Volume 8 Number 1 (2026)
January-June 2026
Page: 365-380

E-ISSN: 2686-4819
P-ISSN: 2686-1607
DOI: 10.37680/almanhaj.v8i1.9538

AL-MANHAJ
Jurnal Hukum dan Pranata Sosial Islam

Normative Analysis of Criminal Liability for Triangle Scheme Fraud in Motorcycle Transactions

Nurloise Viano[1], Yuliana Yuli[2]

[1] National Development University "Veteran" Jakarta, Indonesia; 2210611342@mahasiswa.ac.id
[2] National Development University "Veteran" Jakarta, Indonesia; yuli@upnvj.ac.id

Received: 16/04/2026 Revised: 01/05/2026 Accepted: 23/05/2026

Abstract

Technological advancements have fueled complex cybercrimes, including the "triangular scheme" fraud in online transactions. This scheme introduces a novel issue: the emergence of dual victims (sellers and buyers) simultaneously harmed by perpetrators acting as fictitious intermediaries. This study aims to analyze the application of criminal elements in the Surabaya District Court Decision No. 2051/Pid.B/2025/PN—Sby and to identify obstacles to its enforcement. Using a normative legal method, this study found that the elements of Article 378 of the Criminal Code (KUHP) have been satisfied. However, the finding highlights a legal gap between the application of the Criminal Code and the ITE Law; the judge adjudicated the case under conventional criminal law and disregarded the ITE Law on the dissemination of misleading information, even though electronic means are central to the modus operandi. This gap risks creating a jurisprudential vacuum and exacerbating evidentiary challenges, which are often hindered by the volatility of digital evidence and the anonymity of perpetrators' identities. This study underscores the need for the integrated application of the Criminal Code and the ITE Law, coupled with strengthened digital forensic capabilities among law enforcement, to ensure legal certainty and comprehensive protection for victims.

Keywords

Fraud; pyramid scheme; criminal evidence; criminal liability; Article 378 of the Criminal Code; cybercrime

Corresponding Author
Nurloise Viano
National Development University "Veteran" Jakarta, Indonesia; 2210611342@mahasiswa.ac.id

1. INTRODUCTION

The development of information technology in the digital age has made it easier for the public to engage in various economic activities, including the buying and selling of motor vehicles. However, this progress has not only brought positive impacts but has also given rise to increasingly complex new forms of crime. One tangible impact of the misuse of this technological development is the emergence of online fraud, according to the website patrolisiber.ID, there were 14,496 cases of online fraud, including online shopping scams. (Patroli Siber, 2025)

The rapid development of information technology has given rise to various new fraud schemes in the virtual world (Chandra et al., 2024). One common modus operandi of crime today is the "triangle scam," which is frequently encountered in used motorcycle sales transactions. A triangle scam is a crime involving three parties: the perpetrator, the first victim (the seller or investor), and the second victim (the buyer) (Munawaroh Nafiatul, 2025). In this scheme, the perpetrator (A) acts as a fictitious intermediary between a seller (B) and a buyer (C). A finds B's motorcycle advertisement and reposts it at a lower price to attract C. Communicating separately, A directs C to transfer funds to A's account while promising B a cash buyer. Once C pays, A disappears without compensating B or delivering the motorcycle to C, leaving both parties defrauded. (Fauzi, 2018)

Online fraud is a criminal offense governed by several legal provisions. From a legal perspective, the primary legal basis regulating fraud using the "triangular scheme" in Indonesia is Article 378 of the Criminal Code (KUHP), which serves as *the lex generalis* (general rule) (Purba, 2026). This article defines fraud as an act committed by a person with the intent to obtain unlawful gain for oneself or another, by using a false name or false circumstances, through deceit, or a series of lies, which causes another person to hand over property to them, or to grant a loan or settle a debt. (Mulyadi, 2017)

The primary legal basis governing fraud using the "triangular scheme" in Indonesia is Article 378 of the Criminal Code (KUHP). There is also a special provision (*lex specialis*) in Article 28(1) of the Electronic Information and Transactions Law (ITE Law), which specifically regulates the dissemination of false information that harms consumers in electronic transactions, where Article 32, *in conjunction with* Article 48 of the EIT Law, may also be applied. (Nur, 2025)

Furthermore, an analysis of criminal liability under this framework requires an in-depth examination of culpability theory in the Indonesian legal system. In criminal law, punishment may only be imposed if the perpetrator is at fault (*schuld*), in accordance with the principle of *"geen straf zonder schuld*," meaning "no punishment without fault" (Hapid et al., 2024). A person can only be punished if their act was committed with an element of intent (*dolus*) or negligence (*culpa*) that is attributable to them. (Ahmad Usfa, 2006)

Therefore, an analysis of the perpetrator's criminal liability in triangular-scheme fraud cases is crucial to determine the extent to which they can be held accountable for their actions. Moreover, the definition of the criminal offense of fraud has been reformulated in Article 492 (Putra, 2025). The selection of the appropriate legal provisions in the enforcement of online fraud cases must be based on careful consideration, including the modus operandi of the crime, the strength of the evidence, the extent of the loss, and the technical complexity of the act.

