSN: 1979-5955, E-ISSN: 2746-6094
Faculty of Law, Universitas Negeri Gorontalo

Social Media-Based Triangular Fraud and Cyber Law Enforcement: An Indonesian Transnational Digital Crime Perspective

Erica Natalia Rombe[1], Amir Ilyas[2]

[1] *Faculty of law, Hasanuddin University, Indonesia. E-mail: ericanatalia879@gmail.com*
[2] *Faculty of law, Hasanuddin University, Indonesia. E-mail: amir_fh_unhas@yahoo.com*

Article Info

Article History
Received: May 18, 2025;
Reviewed: Sep 14, 2025;
Accepted: Apr 30,2026.

Keywords:

Cyber Law Enforcement; Triangular Fraud; Social Media Fraud; Digital Evidence; Online Transaction.

Corresponding Author:
Name : Erica Natalia Rombe
Email: *ericanatalia879@gmail.com*

How to cite *[Chicago Manual of Style 17th edition (full note)]:*

Erica Natalia Rombe, Amir Ilyas "Social Media-Based Triangular Fraud and Cyber Law Enforcement: An Indonesian Transnational Digital Crime Perspective" *Jurnal Legalitas* 19, No. 1 (2026): 62–81

DOI :
10.33756/jelta.v19i1.31687

Abstract

This study examines law enforcement against triangular fraud on social media and the strategies adopted by the police to address this emerging form of cyber-enabled deception. The urgency of this research lies in the increasing use of social media as a platform for fraudulent transactions, where perpetrators manipulate buyers and sellers through a three-party scheme that obscures criminal responsibility and complicates evidence tracing. Unlike conventional online fraud, triangular fraud involves layered communication, false representation, and indirect transaction patterns, making it more difficult for law enforcement agencies to investigate and prosecute effectively. This study employs an empirical legal research method, using qualitative analysis presented descriptively based on field data and law enforcement practice. The findings reveal that law enforcement against triangular fraud remains suboptimal due to limited human resources, insufficient cybercrime expertise among police officers, and inadequate facilities for tracking digital evidence. The Makassar Police have responded through three main strategies: pre-emptive efforts by conducting public outreach and legal education, preventive efforts through investigation and inquiry, and repressive efforts aimed at raising public awareness and encouraging caution in online transactions. The novelty of this study lies in its specific focus on triangular fraud as a distinct modus operandi within social media-based cybercrime. Its contribution is to highlight the need for stronger cyber-investigative capacity, improved digital evidence infrastructure, and preventive public education as part of a more adaptive law enforcement model for digital fraud cases. Practical prevention measures include verifying sellers through video calls, documenting communication, and confirming live location before transaction.

1. Introduction

Indonesia is one of the countries that is inseparable from the development of technology and information in the current digital era.[1] Quick advance within the field of data and communication innovation currently shows exceptional advance. This will be seen from different segments of life that have utilized the nearness of innovation, which has had a noteworthy affect on human life in different perspectives. Propels in information and communication innovation have made it simpler for individuals to get and spread data to numerous individuals.[2] Communication can presently be done effectively without being hampered by separate, space, and time. With the continued development of communication and internet technology. People are also encouraged to follow every change that occurs in order to stay relevant and not be left behind.

With the existence of the internet, it has become a driver for changes in the structure of people's living needs, both in economic and social aspects. In addition, the development of information technology also has another impact, namely the emergence of new types of crimes that we often call *cybercrime. Cybercrime* is defined as a general crime committed by individuals or groups who master the use of information technology, such as the internet and mobile phones.[3] As a country that upholds the law, Indonesia has an obligation to protect every citizen from actions that can be detrimental, especially actions that can disrupt the order of life in society and the nation and state. One form of action in question is crime that occurs on social media, which is commonly known as cybercrime.

Various crimes occur in cyberspace, and these cases are clearly detrimental and have negative impacts. This kind of cybercrime is not only limited to Indonesia, but covers the entire world. Some of these crimes occur due to the increasing use of *e-mail, e-banking, and e-commerce* in Indonesia. The increasing cases of cybercrime, especially in Indonesia, have attracted the attention of the government to immediately implement laws that can be used to catch perpetrators of cybercrime.[4]

Cybercrime can be defined as an unlawful act committed using the internet based on sophisticated computer and telecommunications technology. The Prevention of Crime and The Treatment Of Offlenderes in Havana, Cuba in 1999 and in Vienna, Austria in 2000, mentioned 2 known terms:

a. Cybercrime in the narrow sense is called computer crime, which is illegal/violating behavior that is directly and/or data processed by a computer;
b. Cybercrime in the broad sense is called computer related crime, which is illegal/violating behavior related to computer systems and networks.[5]

---

[1] Lucky Nugroho, "The Role of Information for Consumers in the Digital Era (Indonesia Case)," *Artvin Çoruh Üniversitesi Uluslararası Sosyal Bilimler Dergisi* 7, no. 2 (2021): 49–59.
[2] Mark Graham and William H. Dutton, *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives* (Oxford University Press, 2019),
[3] Noor Rahmad, "Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online," *Jurnal Hukum Ekonomi Syariah* 3, no. 2 (2019): 103–17.
[4] Miftakhur Rokhman Habibi and Isnatul Liviani, "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia," *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426.
[5] D. R. Yurizal, *Penegakan Hukum Tindak Pidana Cyber Crime Di Indonesia*, vol. 1 (Media Nusa Creative (MNC Publishing), 2018)

Therefore, every country including Indonesia, has rules or laws that regulate the use of the internet as a limitation or benchmark to prevent misuse and criminal acts in internet access. The ITE Law equates all criminal sanctions, as long as it is carried out using electronic means.[6] In Indonesia, such regulations already exist, namely the ITE Law which handles cybercrime cases. Legal development should be in line with the development of society. Thus, when society changes or develops, the law must also adapt to regulate all changes that occur in an orderly manner amidst the growth of modern society.

The many online shopping sites available today, making this transaction the main choice for a number of buyers. Although online shopping offers various advantages, it also has risks that can cause concern for market players. This risk arises because the interaction between sellers and buyers is carried out without direct meetings, but through the internet (cyberspace) which is often difficult to track.[7] As a result, the most common risks are related to security issues, fraud, and dissatisfaction.

Criminal acts are a term that contains a basic understanding in legal science, as a term formed with awareness in giving certain characteristics to criminal law events. Criminal acts have an abstract meaning from concrete events in the field of criminal law, so that criminal acts must be given a scientific meaning and clearly determined to be able to isolated it from the terms utilized regular in community life.[8] One form of crime that utilizes online media is fraud. Online fraud is a form of crime that utilizes technology in every action.[9] The basic principle of online fraud is the same as conventional fraud, where every case of fraud always involves a victim who suffers a loss and another party who gains illegal benefits. The main difference between online fraud and conventional fraud lies in the use of electronic systems, such as telecommunications devices and computer internet.

