JILPR Vol. 8, No. 1 October 2026
Journal of Indonesia Law & Policy Review 2715-498X

IMPLEMENTATION OF LAW ENFORCEMENT IN TRIANGULAR FRAUD CRIMES

Eben Haezer Efrata Sembiring[1*], Miftahul Haq[2], Hasan Basri[3]
ebensembiring433@gmail.com[1*], haq1980.mh@unilak.ac.id[2], hasanbasriassociates@gmail.com[3]
Master of Laws Postgraduate Program, Lancang Kuning University, Pekanbaru, Indonesia[1,2,3]

Abstract

This study aims to analyze the implementation of law enforcement against triangular fraud within the jurisdiction of the Riau Regional Police and identify the obstacles encountered. Using a sociological legal research method, the findings show that law enforcement involves receiving reports, conducting investigations, collecting evidence, examining witnesses and suspects, tracing bank accounts and financial transactions, and resolving cases in accordance with applicable laws. The main challenges include identifying the actual perpetrators, obtaining electronic evidence, tracing funds transferred through third-party bank accounts, limited digital forensic capabilities, and unreported cases. These difficulties arise because perpetrators often use false identities and involve multiple parties to deceive buyers and sellers. To overcome these obstacles, investigators must strengthen investigative capabilities, improve digital forensic expertise, enhance coordination with banks and digital service providers, and increase public awareness and reporting services. Effective law enforcement requires identifying not only the individuals receiving the money or delivering goods but also the masterminds and other parties knowingly involved in organizing and carrying out the fraud.

Keywords: Law Enforcement, Criminal Offense, Triangular Fraud

INTRODUCTION

The phenomenon of triangular fraud in car sales transactions has become increasingly prevalent in Indonesia, especially since the development of vehicle buying and selling activities through online platforms. This fraud mode can be seen because it involves three parties who do not know each other: the original seller, the original buyer, and the fraudster as a third party who exploits the information gap between the two parties. The perpetrator tricks the seller into handing over the vehicle to another party (the buyer), while the payment never reaches the seller. In this situation, the buyer feels they have paid the fraudster, while the seller receives nothing because the transfer is made to the perpetrator's account. This case raises legal issues in both the criminal and civil realms, particularly regarding the status of car ownership, protection for victims, and the form of legal accountability for the perpetrator.

Transactions no longer always take place directly, but can be conducted through social media, messaging apps, marketplaces, or intermediaries. This situation makes it easier for people to obtain goods, but at the same time creates space for the emergence of fraudulent methods that exploit the limitations of communication and trust between the parties. One method that is developing is triangular fraud, namely an act involving at least three parties in which the perpetrator positions himself as a liaison or certain party in the transaction, even though his identity, position, legal relationship, or true intention do not match the circumstances disclosed to the victim (Arief, 2017). This pattern can cause the party handing over the money, the party handing over the goods, and the party receiving the benefits to be in different positions, making the relationship between the perpetrator, the victim, and the object of the transaction more difficult to trace.

Fraud is a crime against assets that is essentially committed through the use of a false name or position, trickery, or a series of lies to induce another person to hand over goods, grant debt, acknowledge debt, or write off receivables (Chazawi, 2011). Since January 2, 2026, these general criminal provisions have been included in Law Number 1 of 2023 concerning the Criminal Code, specifically Article 492, which regulates the crime of fraud. The explanation of Article 492 also explains that the goods handed over by the victim do not have to be given directly to the perpetrator, but can be given to another person instructed by the perpetrator to accept the transfer. This provision is relevant to the triangular fraud pattern because in this mode the perpetrator can arrange for money or goods to be transferred to another party as part of the series of actions.

From a law enforcement perspective, the primary issue in triangle fraud is not simply determining whether a loss has occurred, but rather proving the relationship between the perpetrator's actions and the occurrence of that loss. Investigators must be able to explain how communication between the parties took place, who provided the initial information, who used a particular identity or position, to whom the money or goods were handed over, and whether there was an intention from the outset to unlawfully benefit oneself or others (Moeljatno, 2015). Therefore, proof is not sufficient based solely on the existence of a transaction and loss, but must be directed at constructing a series of actions that fulfill the elements of the crime of fraud. The official explanation of the National Criminal Code emphasizes the existence of a causal relationship between the means used by the perpetrator and the victim's act of handing over something desired by the perpetrator.