Despite existing legal instruments, debates persist over criminal liability in "triangular schemes" in which dual victims are defrauded through electronic transactions. A key example is the Surabaya District Court Decision No. 2051/Pid.B/2025/PN.Sby. In this case, the defendant committed fraud by feigning interest in a motorcycle advertised on Facebook. To gain the seller's trust, the defendant provided an ID card as collateral to "test drive" the vehicle, only to abscond with it. The panel of judges subsequently found that the defendant's actions satisfied the elements of fraud under Article 378 of the KUHP. This ruling is noteworthy and highlights a legal gap. Although the act was committed via electronic media and demonstrated a pattern of modern fraud, the panel of judges still applied the conventional fraud provisions in the Criminal Code, thereby raising legal questions regarding the basis for determining the criminal liability of perpetrators in crimes involving digital transactions.

In this case, the judges focused on conventional fraud elements and the defendant's lies without considering electronic means as an integral part of the *modus operandi*. This approach is problematic, as the use of social media and electronic transactions may constitute disseminating misleading information under the ITE Law. Ignoring these provisions reflects a tendency to apply conventional law to digital crimes, risking a legal vacuum in addressing complex "triangular schemes." Consequently, perpetrator liability requires an in-depth analysis of the theory of *schuld* within Indonesia's legal positivism framework.

The principle of *geen straf zonder schuld* requires proof of *dolus* or *culpa*, which is often hindered in digital contexts by volatile evidence, anonymous identities, and jurisdictional challenges. Therefore, adjudicating "triangular scheme" fraud should not rely solely on Article 378 of the Criminal Code, but must also integrate Article 28(1) of the ITE Law, which specifically addresses misleading information that harms consumers. Given the centrality of electronic platforms, a combined application of these norms, whether through alternative or subsidiary charges, is essential for legal certainty and optimal victim protection. (Yunita, 2023)

Based on this background, particularly regarding the prevalence of online fraud involving the "triangle scheme" in motorcycle sales transactions and the complexity of applying applicable legal provisions, this study focuses on two main points. First, how does a legal analysis of the coherence in applying the elements of the offense under Article 378 of the Criminal Code (KUHP) without considering the provisions of the ITE Law address the "triangle scheme" modus operandi in the digital context, as reflected in the Decision of the Surabaya District Court No. 2051/Pid.B/2025/PN?Sby. Second, how the legal framework for proving criminal intent (*mens rea*) and causality in "triangle scheme" crimes is constructed to address the deadlock in law enforcement caused by the volatility of digital evidence and to ensure certainty in victim protection.

Thus, the objective of this study is to analyze the application of Article 378 of the Criminal Code to the digital-based "triangle scheme" modus operandi in the absence of the ITE Law, and to examine the proof *of mens rea* and causation to overcome challenges posed by digital evidence and ensure victim protection.

2. METHOD

This study employs a normative legal methodology, specifically a literature review examining legal norms, legal principles, and legislation related to the criminal offense of "triangle scheme" fraud in motorcycle sales transactions (Hadjon & Djatmiati, 2005). Furthermore, the case analysis also draws on deductive legal reasoning techniques, which involve inferring from general premises to specific cases of fraud involving the "triangle scheme" (Arifudin et al., 2024). The analysis examines the application of Article 378 of the Criminal Code and its relevance to electronic transaction-based criminal offenses, to construct a systematic legal argument. The research approach encompasses a legal, conceptual, and teleological approach.

The juridical approach involves an examination of the 1945 Constitution of the Republic of Indonesia, the Criminal Code, Law No. 11 of 2008, in conjunction with Law No. 19 of 2016 on Information and Electronic Transactions, and Law No. 1 of 2023 on the Criminal Code (Aziz, 2012). The conceptual approach is used to examine legal doctrines and the views of legal experts regarding fraud, criminal liability, fault (*schuld*), and proof in electronic transaction-based criminal offenses. Meanwhile, a teleological approach is used to analyze the logical rationale behind the formulation of norms in the Electronic Information and Transactions Law (ITE Law), to determine how the law should be interpreted by the courts to address and fill legal gaps resulting from the hybridization of cybercrime. (Hasibuan & Nst, 2023)

The data sources for this study consist of secondary data, including primary legal materials such as laws and regulations, secondary legal materials such as books and academic journals, and tertiary legal materials such as legal dictionaries and encyclopedias. Regarding the procedure for analyzing legal materials, this study employs a qualitative normative analysis method conducted in a prescriptive manner. The analysis procedure begins with an inventory of primary and secondary legal materials, followed by the systematization of the norms governing criminal fraud and electronic transactions. The structured legal materials are then analyzed using *content analysis* and interpreted teleologically to evaluate the Decision of the Surabaya District Court No. 2051/Pid.B/2025/PN.Sby, thereby enabling the derivation of conclusions that comprehensively address the research problem.