Recently, cybercrime that is currently rampant is fraud with a triangular fraud mode where the perpetrator in carrying out his action deceives the victim as a prospective buyer with the lure of cheap prices.[10] In this fraud mode, the perpetrator will pretend to be a buyer on an online buying and selling platform and ask the seller for a complete photo of the item being sold, which is then used by the perpetrator to find a buyer (victim), after which the perpetrator will pretend to be a seller by using photos of other people's goods (from the original seller).

After the perpetrator gets a victim (buyer), then the perpetrator will bring together the two victims (the original seller and the buyer) at a location that has been determined by the perpetrator, or commonly called the Cash On Delivery (COD) system. In this case, the perpetrator will argue that the person who wants to do COD is the perpetrator's relative, friend, or family, and tells the buyer not to say

---

[6] Amir Ilyas, "Perwujudan Prinsip Legalitas Dalam Tindak Pidana Penghinaan," *Amanna Gappa*, 2017, 79–104.
[7] D. N. Parajuli and Newal Chaudhary, "Rights and Duties of Buyers and Sellers Online in Cyberspace," *Issue 6 Int'l JL Mgmt. & Human.* 7 (2024): 567.
[8] Ilyas, "Perwujudan Prinsip Legalitas Dalam Tindak Pidana Penghinaan."
[9] Kanahaiya Lal Ambashtha and Pramod Kumar, "Online Fraud," in *Financial Crimes*, ed. Chander Mohan Gupta (Springer International Publishing, 2023), https://doi.org/10.1007/978-3-031-29090-9_7.
[10] A. K. Saxena, *Black Money and Economic Crimes* (KK Publications, 2021)

anything to the original seller. After the two victims meet, the perpetrator will ask the buyer to transfer the money to the perpetrator's personal account.

In such a situation, legal action will be applied based on Article 378 of the Criminal Code and Article 28 paragraph (1) of Law No. 19 of 2016 which is an amendment to Law No. 11 of 2008 concerning ITE. The crime of fraud is regulated in Article 378 of the Criminal Code (KUHP). This act is considered a crime and is subject to legal sanctions. In addition, in accordance with Article 28 paragraph (1) of the Electronic Information and Transactions Law (UU ITE), the spread of false and misleading news that is detrimental to consumers can also be subject to sanctions. Therefore, perpetrators of fraud can be charged based on both provisions, namely Article 378 of the Criminal Code and Article 28 paragraph (1) of the ITE Law simultaneously.

For that reason, the birth of Law on Information and Electronic Transactions Number 11 of 2008 has been regulated in such a way as to provide protection to the public in various activities that use the internet, both to obtain information and to make transactions and also to guarantee security, justice, and legal certainty for users and organizers of information technology. It is expected to be able to resolve the problem of cyber crime, although it is realized that there are still many shortcomings and improvements are needed to become a national law related to cyber law problems in Indonesia.

Ardi's research shows that the effectiveness of law enforcement against online fraud in the Wajo Police jurisdiction has not been implemented optimally.[11] Because at the enforcement stage there is still a lack of human resources who master technology, apart from that, in terms of budget it is still lacking when carrying out investigations and inquiries, inadequate facilities and infrastructure, and people who are reluctant to report their cases to the police due to prestige or shame.

Law enforcement efforts to overcome and minimize online fraud in the Wajo Police jurisdiction, the efforts made by the Wajo Police are preventive efforts, these efforts are made to ward off or eliminate criminogenic factors at the earliest possible stage. Preventive efforts, these efforts are the second effort after preemptive, these efforts are made to eliminate the opportunity to commit crimes or online fraud. Repressive efforts, these efforts are taken to prosecute the perpetrators according to their actions and to provide firm action so that the perpetrators are aware that their actions are actions that are contrary to the rules of the law, these repressive enforcement efforts are efforts to provide legal certainty regarding online fraud perpetrators.

Law enforcement against criminal acts of fraud with banking methods through social media is not optimal, while the inhibiting factors are not optimal, namely legal factors, law enforcement factors, community factors, and cultural factors.[12] Of the 4 factors, the most influential on the objectives of law enforcement is the law enforcement factor (readiness of officers) with the lack of ability and skills of law

[11] Aswar Ardi et al., "Law Enforcement Against Online Fraud Crimes: A Case Study at Police District Area of Wajo," *Jurnal Hukum Volkgeist* 6, no. 1 (2021): 51–57.
[12] Apriyas Munik et al., "Law Enforcement And Factors Background To The Crime Of Fraud In Online Selling Transactions In Indonesia," *IJOSPOL-International Journal of Social, Policy and Law* 4, no. 2 (2023): 47–55.

enforcement officers in the field of technology and information or cyber, is one of the inhibiting factors for the police in resolving cases in the cyber field.

The prevention efforts carried out by the Regional Police and Resort Police are preventive efforts to carry out socialization actions to the public about the importance of maintaining the confidentiality of PINs, OTP codes, online transaction security and the police, especially in the cyber sector, patrol an application or website that is considered to be able to cause criminal acts, then it will be reported to the Ministry of Communication and Information. While repressive efforts, namely after a report is received, the police conduct an investigation and investigation but in the process experience difficulties. Banks do not want to provide data required by the police because of the consumer protection law which requires banks to continue to provide protection to protect their customer data.

Cybercrime and fraud conducted through social media constitute a transnational problem, as such activities can be carried out across national borders, involving perpetrators, victims, platforms, and payment systems located in different jurisdictions.[13] At the international level, the General Data Protection Regulation (GDPR) in the European Union governs the protection of personal data, the security of data processing, and the accountability of data controllers within the digital ecosystem. Meanwhile, the United States relies on the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, which addresses unauthorized access, abuse of computer systems, and computer-based fraud. These regulatory frameworks demonstrate that digital fraud is not merely treated as a conventional criminal offense, but also as a threat to data security, the integrity of electronic systems, and public trust in the digital environment.

In the Indonesian context, the regulation of fraud and misuse of social media is primarily linked to Law Number 11 of 2008 on Electronic Information and Transactions, as amended by Law Number 19 of 2016 and Law Number 1 of 2024. The EIT Law provides a legal basis for unlawful acts involving electronic information, electronic documents, electronic systems, and electronic transactions. Consequently, social media is no longer perceived solely as a private communication space, but rather as part of a broader infrastructure of transactions and legal interactions that may give rise to criminal, civil, or administrative consequences when used for fraud, identity manipulation, dissemination of false information, or misuse of personal data.

Triangle fraud on social media has also evolved into a global phenomenon with relatively consistent patterns,[14] in which perpetrators exploit false identities, intermediary accounts, manipulated communications, and electronic transactions to deceive victims and obscure the relationships between buyers, sellers, and beneficiaries. While Indonesia primarily relies on the EIT Law, many other countries adopt a more integrated regulatory approach, combining cybercrime law, personal data protection, digital consumer protection, and electronic transaction regulations.