The nature of triangle fraud becomes even more complex when it occurs in motor vehicle sales transactions. In such transactions, one party may act as the prospective buyer, the second party as the vehicle owner, while the perpetrator acts in between, presenting himself as having authority or a specific relationship with the vehicle or the transaction. The perpetrator may direct payments to a specific account, arrange communication between the parties, or assume the identity of another party, leaving each victim with a different understanding of their counterparty after the transaction. This complexity impacts the

investigation and prosecution process, as law enforcement must distinguish between civil relations arising from failure to fulfill an agreement and acts that have involved deception or a series of lies from the outset.

The distinction between civil disputes and criminal acts is crucial in law enforcement practices against triangular fraud. Not every transaction that fails or results in a loss automatically constitutes a criminal act of fraud (Hamzah, 2016). The existence of an agreement, outstanding payment, late delivery of goods, or cancellation of a transaction must first be examined in terms of the legal relationship. Conversely, if a transaction is constructed from the outset through false identities, deliberately falsified information, deception, or a series of lies that induce the victim to hand over money or goods, then the matter can fall under the criminal realm. Court decisions also demonstrate the importance of distinguishing between civil and criminal aspects by examining the presence or absence of elements of deception or deception in the transaction.

In the current context of positive law, the transition from the old Criminal Code to the National Criminal Code is also a crucial element in research on triangular fraud. Law No. 1 of 2023 concerning the Criminal Code came into effect on January 2, 2026, and regulates fraud under Article 492, while Article 493 specifically regulates sellers who deceive buyers regarding delivered goods. Furthermore, Law No. 1 of 2026 concerning Criminal Adjustments was issued to align criminal provisions in various regulations with the National Criminal Code. These changes require law enforcement officials to ensure the application of criminal norms in accordance with the legal regime in force at the time the case is handled.

This issue is particularly relevant to law enforcement within the jurisdiction of the Riau Regional Police. The Riau Regional Police, as part of the Indonesian National Police, has the function of investigating and investigating alleged criminal acts, in accordance with the authority granted by criminal procedure law. In the triangular fraud case, the implementation of this function faces a case that is not always simple because a single incident can involve multiple accounts, telephone numbers, social media accounts, vehicle documents, transfer receipts, electronic conversations, and parties with different positions in a transaction. Therefore, the effectiveness of law enforcement is closely related to the investigator's ability to construct a case based on evidence and the interconnected roles of each party.

Beyond the issue of proof, handling triangular fraud also relates to victim protection. The victim in this scheme is not always a single person. The party who loses money may be different from the party who loses a vehicle or goods, while the party whose name is used in the transaction may also suffer losses due to misuse of their identity. This situation requires investigators to accurately identify the status of each party to avoid errors in determining who is a victim, who is a witness, and who deserves criminal responsibility. This determination is crucial because the construction of a criminal case must be based on concrete actions and a causal relationship between the perpetrator's actions and the losses suffered by the other party.

In practice, handling fraud cases can also face challenges when the perpetrator uses a third party to receive money or goods. The explanation of Article 492 of the National Criminal Code explicitly states that the delivery of goods in a fraud crime does not have to be made directly to the perpetrator, but can be made to another person instructed by the perpetrator to receive the delivery. Therefore, the fact that the money or goods are not directly transferred to the perpetrator's account or control does not automatically eliminate the possibility of criminal liability. The legal issue lies in proving the relationship between the main perpetrator and the party receiving the delivery, as well as the knowledge and role of each in the series of actions.

From a criminal law perspective, the characteristics of triangular fraud indicate the use of deception and a series of false statements to induce another party to hand over money or

goods. In the legal context that has been in effect since January 2, 2026, this act can be analyzed under Article 492 of Law Number 1 of 2023 concerning the Criminal Code if all elements of the crime are met. This provision regulates acts committed with the intention of unlawfully benefiting oneself or another person through the use of a false name, false position, deception, or a series of false statements to induce someone to hand over goods, grant debt, acknowledge debt, or write off receivables. If the act occurred before the enactment of the National Criminal Code, the application of the criminal provisions must take into account the time of the crime, transitional provisions, and applicable criminal law principles.