3. FINDINGS AND DISCUSSION

3.1. Application of the Elements of the Criminal Offense of Fraud under Article 378 of the Criminal Code to Perpetrators of Triangle Scheme Fraud in Motorcycle Sales Transactions Based on Judgment No. 2051/Pid.B/2025/PN.Sby

3.1.1. Definition and Elements of Fraud under Article 378 of the Criminal Code

In Decision No. 2051/Pid.B/2025/PN. Sby, the judges used Article 378 of the Criminal Code (KUHP) as the primary basis for adjudicating the "triangular scheme." Property protection is explicitly regulated under this article (Wuisan, 2020). Essentially, the Criminal Code does not provide a separate definition of fraud but rather defines it by reference to the elements of the offense (Mulyadi, 2017). According to M. Sudrajat Bassar, the methods that can be used to commit the criminal offense of fraud, as referred to in Article 378 of the Criminal Code, include using a false name, using a false position or status, using deceitful schemes, and using a series of lies. (Angraeni & Arifin, 2023)

A person may be deemed to have committed the criminal offense of fraud if they have fulfilled the elements stipulated in Article 378. The elements contained in that article, according to the view of R. Soesilo, are as follows: (Zamroni, 2026)

a. Any person
b. With the intent to benefit oneself or another person
c. By using a false name or false status, deceit, or a series of lies
d. Persuades another person to hand over property

Under national criminal law reform, these provisions are reformulated in Article 492 of Law No. 1 of 2023. While the wording is simplified, the essence remains unchanged: fraud is a property crime requiring intent and deceit (Paluaran et al., 2024). Based on this framework, the analysis examines how the judges subsumed these four normative elements into the trial facts of the Surabaya decision.

3.1.2. Analysis of the Application of the Elements of Article 378 in Judgment No.2051/Pid.B/2025/PN. Sby

In Judgment No. 2051/Pid.B/2025/PN. Sby, the criminal act of fraud began on July 2, 2025, when witness Anam Malik advertised a 2018 Suzuki GSX R150 motorcycle on Facebook for Rp14,000,000. The following day, the defendant, Octavianto Heri Kusuma, contacted the victim and expressed interest in purchasing the motorcycle. A meeting took place on July 4, 2025, at the victim's residence in Wonokromo, Surabaya. After inspecting the vehicle, the defendant requested permission to test-drive it and handed over his ID card as collateral.

However, after taking the motorcycle, the defendant did not return and cut off communication with the victim, thereby causing financial loss. The victim then took the initiative to track down the defendant and successfully located the motorcycle at the defendant's rented room in Surabaya. Based on this discovery, the defendant was arrested and prosecuted. During the trial, the defendant admitted to the act and stated that from the outset, he had indeed intended to take possession of the victim's motorcycle.

Based on this factual chronology of events, to prove that the defendant has legally and convincingly committed the criminal act of fraud, a thorough analysis of the elements of the offense under Article 378 of the Criminal Code must be conducted. The legal fulfillment of these elements requires the support of at least two valid pieces of evidence, which simultaneously serve to guide the Public Prosecutor in systematically constructing the indictment (Alamri, 2017). In analyzing this provision, drawing on S. R. Sianturi's perspective, the construction of a criminal offense can be fundamentally classified into objective and subjective dimensions. The objective element focuses on the physical acts committed by an individual, the tangible consequences arising from those acts, and the specific factual circumstances accompanying their commission. (Ponglabba, 2017)

The proof of a criminal act also cannot be separated from the subjective element inherent in the perpetrator as a legal subject who can be held criminally liable. This subjective element is closely related to the doctrine of fault (*schuld*), under which an act must be proven to have been committed based on fault—whether regarding the intent, the resulting consequences, or the awareness of the conditions at the time the act was committed (Utoyo et al., 2020). In Case No. 2051/Pid.B/2025/Pn. Sby, the elements required under Article 378 of the Criminal Code have been met, as elaborated in the subsequent discussion. (Al Miski et al., 2025)

Whoever

If a person is proven to have committed a criminal act, this does not automatically mean that they can be sentenced to a criminal penalty, as the element of fault must still be satisfied as the basis for criminal liability (Fernando & Wasiska, 2023). This interpretation is closely related to the element of "any person" in Article 378 of the Criminal Code. The element of "anyone" does not merely refer to a legal subject as the perpetrator of a criminal act, but also implies that the perpetrator must be criminally competent.