---

[13] Desia Rakhma Banjarani and Muhammad Apriliansyah Rahmadhani, "Cybercrime as Transnational Crime: Law Enforcement and Countermeasure Problems in the Perspective of International Criminal Law," *Yustisia Tirtayasa: Jurnal Tugas Akhir* 4, no. 4 (2024): 144–64.

[14] Anastasia Cheliatsidou et al., "The International Fraud Triangle," *Journal of Money Laundering Control* 26, no. 1 (2023): 106–32.

These differing regulatory models indicate that addressing triangle fraud cannot rely solely on punitive measures against perpetrators, but also requires strengthening platform governance, enhancing personal data protection, implementing digital identity verification, ensuring transaction security, and fostering cross-border cooperation in law enforcement.

Based on the background of the problem above, the author formulates the problem in writing this thesis as follows how is the law enforcement against criminal acts of fraud with the triangular fraud mode on social media and what efforts are made by the police to overcome criminal acts of fraud with the triangular fraud mode on social media and the purpose of the research is to analyze law enforcement against criminal acts of fraud using the triangular fraud method on social media and to analyze efforts made by the police to combat criminal acts of fraud using the triangular fraud method on social media.

2. Method

The study employs an empirical legal research method, emphasizing the collection and analysis of primary data derived from law enforcement practices in the field.[15] This approach is implemented through in-depth interviews with key law enforcement actors, including police investigators, prosecutors, and other relevant stakeholders directly involved in handling social media fraud cases.

In addition, the research is supported by observations of case-handling processes and an examination of pertinent legal documents. The collected data are subsequently analyzed qualitatively using a descriptive-analytical approach to identify patterns, constraints, and strategies applied in the enforcement of laws against such offenses.

To enhance the study's global relevance, the empirical method is further developed through a cross-jurisdictional comparative approach.[16] In this regard, interviews are not confined to law enforcement officials within a single country but also include respondents from multiple jurisdictions with differing legal traditions, including both civil law and common law systems.

This approach enables a more comprehensive understanding of variations in enforcement strategies, inter-agency coordination mechanisms, and the normative as well as practical challenges in addressing social media fraud at the international level. The findings from this comparative analysis are expected to contribute both theoretically and practically to the formulation of a more adaptive and responsive law enforcement model in dealing with transnational digital crimes.

---

[15] Michael G. Aamodt, *Research in Law Enforcement Selection* (BrownWalker press, 2004), https://books.google.com/books?hl=id&lr=&id=xcYvYziiElsC&oi=fnd&pg=PA1&dq=collection+and+analysis+of+primary+data+derived+from+law+enforcement+practices+in+the+field&ots=LZr7O3w0mO&sig=9uSAvwMkKO3v-Y8mdOooY11-YG0.

[16] Mr Ayaz Khan et al., "Methodological Foundations of Legal Research: A Critical Examination of Doctrinal, Comparative, and Socio-Legal Approaches," *ASSAJ* 5, no. 2 (2026): 106–13.

3. Analysis or Discussion

Law enforcement constitutes a dynamic and multifaceted process aimed at realizing the three fundamental ideals of law, namely justice, legal certainty, and utility. As the prominent Indonesian legal scholar Satjipto Rahardjo defined, law enforcement is the process of translating legislative desires, that is, the thoughts of the legislative body formulated in legal regulations, into social reality.[17]

However, this translation process rarely proceeds in a linear or frictionless manner. In practice, the effectiveness of law enforcement is contingent upon a complex interplay of systemic factors, including the quality of legal regulations themselves, the competence and integrity of enforcement personnel, the availability of infrastructure and technological tools, the level of public awareness and cooperation, and the prevailing legal culture within society.[18] In the context of triangular fraud on social media, each of these factors presents distinct challenges that require careful academic scrutiny.

Fraud, derived from the Indonesian word tipu, signifies dishonest or deceptive conduct, whether through words or actions, undertaken with the intention to mislead, trick, or secure unlawful profit.[19] Fraudulent acts inherently inflict harm upon others and therefore fall within the purview of criminal sanctions. The conventional legal basis for prosecuting fraud in Indonesia is codified in Article 378 of the Criminal Code (Kitab Undang Undang Hukum Pidana, hereinafter KUHP), which provides as follows: "Any person who, with the intention of benefiting himself or another unlawfully, either by using a false name or false status, either by means of trickery and deceit, or by fabricating a series of false words, persuades another person to deliver something, to create a debt, or to cancel a receivable, shall be punished for fraud with a maximum imprisonment of four years."[20]

According to the authoritative commentary by R. Soesilo in his seminal work entitled Complete Criminal Code (KUHP) and Complete Comments Article by Article, the crime defined in Article 378 KUHP is properly termed fraud, wherein the offender's primary modus operandi is to persuade another person to deliver goods, incur a debt, or cancel a receivable.[21]

The article contains four principal elements that must be proven cumulatively for a conviction to stand. The first element is the intention to benefit oneself or another unlawfully. This element refers to the subjective purpose of the perpetrator, namely that the perpetrator seeks to obtain a benefit. This benefit constitutes the primary objective of the perpetrator through unlawful means.[22]

---

[17] Satjipto Rahardjo, *Penegakan Hukum: Suatu Tinjauan Sosiologis* (Genta Publishing, 2009), 12, https://library.stik-ptik.ac.id/detail?id=9217&lokasi=lokal.
[18] Zabidin Zabidin, "Analisis Penegakan Hukum Tindak Pidana Penipuan Online Di Indonesia," *SPEKTRUM HUKUM* 18, no. 2 (2021).
[19] I. Gusti Made Jaya Kesuma et al., "Penegakan Hukum Terhadap Penipuan Melalui Media Elektronik," *Jurnal Preferensi Hukum* 1, no. 2 (2020): 72–77.
[20] Raden Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP): Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal: Untuk Para Pejabat Kepolisian Negara, Kejaksaan/Pengadilan Negeri, Pamong Praja, Dsb.* (Politeia, 1974), 245–47, https://cir.nii.ac.jp/crid/1130282271588828800.
[21] Soesilo, *Kitab Undang-Undang Hukum Pidana (KUHP)*.
[22] Renata Christha Auli, "Bunyi dan Unsur Pasal 378 KUHP tentang Penipuan | Klinik Hukumonline," December 7, 2023, https://www.hukumonline.com/klinik/a/pasal-378-kuhp-tentang-penipuan-lt6571693c4c627/.

The perpetrator must also intend further actions because the mere desire for benefit, absent concrete deceptive acts, cannot satisfy the actus reus requirement. Consequently, the intention must be directed at both profit and law violation, meaning that the perpetrator must know that the profit he or she seeks is unlawful. In the context of triangular fraud on social media, the perpetrator carries out his or her scheme by first requesting the account number of the original seller under the false pretense that the perpetrator intends to purchase and pay for the advertised goods, even though no such purchase ever materializes.