Thus, even if the objective elements of fraud have been met, a criminal sentence still requires the presence of fault and criminal competence on the part of the defendant. In this case, Judgment No. 2051/Pid.B/2025/PN. Sby, the element of "anyone" refers to the Defendant as fully identified in the indictment and the judgment. The defendant is a legal subject in the form of a natural person with legal

capacity, is not in a condition that negates the capacity to be held accountable, and was present and examined at trial. The defendant himself confirmed this identity and was not contested during the trial; thus, legally, the element of "anyone" has been satisfied.

With the intent to benefit oneself or another

The element "with the intent to benefit oneself or another person" is part of the subjective element in the criminal offense of fraud (Mardina, 2022). This element emphasizes *the presence of dolus,* or intent, directed toward a specific purpose: namely, obtaining unlawful gain. The phrase "intent" in this element indicates the presence of an inner will or *"willens en watens"* on the part of the perpetrator to achieve the desired result (Husna et al., 2025). Moeljatno argues that the element of intent in criminal law implies that the perpetrator is aware of and desires the consequences of their actions. Thus, in the context of fraud, the perpetrator does not merely commit a deceptive act but also consciously intends for their actions to yield a benefit, whether for themselves or another party. The benefit in question is not limited to material gain but also includes non-material benefits as long as they hold value for the perpetrator. (Amri, 2021)

In the present case, this element is reflected in the Defendant's actions, who deliberately devised a triangular scheme in the motorcycle sales transaction to obtain money from the victim. The Defendant knew that the vehicle being offered was not lawfully his to sell in that manner, yet he still persuaded the victim to hand over money. This fact demonstrates a clear intent and purpose to obtain unlawful gain, thereby fulfilling the subjective element of "with the intent to benefit oneself or another." The fulfillment of this element simultaneously proves the existence of fault in the form of direct intent (*opzet als oogmerk*), as the act was committed from the outset with the primary purpose of obtaining gain through fraud.

By using a false name or false identity, deception, or a series of lies

The element involving the use of a false name or identity, deception, or a series of lies is understood as an act that influences a person's will through dishonest and deceptive means, thereby causing the victim to become convinced and hand over property or provide a benefit to the perpetrator (Wibisono & Mahanani, 2023). In this context, the fraud in question is not merely a single false statement.

However, it may consist of a series of actions or statements that build trust, making the transaction or relationship appear legitimate and valid. In Judgment No. 2051/Pid.B/2025/PN.Sby, the defendant's actions—offering a motorcycle under a test-drive scheme, providing an ID card as collateral, and cutting off communication after obtaining the vehicle—demonstrate that this modus operandi consists of a series of deliberate lies and a fraudulent scheme. These lies are an integral part of the method of manipulating the victim, so that this objective element can be legally and convincingly

considered fulfilled.

Including another person to surrender property

The element of persuasion in Article 378 of the Criminal Code implies that the perpetrator's fraudulent acts must directly influence the victim's will, leading them to consciously surrender property, grant a loan, or discharge a debt. This requires a clear causal relationship between the deception and the victim's actions (Chaerunnisa & Fadlian, 2022). The term "persuading" should be interpreted broadly as influencing another's will through dishonestly means, rather than merely requesting or receiving property (Sumenge, 2013). The fulfillment of this element depends on proving that the surrender of property was not due to independent reasons, but was a direct result of the fraud. Essentially, the crux of this element lies in the "but-for" causation: without the specific deception or series of lies, the victim would not have surrendered the property.

Referring to the explanation in the previous paragraph, in *this* case, the defendant employed a "triangular scheme" by establishing a convincing relationship, devising a transaction plan that appeared legitimate, and providing false information to the victim. This series of fraudulent acts clearly influenced the victim to the point of handing over a motorcycle or money to the defendant. Trial evidence indicates that such a handover would not have occurred had the victim known the true circumstances. Therefore, there is a clear causal relationship between the defendant's fraud and the victim's act of handing over property, thereby establishing the element of "persuading another person to hand over property" as legally and convincingly proven.

Based on the trial facts in Judgment No. 2051/Pid.B/2025/PN. Sby, all elements of Article 378 of the Criminal Code have been fulfilled. The defendant, as a competent legal subject, was proven to have intended unlawful self-enrichment through a series of lies, specifically the "test drive" pretext, which directly caused the victim to surrender the vehicle. This classification remains consistent with the formulation of Article 492 of the Law No. 1/2023. However, since the crime was orchestrated via Facebook and WhatsApp, the act normatively intersects with the ITE Law regarding the dissemination of misleading information. This intersection highlights the urgency of examining cumulative or alternative legal applications to adequately address the electronic dimensions of the "triangular scheme" and ensure comprehensive legal certainty.

3.1.3. Analysis of the Judge's Rationale in the Judgment

This case can be analyzed through the theory of ratio decidendi, the primary legal foundation of a judicial decision. Sudikno Mertokusumo asserts that a ruling gains legitimacy if its reasoning is logical, systematic, and legally accountable (Azmi, 2024). In this decision, the judges' reasoning appears consistent, with a structured presentation of the criminal elements, demonstrating mature judicial

argumentation. Regarding the theory of fault, Pompe defines fault as the mental connection, either intent (*dolus*) or negligence (*culpa*), between the perpetrator and their act (Sanjaya, 2024). The judges implicitly confirmed intent as a purpose (*opzet als oogmerk*), identified from the defendant's scheme to control the victim's vehicle illegally. Thus, the court examined both external actions and the defendant's mens rea.

Furthermore, the theory of sufficient causation explains the causal relationship here. This theory states that an act is a cause if, by general experience, it reasonably leads to specific legal consequences (Sofian, 2015). The defendant's deceptions constituted a sufficient cause for the victim to surrender the vehicle. Consequently, the judge's assessment of the correlation between the lies and the financial loss aligns with the modern causation doctrine. Finally, the use of social media and messaging apps places this offense within the spectrum of cyber-enabled crime.

The normative use of Facebook and WhatsApp platforms opens the possibility of applying Article 28(1) of the ITE Law to the dissemination of false news that harms consumers in electronic transactions. However, from a theoretical perspective, the principle *of lex specialis derogat legi generali* must be considered (Agustina, 2015). If the factual circumstances are more accurately described under the offense of fraud in the Criminal Code (KUHP), then the application of the KUHP is deemed legally sufficient. Nevertheless, this normative satisfaction warrants critical evaluation as it reveals a flaw in reasoning when accommodating the reality of cybercrime. Setting aside the ITE Law is tantamount to reducing cybercrime to mere conventional crimes, risking that jurisprudence will lose its anticipatory power to technological developments.

When viewed through the theory *of ideal convergence*, a single series of the defendant's acts could actually violate both Article 378 of the Criminal Code and Article 28(1) of the ITE Law simultaneously (Dewi & Yuliawan, 2025). However, given that judges are bound by the principle of *nullum crimen sine lege stricta* and the limitations of the indictment, they cannot go beyond what is charged by the Public (Wicaksana, 2026). The judge's limitation under the principle in adjudicating this case fundamentally stems from the weakness of the charges brought by the Public Prosecutor (JPU). In the criminal justice system, the judge adopts a passive role regarding the scope of the offense and is bound by the principle that a judgment must not exceed the scope of the charges. (Luis, 2021)

In addressing the complexities of cybercrimes such as "pyramid schemes," prosecutors should adopt a progressive law enforcement approach by drafting multi-layered indictments. The use of alternative charges—such as the first charge referencing Article 28(1) of the ITE Law and the second charge referencing Article 378 of the Criminal Code—is highly effective as a safety net. If the Public Prosecutor faces difficulties proving specific elements of electronic transactions during the trial due to the volatility of digital evidence, the defendant can still be prosecuted for conventional fraud. On the

other hand, by referring to the concept of concurrent criminal acts (*concursus idealis* or *eendaadse samenloop*) under Article 63(1) of the Criminal Code, the Prosecutor may also construct a subsidiary charge (Keintjem et al., 2021). In this hierarchy, the ITE Law is the primary charge, as *lex specialis*, while Article 378 of the Criminal Code is the subsidiary charge.

The Public Prosecutor's failure to formulate this responsive and layered charge ultimately forces the judiciary into a narrow path**.** The panel's judicial stance, which merely opts for a pragmatic path, confirms the persistence of a rigid legal positivist mindset. Judges tend to position themselves merely as the mouthpiece of the law, or *la bouche de la loi,* rather than engaging in legal discovery responsive to the malpractice in drafting charges. Although not included in the dispositive portion of the ruling, it would be more progressive if the judges provided *an obiter dictum* regarding the electronic dimension as a modus operandi to enrich legal interpretation for similar cases in the future. It is this lack of breakthroughs in the judiciary that ultimately perpetuates the legal gap in the handling of "triangle scheme" cybercrimes in Indonesia.

3.2. Evidentiary and Law Enforcement Challenges Regarding Triangle Scheme Fraud Crimes and Efforts to Address Them

Triangular fraud is a fairly complex form of crime because it involves more than two parties in the transaction scheme (Andi Marlina & Nur Alim Rachim, 2026). Perpetrators of this type of fraud exploit the relationship between buyers and sellers, who generally do not know each other, to obtain illicit gains. This pattern makes proving criminal fraud involving a triangular scheme more difficult than proving other types of fraud. The difficulties in proving this triangular scheme can essentially be categorized into two dimensions: technical and forensic obstacles, and structural and jurisdictional obstacles.

From a technical and forensic perspective, perpetrators of triangular fraud are often difficult to track because they do not use real identities, bank account numbers, or disposable phone numbers, factors that complicate tracking and hinder the investigative process (Ihsan, n.d.). Furthermore, as technology advances, the use of *intermediary accounts* and prepaid SIM cards has become a primary tool in triangular fraud, and the exploitation of the digital realm in this crime further complicates the verification of fraudsters' identities.