After the perpetrator successfully deceives both the seller and the prospective buyer, the perpetrator then provides his or her own personal bank account number to the buyer to execute the transaction. The funds transferred by the buyer ultimately become the perpetrator's personal property, thereby realizing the unlawful benefit.[23] This layered deception distinguishes triangular fraud from conventional two party fraud, as the perpetrator never directly interacts with both parties in a transparent manner.

The second element requires that the perpetrator employs one or more fraudulent driving tools, meaning the specific deceptive mechanisms that induce the victim to act. The KUHP enumerates four categories of such tools. First, a false name or false status, which includes any name different from the perpetrator's real name, even if the difference is minimal, and extends to cases where the perpetrator uses another person's name that coincidentally matches his or her own name. Second, clever trickery, which encompasses actions carried out in such a way that the conduct creates trust or confidence in another person, and this trickery is manifested through deeds or actions rather than mere verbal statements.

Third, false dignity or false condition, which occurs when a person makes a statement that he or she occupies a certain status or condition that confers rights only available to persons genuinely holding that status. Fourth, a series of lies, which must be articulated in an orderly and coherent manner so as to form a logically acceptable narrative, wherein each statement reinforces or justifies another. In triangular fraud, the perpetrator typically creates a detailed scenario and falsely claims that friends, relatives, or family members will visit the original seller to inspect the goods, thereby manufacturing credibility.[24] The third element consists of moving another person to hand over an item, to incur a debt, or to cancel a receivable.

This element implies a causal relationship between the perpetrator's deceptive driving tools and the victim's subsequent act of transfer.[25] Without such causation, meaning if the victim would have transferred the item regardless of the deception, the element remains unfulfilled. In triangular fraud, the buyer transfers money to the perpetrator's account precisely because the perpetrator has falsely represented himself or herself as the legitimate seller entitled to receive payment. Similarly, the

---

[23] Nicole F. Stowell et al., "The Use of Wills and Asset Protection Trusts in Fraud and Other Financial Crimes," *Drake L. Rev.* 65 (2017): 509.
[24] Arjan Reurink, "Financial Fraud: A Literature Review," in *Contemporary Topics in Finance*, 1st ed., ed. Iris Claus and Leo Krippner (Wiley, 2019), https://doi.org/10.1002/9781119565178.ch4.
[25] Vera Bergelson, "Victims and Perpetrators: An Argument for Comparative Liability in Criminal Law," *Buffalo Criminal Law Review* 8, no. 2 (2005): 385–487, https://doi.org/10.1525/nclr.2005.8.2.385.

original seller delivers goods to the buyer because the seller believes, based on the perpetrator's false assurances, that payment has been secured. Causation thus runs directly from the perpetrator's series of lies to the victim's detrimental act.

In addition to the KUHP, Indonesia has enacted special legislation governing cybercrimes, namely Law Number 11 of 2008 concerning Information and Electronic Transactions, as amended by Law Number 19 of 2016 (hereinafter the ITE Law). Article 28 paragraph 1 of the ITE Law stipulates as follows: "Any person who intentionally and without right disseminates false and misleading news that results in consumer losses in Electronic Transactions." The criminal sanction applicable to this offense is articulated in Article 45 paragraph 2, which provides: "Any person who fulfills the elements as referred to in Article 28 paragraph 1 or paragraph 2 shall be punished with imprisonment for a maximum of 6 years and or a maximum fine of Rp1,000,000,000.00 (one billion rupiah)."

Although Article 28 paragraph 1 does not explicitly employ the term fraud, it is directly relevant to triangular fraud for several reasons. First, the provision requires the dissemination of false and misleading news, which functionally equates to the series of lies or trickery element found in Article 378 KUHP. Second, the provision explicitly requires consumer losses arising from electronic transactions, thereby anchoring the offense in the digital commerce context where triangular fraud typically occurs. Third, the legislative history of the ITE Law indicates that Article 28 paragraph 1 was intended to capture deceptive conduct in cyberspace that might not fit neatly within the conventional elements of KUHP Article 378, particularly because the latter was drafted before the advent of social media, electronic payments, and anonymous digital identities.

Scholarly consensus supports the view that Article 28 paragraph 1 of the ITE Law constitutes an expansion of conventional criminal law into the digital domain. For triangular fraud cases, law enforcement officials routinely invoke both Article 378 KUHP and Article 28 paragraph 1 of the ITE Law simultaneously, thereby providing a dual legal basis that maximizes prosecutorial flexibility.[26] The ITE Law also confers evidentiary validity upon electronic evidence, including chat logs, screenshots, digital payment records, and metadata, which are often dispositive in triangular fraud cases where documentary evidence in physical form is entirely absent.

The implementation of law enforcement against triangular fraud does not always follow the ideal trajectory envisioned by the drafters of the KUHP and the ITE Law. Based on empirical data collected from fieldwork conducted at the Makassar Police, including interviews with investigators and case file reviews, five principal factors influence the effectiveness of enforcement. These factors are adapted from the general theory of legal effectiveness and contextualized to the specific characteristics of social media based triangular fraud. The first factor concerns the legal framework itself, including the clarity, completeness, and operationalizability of applicable regulations. In the Indonesian context, the substantive dimension refers to whether the relevant articles adequately capture the criminal conduct. Both provisions have been held by courts to apply to triangular

[26] Padri Achyarsyah et al., "The Role of Digital Evidence in Criminal Law Enforcement: Challenges of Authentication and Admissibility in Court," *Research Horizon* 5, no. 6 (2025): 2987–98.

fraud, and thus the substantive legal basis is generally sufficient based on available court decisions.[27]

The procedural dimension, however, presents greater difficulty. The absence of specific implementing regulations governing the investigation of triangular fraud, such as standardized protocols for obtaining electronic evidence from social media platforms based outside Indonesia, creates practical obstacles.[28] Furthermore, ambiguities in the definition of key terms, such as dissemination in Article 28 paragraph 1, can give rise to interpretive disputes between investigators, prosecutors, and defense counsel, thereby delaying case resolution.

The second factor pertains to the human resources involved in the law enforcement process, particularly police investigators. Law enforcers serve as role models within society and are expected to possess certain competencies that align with societal aspirations.[29] They must be able to communicate effectively and gain understanding from the target community in addition to carrying out their investigative functions.

Investigators play a crucial role in the implementation of law enforcement, and their performance directly determines whether cases progress from initial reports to successful prosecutions. Based on an interview conducted with an investigator at the Makassar Police, the procedural workflow for triangular fraud cases follows a structured sequence.