In this context, the misuse of technological advancements has significant implications and demands a more adaptive law enforcement approach. Furthermore, regarding structural and jurisdictional barriers, law enforcement officials are often hindered by bureaucratic rigidity, such as time-consuming bank secrecy disclosure procedures, which ultimately provide a window of opportunity for perpetrators to transfer assets across borders or convert them into cryptocurrency.

The shortcomings in addressing cybercrime in Indonesia often stem from the slow adaptation of conventional criminal procedure laws. Compared to other *civil law* countries, such as the Netherlands, law enforcement regarding digital crimes has been accommodated through the modernization of *the Wetboek van Strafvordering*. The Dutch legal system provides a more progressive jurisdictional foundation for authorities to swiftly intercept data and freeze digital assets without being hindered by conventional bureaucratic procedures. This flexibility has long been a weakness in Indonesia's old Criminal Procedure Code (Erawan et al., 2026). In Indonesia, Law No. 1 of 2023 on the Criminal Code offers new hope for supporting adaptive law enforcement.

Law No. 1 of 2023 represents an effort to decolonize the old Criminal Code. Under the new Criminal Code's provisions on fraud, the criminal act is still categorized as a property crime, emphasizing deception and abuse of trust. It is reinforced by relevant adjustments to the social, economic, and technological context (Harefa & Bakhtiar, 2025). This bridge of reform is further solidified by the enactment of the New Law No. 20 of 2025, which emphasizes strengthening standards for the protection of suspects' rights, establishing more precise evidentiary parameters, and fully legitimizing the use of electronic evidence in judicial proceedings (Nugraha, 2025). This is particularly crucial in addressing "triangle scheme" fraud cases, where the criminal trail is largely digital, thereby ensuring greater legal certainty in the evidentiary process.

To overcome these obstacles, the main strategy and its implementation must focus on two pillars: progressive (repressive) law enforcement and the strengthening of the digital ecosystem (preventive).

a. Repressive Implementation. Law enforcement's competence in digital forensics must be strengthened to ensure a valid, indisputable chain of custody for electronic evidence. This requires an Integrated Task Force comprising the Police, PPATK, and the Ministry of Communication and Digital Affairs to eliminate bureaucratic hurdles and track illegal fund flows in real-time.
b. Preventive Implementation: Strategic measures must go beyond digital literacy to include corporate accountability. Banking institutions and digital platforms must tighten Know Your Customer (KYC) and Customer Due Diligence (CDD) protocols. Furthermore, automated oversight of account openings and transaction anomalies is essential to prevent accounts from being misused for money laundering.

By properly classifying problems and implementing strategies that combine law enforcement's forensic capabilities with systemic banking compliance, the eradication of "triangle scheme" fraud can proceed comprehensively and ensure legal certainty for the public.

4. CONCLUSION

Based on the entire discussion above, it can be concluded that the application of Article 378 of the Criminal Code in the Surabaya District Court Decision No. 2051/Pid.B/2025/PN. Sby has legally and precisely satisfied all elements of the offense of fraud. The causal link between the Defendant's *mens rea*, the manipulative instrument in the form of the *test drive* pretext, and the victim's property loss has been absolutely proven. This conventional criminal framework is also identified as remaining essentially relevant within the framework of Law No. 1 of 2023.

Nevertheless, this study makes a scientific contribution by exposing the dogmatic weaknesses of the judiciary (*judicial blind spots*) that reductively disregard the provisions of the ITE Law, even though the orchestration of the "triangular scheme" crime was purely carried out through electronic means. As a novel concept and *policy recommendation*, this research emphasizes that the complexity of cybercrime cannot be addressed in isolation. Future law enforcement demands a reconceptualization through two integrated pillars: normative synchronization involving the application of layered charges (the Criminal Code and the ITE Law) by public prosecutors as a screening instrument, and systemic strengthening through the acceleration of law enforcement's digital forensic capabilities, accompanied by stricter institutional compliance (*Know Your Customer*) in the banking sector and digital platforms.

REFERENCES

Agustina, S. (2015). Implementasi Asas Lex Specialis Derogat Legi Generali dalam Sistem Peradilan Pidana. *Masalah-Masalah Hukum*, *44*(4), 503–510.

Ahmad Usfa, F. (2006). *Pengantar Hukum Pidana: Cetakan Kedua* (Edisi Revisi). UMM Press.

Al Miski, Y. R., Putra, S. M., Purwanto, M. I., & Luthfiyyah, S. (2025). Eksistensi Tindak Pidana Penipuan (Bedrog) dalam Pasal 378 KUHP di Era Digital. *Journal Equitable*, *10*(2), 369–389.

Alamri, H. (2017). Kedudukan Keterangan Ahli Sebagai Alat Bukti Menurut Kitab Undang-Undang Hukum Acara Pidana. *Lex Privatum*, *5*(1), 149418.

Amri, W. M. (2021). Perbuatan Melawan Hukum Materiil Berfungsi Positif dan Berfungsi Negatif dalam Tindak Pidana Korupsi. *Kajian Hukum*, *6*(2), 35.

Andi Marlina, & Nur Alim Rachim. (2026). *Tindak Pidana Penipuan Berbasis Elektronik*. Penerbit KBM Indonesia.

Angraeni, M., & Arifin, T. (2023). Penggandaan Uang dalam Perspektif Pasal 378 KUHP dan Hadits Riwayat Imam Muslim. *Al-Rasīkh: Jurnal Hukum Islam*, *12*(2), 129–146.

Arifudin, N., Jufrin, J., Asriyani, A., Narwadan, T. N. A., Pusvita, D. E., Abqa, M. A. R., Satrul, H. S., Syarif, M., Rohayati, A. C., & Hermawan, I. A. (2024). *Pengantar Ilmu Hukum*. CV. Gita Lentera.

Aziz, N. M. (2012). Urgensi Penelitian dan Pengkajian Hukum dalam Pembentukan Peraturan Perundang-Undangan. *Jurnal Rechtsvinding: Media Pembinaan Hukum Nasional*, *1*(1), 208. https://doi.org/http://dx.doi.org/10.33331/rechtsvinding.v1i1.104

Azmi, I. (2024). Yurisprudensi Sebagai Sumber Hukum Tidak Tertulis: Analisis dalam Sistem Hukum Indonesia. *Yudhistira: Jurnal Yurisprudensi, Hukum dan Peradilan*, *2*(1), 46–54.

Chaerunnisa, R., & Fadlian, A. (2022). Analisis Yuridis Tindak Pidana Penipuan Atas Tipu Muslihat Terhadap Pekerja Seks Komersial Berdasarkan Pasal 378 Kuhp Tentang Tindak Pidana Penipuan. *Jurnal Ilmiah Wahana Pendidikan*, *8*(15), 487–498.

Chandra, T., Munawar, A., & Aini, D. M. (2024). Tinjauan Yuridis Terhadap Mekanisme Penyelidikan pada Tindak Pidana Penipuan Melalui Media Transaksi Elektronik oleh Kepolisian dalam Sistem Peradilan Pidana di Indonesia. *Rewang Rencang: Jurnal Hukum Lex Generalis*, *5*(7), 3. https://jhlg.rewangrencang.com/

Dewi, S. O., & Yuliawan, I. (2025). Pertanggungjawaban Pidana dalam Kasus Penipuan Investasi Bodong: Analisis Pasal 378 KUHP. *J-Ceki: Jurnal Cendekia Ilmiah*, *4*(5), 2899–2906.

Erawan, Y. M., Arinurdin, N., & Yuliandy, M. D. (2026). Tantangan Pembuktian Kejahatan Siber (Cybercrime) dalam Peradilan Pidana. *Al-Zayn: Jurnal Ilmu Sosial & Hukum*, *4*(2), 3069–3075.

Fauzi, S. N. (2018). Tindak Pidana Penipuan dalam Transaksi di Situs Jual Beli Online (E-Commerce). *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan*, *7*(3), 250–261.

Fernando, Y., & Wasiska, A. (2023). Tindak Pidana dan Unsur-Unsurnya Versus Deelneming Delicten/Tindak Pidana Penyertaan Versus Pertanggungjawaban Tindak Pidana. *Manazir: Jurnal Ilmiah Universitas Ibnu Chaldun*, *1*(1), 57.

Hadjon, P. M., & Djatmiati, T. S. (2005). *Argumentasi Hukum (Legal Argumentation/Legal Reasoning)* (Cetakan Kedua). Gadjah Mada University Press.

Hapid, F. M., Suntana, I., & Royani, M. Y. (2024). Penerapan Asas Geen Straf Zonder Schuld dalam Penindakan Terhadap Kejahatan Penyalahgunaan Teknologi Deepfake. *Journal USM Law Review*, *7*(3), 1155–1174.

Harefa, B., & Bakhtiar, H. S. (2025). *Tindak Pidana*. Rajawali Pers.

Hasibuan, H. A. L., & Nst, A. H. (2023). Metode Penafsiran Hukum Sebagai Alat Mencari Keadilan Hakiki. *Journal Legisia*, *15*(2), 136–145.

Husna, S. U., Darmawijaya, E., & Fithria, N. (2025). Analisis Penetapan Hukuman Pidana Menurut Teori Pertanggungjawaban Pidana: (Studi Terhadap Putusan Nomor 234/Pid. Sus/2023/Pt Bna). *Parhesia*, *3*(1), 67–79.