When a report is received, the police initially conduct an investigation. The victim first comes to the police station and files a formal report. After the report is accepted, an investigation warrant, known as sprindiki, is issued. At this stage, the police conduct the investigation by identifying the perpetrator's modus operandi, the bank account numbers used, the frequency of account number changes, the cellular phone numbers employed, whether those numbers remain active, and the geographical location of the perpetrator.

After obtaining instructions from this preliminary analysis, the police issue a letter of notification of investigation progress results, abbreviated as sp2hp, to the victim. Once the victim receives this letter, the victim is informed that the report is under active investigation and is provided with the name of the assigned investigator. If the perpetrator is subsequently located, the victim is notified again to return to the police station for further proceedings.

Despite this structured workflow, the interview revealed significant human resource constraints. There is a notable shortage of human resources and police officers who master technology in the cyber field. Even so, the police consistently endeavor to provide optimal services and enforcement efforts, although it must be acknowledged that the current level of service has not yet reached the standard of

---

[27] Dan Amiram et al., "Financial Reporting Fraud and Other Forms of Misconduct: A Multidisciplinary Review of the Literature," *Review of Accounting Studies* 23, no. 2 (2018): 732–83, https://doi.org/10.1007/s11142-017-9435-x.

[28] Erfan Mukhlas Ali et al., "Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia," *International Journal of Service Science, Management, Engineering, and Technology* 6, no. 3 (2024): 27–38.

[29] Sara E. McClellan and Bryon G. Gustafson, "Communicating Law Enforcement Professionalization: Social Construction of Standards," *Policing: An International Journal of Police Strategies & Management* 35, no. 1 (2012): 104–23.

perfection.[30] The lack of specialized cyber training among general duty investigators means that many triangular fraud cases are investigated using conventional methods designed for physical property crimes, which are often inadequate for tracing digital footprints.

The third factor comprises the facilities and infrastructure that support police operations, without which the enforcement process cannot run smoothly. These facilities and infrastructure include educated and skilled human resources, well structured organization, adequate equipment, sufficient financial resources, and physical infrastructure that supports the success of the law enforcement process.[31] If these prerequisites are not met, it is impossible for law enforcement to achieve its intended goals. In the case of the Makassar Police, specific deficiencies in facilities and infrastructure have been identified.

Several investigative tools are either not sufficiently specific or remain incomplete for the purpose of fully revealing online fraud cases. Tools for tracking digital evidence, including software and hardware used to verify whether a cellular phone number remains active, to geolocate the perpetrator, and to preserve digital evidence for court presentation, are lacking. Additionally, the police cyber infrastructure that would support real time data sharing and forensic analysis remains underdeveloped.[32] Consequently, investigators often rely on manual methods and third party cooperation, such as requesting data from financial institutions and telecommunications providers, which introduces delays and increases the likelihood of evidence spoliation.

The fourth factor concerns community variables, which are related to the public's understanding and knowledge of legal rules and norms. This factor also includes the community's trust in and perceptions of law enforcement officers. The community, as the environment in which the law is enforced and applied, plays an important role in the success or failure of law enforcement.[33] Without active community cooperation, including reporting incidents, preserving evidence, and testifying in court, even the most well resourced police force cannot effectively combat triangular fraud.

In triangular fraud cases, buyers who are strongly attracted to exceptionally low prices often exhibit a high level of trust that perpetrators can quickly exploit. When a buyer becomes interested in a product photograph that has been re uploaded by the perpetrator without authorization from the original seller, the buyer automatically contacts the perpetrator through the social media platform's messaging feature. Using various psychological tricks and fabricated narratives, the perpetrator facilitates the smooth operation of the fraudulent scheme.[34]

---

[30] Micol Seigel, *Violence Work: State Power and the Limits of Police* (Duke University Press, 2018).
[31] Bachtari Alam Hidayat, "Local Government Policy: Education, Training, and Improved Work Infrastructure Enhance Firefighter Performance," *Jurnal Bina Praja* 16, no. 2 (2024): 361–76.
[32] Michael M. Losavio et al., "The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy, and Security," *SECURITY AND PRIVACY* 1, no. 3 (2018): e23, https://doi.org/10.1002/spy2.23.
[33] John Kenedi, *Buku Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia* (Pustaka Pelajar, 2017)
[34] Ntogwa Ng'habi Bundala, "Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures," *Asian Journal of Research in Computer Science* 17, no. 12 (2024): 234–51.

Therefore, one of the primary causative factors enabling triangular fraud is the lack of knowledge and digital literacy within the community. Many individuals take actions that they perceive to benefit themselves, such as immediately transferring money to secure a bargain, without realizing that those actions are actually part of the perpetrator's deliberate strategy to facilitate the fraud. People tend to judge the quality of goods solely based on their visual appearance in photographs, without considering the long term impact of the decisions they make. Sometimes the purchased product proves unsatisfactory, meaning the item does not match what was depicted in the photograph.

Moreover, the price offered by the perpetrator is often low enough to attract buyers without triggering suspicion. Based on community outreach activities documented during fieldwork, several preventive measures have been recommended to the public to reduce vulnerability to triangular fraud. These include avoiding the purchase of goods at prices that deviate significantly from market norms, refusing to use the services of unknown or unverified brokers, avoiding suspicious transaction conditions such as a seller who refuses to be physically present at the location when the buyer wishes to inspect the unit to be purchased, always checking the ownership documentation of the unit and matching it against the seller's personal identification data, and using cash payments where feasible to reduce the chance of transaction errors or mistaken transfers.

The fifth factor is legal culture, which encompasses habits, opinions, mindsets, and actions carried out by members of society in relation to law and legal institutions. Legal culture may be defined as a set of values, behaviors, and traditions adopted by a society either in order to comply with legal controls or, conversely, to evade or resist them.[35] A person is considered to possess a high level of legal awareness only when his or her behavior aligns with applicable legal norms. Legal culture is often passed down from generation to generation through socialization within families, educational institutions, and peer groups.

Social and cultural factors can also influence the occurrence of cybercrimes, including online fraud. The transition from traditional to modern culture, characterized by the rapid adoption of social media platforms and digital payment systems without corresponding adaptation of precautionary habits, has created new opportunities for perpetrators.[36]

Social factors are also suspected to be among the causes of weak law enforcement against criminal acts of e commerce based fraud. A culture that prioritizes convenience and speed over verification and security, combined with low levels of legal literacy regarding digital transactions, enables perpetrators to operate with relative impunity. Furthermore, a cultural tendency to avoid formal legal processes due to perceptions of complexity, cost, or time delay means that many triangular fraud cases go unreported, thereby depriving the police of both data and opportunities for intervention.

---

[35] Sufirman Rahman and Anggreany Arief, "Efektivitas Penyelidikan Dalam Pengungkapan Tindak Pidana Penipuan Online Melalui Media Elektronik Internet Di Polrestabes Makassar," *Journal of Lex Generalis (JLG)* 3, no. 5 (2022): 1053–66.

[36] Tony Yuri Rahmanto et al., "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik," *Jurnal Penelitian Hukum De Jure* 19, no. 1 (2019): 31.

A comparative assessment of cyber law enforcement policies between Indonesia and advanced jurisdictions such as the European Union and the United States reveals fundamental differences in regulatory design, institutional capacity, and the degree of inter agency integration. In the European Union, the General Data Protection Regulation, commonly known as the GDPR, operates not only as a data protection instrument but also as a robust enforcement framework grounded in principles of accountability, mandatory breach notification, and substantial administrative sanctions.

By contrast, in the United States, the Computer Fraud and Abuse Act, hereinafter CFAA, provides a broad legal basis for prosecuting unauthorized access to and misuse of computer systems, although it has been subject to criticism for potential overcriminalization. Together, these regimes demonstrate that effective cyber law enforcement relies on normative clarity, interpretive flexibility, and enforcement infrastructures capable of adapting to rapid technological change. The legal foundation for cybercrime enforcement in Indonesia is rooted in Law Number 11 of 2008 on Electronic Information and Transactions as amended. Within this regime, statutory provisions delineate and classify a range of acts as cyber offenses, including unauthorized access, unlawful interception, manipulation of electronic data, and the dissemination of illegal content, while simultaneously recognizing and conferring evidentiary validity upon electronic evidence in judicial proceedings.

Furthermore, the dimension of personal data protection is reinforced through Law Number 27 of 2022 on Personal Data Protection, which incorporates universally recognized principles such as lawful processing, purpose limitation, and the acknowledgment of data subject rights, thereby establishing a normative basis for the prevention and prosecution of data misuse in cyberspace.

Accordingly, Indonesia's national legal framework reflects a trajectory toward a more comprehensive system, albeit one that still requires normative consolidation and enhanced effectiveness in implementation. Lessons drawn from the GDPR and the CFAA may therefore be translated into several strategic reforms, including strengthening accountability obligations for electronic system operators, enhancing mandatory reporting of cyber incidents, and developing sanctioning mechanisms that are both proportionate and effective.

At the international level, the legal framework governing cybercrime enforcement is shaped by the evolution of cross jurisdictional instruments and practices, including standards embodied in the GDPR within the European Union and the CFAA in the United States. The GDPR advances an administrative regulatory approach characterized by the imposition of significant sanctions for data breaches, whereas the CFAA emphasizes a criminal law regime targeting unauthorized access to and misuse of computer systems. In addition, the effectiveness of transnational enforcement is strengthened through international cooperation mechanisms facilitated by institutions such as Interpol and Europol, which provide platforms for coordination and information exchange among authorities.

Normatively, this configuration underscores that the legal basis for cybercrime enforcement has evolved beyond a purely domestic framework into a global legal order that necessitates harmonization and convergence of national policies. Furthermore, the effectiveness of cyber law enforcement cannot be separated from international cooperation, given the inherently transnational nature of cybercrime.

Perpetrators of triangular fraud often use social media platforms hosted in multiple jurisdictions, bank accounts opened under false identities in different countries, and anonymizing technologies that obscure their physical location.

In this regard, institutions such as Interpol and Europol play a pivotal role in facilitating information exchange, coordinating investigations, and conducting joint cross border operations. Such collaboration illustrates that the limitations of national jurisdiction can be mitigated through institutionalized cooperative mechanisms, provided that domestic legal frameworks permit the sharing of evidence and the execution of mutual assistance requests in a timely manner.

For Indonesia, strengthening engagement in international law enforcement networks alongside enhancing technical capacity and legal diplomacy constitutes a strategic pathway to improving the effectiveness of cybercrime control. Ultimately, the integration of domestic legal reform with optimized global cooperation stands as a key prerequisite for establishing a comprehensive and competitive cyber law enforcement system capable of addressing triangular fraud and other emerging forms of social media enabled deception.

3.2 Police Efforts in Combating Triangular Fraud on Social Media

Crime prevention is an integral component of criminal policy, social defense, and the broader pursuit of public welfare.[37] In the context of cyber-enabled fraud, prevention cannot be understood merely as the suppression of criminal acts after they occur, but must be situated within a comprehensive strategy that combines public education, risk reduction, investigative capacity, and post-offense law enforcement. This is particularly important in triangular fraud on social media, where perpetrators exploit digital communication, false identity construction, electronic transactions, and the absence of direct interaction between buyers and sellers to obscure criminal responsibility.

Triangular fraud differs from ordinary online fraud because it involves at least three actors: the original seller, the prospective buyer, and the perpetrator who manipulates both parties. The perpetrator usually positions himself as an intermediary or apparent seller, uses product images obtained from the legitimate seller, persuades the buyer to transfer money to the perpetrator's account, and simultaneously convinces the original seller that the person coming to inspect or collect the goods is a relative, friend, or representative. This layered structure creates evidentiary and investigative challenges because the deception is distributed across multiple conversations, accounts, payment channels, and sometimes different locations. Based on the interview with Brigpol Muh. Khaerul Anshary of the Makassar Police, police efforts in addressing triangular fraud on social media may be classified into three interrelated approaches, namely:

Pre-emptive Measures

Pre-emptive measures constitute the earliest stage of crime prevention and are directed at reducing the social and behavioral factors that make individuals vulnerable to triangular fraud. In social media-based fraud, victims are often

[37] Sidik Sunaryo, *Kapita Selekta Sistem Peradilan Pidana* (Penerbitan Universitas Muhammadiyah Malang, 2004).

deceived because of limited digital literacy, excessive trust in online communication, and attraction to prices that are significantly lower than market value.[38]

Based on the interview with Brigpol Muh. Khaerul Anshary of the Makassar Police, pre-emptive efforts are mainly carried out through community education by Bhabinkamtibmas or community policing officers. Their role is to provide legal awareness, educate residents about crime prevention, and offer practical guidance when people intend to conduct online buying and selling transactions.

In triangular fraud cases, such education should focus on concrete warning signs, including the use of third-party representatives, refusal to allow direct communication between buyer and seller, mismatched bank account identities, unusually low prices, and pressure to transfer money quickly. Therefore, pre-emptive policing should not merely advise the public to be careful, but should explain the specific modus operandi used by perpetrators so that potential victims can identify suspicious transaction patterns before losses occur.

Preventive Measures

Preventive measures aim to reduce opportunities for crime before triangular fraud is completed. Unlike pre-emptive measures, which emphasize public awareness, preventive measures focus on practical risk reduction in online transactions. In this context, the police may conduct public warnings, digital monitoring, community reporting, and coordination with relevant institutions such as banks, telecommunications providers, and social media platforms.[39]

Preventive efforts should encourage buyers and sellers to verify each other directly before completing a transaction. Buyers should confirm the seller's identity through video calls, ensure that the bank account name matches the seller's identity, request live location sharing, and document all communication. Sellers should avoid releasing goods based on instructions from third parties and should ensure that payment is received in their own verified account.