Ihsan, M. (n.d.). Hambatan dalam Menangani Tindak Pidana Penipuan Melalui Media Sosial (Online) oleh Siber Dit Reskrimsus Polda Sumsel. *Rio Law Journal*, *2*, 2024–2722.

https://doi.org/10.36355/.v1i2

Keintjem, F. A., Elias, R. F., & Nachrawy, N. (2021). Konsep Perbarengan Tindak Pidana (Concurcus) Menurut Kitab Undang-Undang Hukum Pidana. *Lex Crimen*, *10*(5), 190–198.

Luis, L. (2021). Legalitas Ultra Petitum dalam Hukum Acara Pidana pada Putusan Pengadilan. *Jurnal Hukum Adigama*, *4*(2), 1630–1654.

Mardina, D. (2022). Penerapan Pasal 378 Kitab Undang-Undang Hukum Pidana dalam Penerbitan Bilyet Giro Kosong (Studi Kasus Putusan Nomor 291/PID. B/2014/PN. Yyk). *Constitutum: Jurnal Ilmiah Hukum*, *1*(1).

Mulyadi, H. D. (2017). Unsur-Unsur Penipuan dalam Pasal 378 KUHP Dikaitkan dengan Jual Beli Tanah. *Jurnal Universitas Galuh*, *5*(2), 209. https://doi.org/http://dx.doi.org/10.25157/jigj.v5i2.798

Munawaroh Nafiatul. (2025). Tips Terhindar dari Penipuan Mobil Skema Segitiga . *Hukum Online*. https://www.hukumonline.com/klinik/a/tips-terhindar-dari-penipuan-mobil-skema-segitiga-lt66a12b77d0258/

Nugraha, M. R. (2025). Jenis Alat Bukti Sah Menurut KUHAP Baru . *Hukum Online*. https://www.hukumonline.com/klinik/a/jenis-alat-bukti-sah-menurut-kuhap-baru-lt657ae25924ac9/

Nur, F. (2025). Pertanggungjawaban Pidana Terhadap Pelaku Tindak Pidana Penipuan Online Dengan Modus Social Engineering. *Innovative: Journal of Social Science Research*, *5*(4), 342–355. https://j-innovative.org/index.php/Innovative

Paluaran, D., Purwanda, S., Kasim, A., & Jumardin, J. (2024). Analisis Komparatif Tindak Pidana Penipuan dalam KUHP Kolonial dan KUHP Nasional. *Jurnal Litigasi Amsir*, *11*(3), 345–351.

Patrol Siber. (2025). *Jumlah Laporan Polisi Yang Dibuat Masyarakat*. https://patrolisiber.id/statistic/

Ponglabba, C. S. R. (2017). Tinjauan Yuridis Penyertaan dalam Tindak Pidana Menurut KUHP. *Lex Crimen*, *6*(6), 147158.

Purba, Y. Y. (2026). Penafsiran Pasal 378 KUHP tentang Tindak Pidana Penipuan dalam Konteks Ekonomi Digital. *Journal Minfo Polgan*, *15*(1), 86–94.

Putra, M. H. (2025). The Position of Customary Criminal Law in Law No. 1 of 2023 on the Criminal Code. *International Journal of Law and Society*, 170–179.

Sanjaya, A. W. (2024). *Ajaran Kesalahan dalam Hukum Pidana*. PT. Raja Grafindo Persada-Rajawali Pers.

Sofian, A. (2015). Kausalitas dalam Hukum Pidana pada Keluarga Civil Law dan Common Law. *Philosophy*, *71*, 605–616.

Sumenge, M. (2013). Penipuan Menggunakan Media Internet Berupa Jual-Beli Online. *Lex Crimen*, *2*(4), 3063.

Utoyo, M., Afriani, K., Rusmini, R., & Husnaini, H. (2020). Sengaja dan Tidak Sengaja dalam Hukum

Pidana Indonesia. *Lex Librum*, *7*(1), 75–85.

Wibisono, C. S., & Mahanani, A. E. E. (2023). Analisis Yuridis Terhadap Tindak Pidana Penipuan dalam Transaksi Elektronik Melalui Media Sosial (Twitter). *Jurnal Hukum, Politik dan Ilmu Sosial*, *2*(2), 21–30.

Wicaksana, P. B. (2026). *Hukum Pidana: Teori, Asas, dan Perkembangannya di Indonesia*. CV Eureka Media Aksara.

Wuisan, R. (2020). Kajian Hukum terhadap Tindakan Pidana dalam Perkembangan Hukum Pidana. *Jurnal Elektronik Bagian Hukum Pidana Fakultas Hukum Unsrat*, *9*(2), 181–189.

Yunita, F. (2023). Aspek Hukum Penggunaan Media Sosial Berbasis Internet. *Jurnal Notarius*, *2*(1).

Zamroni. (2026). Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Melalui Aplikasi Digital. In *(Doctoral dissertation, Universitas Islam Sultan Agung Semarang)*.