Accordingly, preventive efforts should be distinguished from coercive legal actions such as arrest, detention, search, and seizure. These coercive actions belong to the repressive stage because they are taken after a criminal act has occurred. Preventive measures should instead focus on early detection, transaction verification, and reduction of opportunities for perpetrators to manipulate communication between buyers and sellers.

Repressive Measures

Repressive measures are actions taken after triangular fraud has occurred. Their purpose is to investigate the offense, identify the perpetrator, secure evidence, and bring the case into the criminal justice process. Based on the interview with Brigpol Muh. Khaerul Anshary, once a report is received, the police conduct investigation and inquiry. At this stage, coercive measures such as arrest, detention, search, and seizure may be carried out in accordance with criminal procedure.[40]

---

[38] Januri Januri et al., "Upaya Kepolisian Dalam Penanggulangan Kejahatan Cyber Terorganisir," *Audi Et AP: Jurnal Penelitian Hukum* 1, no. 02 (2022): 94–100.
[39] Rinal Krishna Triananda et al., "Efektivitas Pencegahan Dan Penanggulangan Tindak Pidana Penipuan Jual Beli Online," *Journal of Lex Philosophy (JLP)* 5, no. 2 (2024): 471–86.
[40] Brigita Shinta Bethari, "Penegakan Hukum Bagi Pelaku Tindak Pidana Penipuan Arisan Online," *Supremasi: Jurnal Hukum* 4, no. 1 (2021): 77–94.

In triangular fraud cases, repressive efforts require careful handling of electronic evidence, including chat histories, screenshots, social media accounts, phone numbers, transfer receipts, bank account information, and witness statements from both the buyer and the original seller. Since the perpetrator manipulates both parties separately, investigators must reconstruct the sequence of communication to prove the causal link between deception and financial loss.

Repressive enforcement also has a deterrent function. Legal action against perpetrators demonstrates that social media-based fraud is subject to criminal liability. However, the results of investigation should also be used to strengthen future prevention by identifying recurring patterns, frequently used platforms, suspicious accounts, and common victim vulnerabilities. Thus, repressive measures should support not only punishment, but also the improvement of broader cybercrime prevention strategies.

3. Conclusion

This study has examined law enforcement against triangular fraud on social media and the strategies adopted by the Indonesian police, particularly the Makassar Police. The findings reveal that triangular fraud differs fundamentally from conventional online fraud due to its tripartite structure, layered communication, and indirect transaction patterns, which obscure criminal responsibility and complicate digital evidence tracing. Empirically, law enforcement remains suboptimal due to limited human resources, insufficient cybercrime expertise, and inadequate forensic infrastructure. In response, the Makassar Police have implemented three strategies: pre emptive efforts through public outreach, preventive efforts through investigation, and repressive efforts through legal action and public awareness measures. However, these strategies have not yet reached full effectiveness.

The novelty of this study lies in its specific focus on triangular fraud as a distinct modus operandi within social media based cybercrime, contributing a typology that can inform investigative protocols and legislative reform in the Indonesian context. Several policy implications follow. Institutionally, Indonesia must invest in specialized cybercrime units and forensic training. Regulatorily, the ITE Law requires implementing regulations that address evidentiary challenges unique to triangular fraud. Internationally, Indonesia should strengthen engagement with Interpol, Europol, and the Budapest Convention framework. For the public, prevention measures include seller verification through video calls, documentation of communication, live location confirmation, and immediate reporting of suspicious activities. Future research should conduct comparative empirical studies across multiple police jurisdictions and examine the harmonization of Indonesian cybercrime laws with international instruments.

References

Aamodt, Michael G. *Research in Law Enforcement Selection*. BrownWalker press, 2004.

Achyarsyah, Padri, Sugeng Riyadi, Kusno Widodo, and Mochammad Chamim. "The Role of Digital Evidence in Criminal Law Enforcement: Challenges of

Authentication and Admissibility in Court." *Research Horizon* 5, no. 6 (2025): 2987–98.

Ali, Erfan Mukhlas, Febrian Dirgantara, and Didit Darmawan. "Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia." *International Journal of Service Science, Management, Engineering, and Technology* 6, no. 3 (2024): 27–38.

Ambashtha, Kanahaiya Lal, and Pramod Kumar. "Online Fraud." In *Financial Crimes*, edited by Chander Mohan Gupta. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-29090-9_7.

Amiram, Dan, Zahn Bozanic, James D. Cox, Quentin Dupont, Jonathan M. Karpoff, and Richard Sloan. "Financial Reporting Fraud and Other Forms of Misconduct: A Multidisciplinary Review of the Literature." *Review of Accounting Studies* 23, no. 2 (2018): 732–83. https://doi.org/10.1007/s11142-017-9435-x.

Ardi, Aswar, M. Said Karim, and Haeranah Haeranah. "Law Enforcement Against Online Fraud Crimes: A Case Study at Police District Area of Wajo." *Jurnal Hukum Volkgeist* 6, no. 1 (2021): 51–57.

Auli, Renata Christha. "Bunyi dan Unsur Pasal 378 KUHP tentang Penipuan | Klinik Hukumonline." December 7, 2023. https://www.hukumonline.com/klinik/a/pasal-378-kuhp-tentang-penipuan-lt6571693c4c627/.

Banjarani, Desia Rakhma, and Muhammad Apriliansyah Rahmadhani. "Cybercrime as Transnational Crime: Law Enforcement and Countermeasure Problems in the Perspective of International Criminal Law." *Yustisia Tirtayasa: Jurnal Tugas Akhir* 4, no. 4 (2024): 144–64.

Bergelson, Vera. "Victims and Perpetrators: An Argument for Comparative Liability in Criminal Law." *Buffalo Criminal Law Review* 8, no. 2 (2005): 385–487. https://doi.org/10.1525/nclr.2005.8.2.385.

Bethari, Brigita Shinta. "Penegakan Hukum Bagi Pelaku Tindak Pidana Penipuan Arisan Online." *Supremasi: Jurnal Hukum* 4, no. 1 (2021): 77–94.

Bundala, Ntogwa Ng'habi. "Understanding Cybercrime Modus Operandi: Techniques, Psychological Tricks, and Countermeasures." *Asian Journal of Research in Computer Science* 17, no. 12 (2024): 234–51.

Cheliatsidou, Anastasia, Nikolaos Sariannidis, Alexandros Garefalakis, Jamel Azibi, and Paschalis Kagias. "The International Fraud Triangle." *Journal of Money Laundering Control* 26, no. 1 (2023): 106–32.

Graham, Mark, and William H. Dutton. *Society and the Internet: How Networks of Information and Communication Are Changing Our Lives*. Oxford University Press, 2019.

Habibi, Miftakhur Rokhman, and Isnatul Liviani. "Kejahatan Teknologi Informasi (Cyber Crime) Dan Penanggulangannya Dalam Sistem Hukum Indonesia." *Al-Qanun: Jurnal Pemikiran Dan Pembaharuan Hukum Islam* 23, no. 2 (2020): 400–426.

Hidayat, Bachtari Alam. "Local Government Policy: Education, Training, and Improved Work Infrastructure Enhance Firefighter Performance." *Jurnal Bina Praja* 16, no. 2 (2024): 361–76.

Ilyas, Amir. "Perwujudan Prinsip Legalitas Dalam Tindak Pidana Penghinaan." *Amanna Gappa*, 2017, 79–104.

Januri, Januri, Dwi Putri Melati, and Muhadi Muhadi. "Upaya Kepolisian Dalam Penanggulangan Kejahatan Cyber Terorganisir." *Audi Et AP: Jurnal Penelitian Hukum* 1, no. 02 (2022): 94–100.

Jones, Owen D., Owen D. Jones, and Francis X. Shen. "Law and Neuroscience in the United States." In *International Neurolaw*, edited by Tade Matthias Spranger. Springer Berlin Heidelberg, 2012. https://doi.org/10.1007/978-3-642-21541-4_19.

Kenedi, John. *Buku Kebijakan Hukum Pidana (Penal Policy) Dalam Sistem Penegakan Hukum Di Indonesia*. Pustaka Pelajar, 2017.

Kesuma, I. Gusti Made Jaya, Ida Ayu Putu Widiati, and I. Nyoman Gede Sugiartha. "Penegakan Hukum Terhadap Penipuan Melalui Media Elektronik." *Jurnal Preferensi Hukum* 1, no. 2 (2020): 72–77.

Khan, Mr Ayaz, Aisha Nayab Qureshi, and Muhammad Zubair Khan. "Methodological Foundations of Legal Research: A Critical Examination of Doctrinal, Comparative, and Socio-Legal Approaches." *ASSAJ* 5, no. 2 (2026): 106–13.

Losavio, Michael M., K. P. Chow, Andras Koltay, and Joshua James. "The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy, and Security." *SECURITY AND PRIVACY* 1, no. 3 (2018): e23. https://doi.org/10.1002/spy2.23.

Mashdurohatun, Anis, Euis Sopiah, Muhammad Harris, Porman Patuan Radot, and Jhon Mulia. "Legal Reform for Rectifying Child Violence in Educational Settings through the Lens of Justice." *Edelweiss Applied Science and Technology* 9, no. 2 (2025): 1082–89. https://doi.org/10.55214/25768484.v9i2.4658.

McClellan, Sara E., and Bryon G. Gustafson. "Communicating Law Enforcement Professionalization: Social Construction of Standards." *Policing: An International Journal of Police Strategies & Management* 35, no. 1 (2012): 104–23.

Munik, Apriyas, Fajar Ali Syabana, Ewin Eka ijayanto Wijayanto, Ali Rasya, and Sufiarina Sufiarina. "Law Enforcement And Factors Background To The Crime Of Fraud In Online Selling Transactions In Indonesia." *IJOSPOL-International Journal of Social, Policy and Law* 4, no. 2 (2023): 47–55.

Nugroho, Lucky. "The Role of Information for Consumers in the Digital Era (Indonesia Case)." *Artvin Çoruh Üniversitesi Uluslararası Sosyal Bilimler Dergisi* 7, no. 2 (2021): 49–59.

Parajuli, D. N., and Newal Chaudhary. "Rights and Duties of Buyers and Sellers Online in Cyberspace." *Issue 6 Int'l JL Mgmt. & Human.* 7 (2024): 567.

Rahardjo, Satjipto. *Penegakan Hukum: Suatu Tinjauan Sosiologis*. Genta Publishing, 2009. https://library.stik-ptik.ac.id/detail?id=9217&lokasi=lokal.

Rahmad, Noor. "Kajian Hukum Terhadap Tindak Pidana Penipuan Secara Online." *Jurnal Hukum Ekonomi Syariah* 3, no. 2 (2019): 103–17.

Rahman, Sufirman, and Anggreany Arief. "Efektivitas Penyelidikan Dalam Pengungkapan Tindak Pidana Penipuan Online Melalui Media Elektronik Internet Di Polrestabes Makassar." *Journal of Lex Generalis (JLG)* 3, no. 5 (2022): 1053–66.

Rahmanto, Tony Yuri, JHRS Kav, and Jakarta Selatan Kuningan. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik." *Jurnal Penelitian Hukum De Jure* 19, no. 1 (2019): 31.

Reurink, Arjan. "Financial Fraud: A Literature Review." In *Contemporary Topics in Finance*, 1st ed., edited by Iris Claus and Leo Krippner. Wiley, 2019. https://doi.org/10.1002/9781119565178.ch4.

Saxena, A. K. *Black Money and Economic Crimes*. KK Publications, 2021..

Seigel, Micol. *Violence Work: State Power and the Limits of Police*. Duke University Press, 2018.

Sitompul, Josua. "Developing a Legal Framework of Personal Data Protection in the Indonesian Criminal Procedure Law." *Indonesia Law Review* 9, no. 3 (2019). https://doi.org/10.15742/ilrev.v9n3.582.

Soesilo, Raden. *Kitab Undang-Undang Hukum Pidana (KUHP): Serta Komentar-Komentarnya Lengkap Pasal Demi Pasal: Untuk Para Pejabat Kepolisian Negara, Kejaksaan/Pengadilan Negeri, Pamong Praja, Dsb.* Politeia, 1974. https://cir.nii.ac.jp/crid/1130282271588828800.

Stowell, Nicole F., Erik Johanson, and Carl Pacini. "The Use of Wills and Asset Protection Trusts in Fraud and Other Financial Crimes." *Drake L. Rev.* 65 (2017): 509.

Sunaryo, Sidik. *Kapita Selekta Sistem Peradilan Pidana*. Penerbitan Universitas Muhammadiyah Malang, 2004.

Triananda, Rinal Krishna, Askari Razak, and Nur Fadhillah Mappaselleng. "Efektivitas Pencegahan Dan Penanggulangan Tindak Pidana Penipuan Jual Beli Online." *Journal of Lex Philosophy (JLP)* 5, no. 2 (2024): 471–86.

Yurizal, D. R. *Penegakan Hukum Tindak Pidana Cyber Crime Di Indonesia*. Vol. 1. Media Nusa Creative (MNC Publishing), 2018.

Zabidin, Zabidin. "Analisis Penegakan Hukum Tindak Pidana Penipuan Online Di Indonesia." *SPEKTRUM HUKUM* 18, no. 2 (2021).

Conflict of Interest Statement: The author(s) declares that the research was conducted in the absence of any commercial or financial relationship that could be construed as a potential conflict of interest.