According to the author's analysis, triangle fraud presents a different level of complexity than conventional fraud because the perpetrators do not always have direct contact with the party handing over the money or goods as the true owner. Instead, the perpetrators establish different communication relationships with each victim, creating perceptions that are inconsistent with the actual situation. This issue can complicate the evidentiary process because investigators must thoroughly describe the communication relationships, transaction agreements, recipient account identities, money transfers, and the roles of each party. Investigators must not only prove that the victim transferred the money but also uncover who controlled the transaction, who created the false information, who benefited from the proceeds of the crime, and how the series of actions led to the losses.

According to the author, the most important issue in law enforcement against triangle fraud is the possibility of errors in determining the legal standing of the parties. In practice, sellers and buyers may both consider the other party to be the perpetrator because each feels they have carried out the transaction correctly. In fact, the account holder who receives the funds is not necessarily the main perpetrator because the account could be used or controlled by someone else. Therefore, investigators must distinguish between the main perpetrator, co-conspirators, assisters, victims, and parties whose accounts are only used in the series of crimes. Determining criminal responsibility must be based on evidence and the actual involvement of each party, not solely on the basis of their names appearing on the transfer receipt.

From the government's perspective, the existence of the triangular fraud scheme demonstrates that the development of digital transactions must be accompanied by strengthened oversight, prevention, and law enforcement. The government, through the police, particularly the Riau Regional Police, needs to improve its investigative capabilities for crimes involving electronic means, including tracing recipient accounts, analyzing digital communications, collecting electronic evidence, and coordinating with online trading platform providers and financial institutions. In addition to enforcement, preventative measures must also be implemented through public education on the importance of verifying the identities of sellers and buyers, checking the conformity of account holder names, and prohibiting payments to parties whose identities and authority have not been confirmed.

The author argues that addressing triangle fraud cannot simply rely on public warnings to be cautious when conducting online transactions. The government needs to ensure that every public report is followed up through a professional, transparent legal process that provides legal certainty to victims. Furthermore, collaboration between the police, banks, electronic system providers, and relevant agencies is needed to expedite the tracing of fund flows and identify those controlling accounts and communications in these transactions. This step is crucial because perpetrators can exploit differences in regional boundaries, digital identities, and the use of third-party accounts to hinder the investigation process.

This situation demonstrates the need to examine the implementation of law enforcement against triangular fraud, specifically within the Riau Regional Police. The research is not only directed at examining whether public reports are followed up, but also

how investigators identify triangular fraud, determine the structure of the crime, collect and evaluate evidence, determine the responsible parties, and address obstacles in the investigation process. With this approach, the research can illustrate the relationship between the legal provisions that should be applied (das sollen) and the implementation of law enforcement that occurs in practice (das sein). The research focuses on the implementation of law enforcement against fraud involving more than two parties, specifically regarding the case handling process, the application of criminal provisions, proving the perpetrator's involvement, and the obstacles faced by investigators.

Based on the description of the background of the problem above, the main problem can be formulated as follows: 1. How is law enforcement carried out in the case of triangular fraud at the Riau Regional Police? 2. What are the obstacles in implementing law enforcement in the crime of triangular fraud at the Riau Regional Police? 3. How are the efforts to overcome obstacles in implementing law enforcement in the crime of triangular fraud at the Riau Regional Police?

RESEARCH METHODS

This research uses sociological legal research or empirical legal research, namely research that examines the implementation of law in the reality of society, specifically law enforcement against the crime of triangular fraud in the jurisdiction of the Riau Regional Police. The approaches used include a statutory approach to examine the legal provisions of the crime of fraud, a conceptual approach to understand the concept of triangular fraud and law enforcement, and an analytical approach to connect legal provisions with facts found in the field.

Data sources consist of primary data obtained through interviews and observations, secondary data in the form of books, journals, and laws and regulations, and tertiary data in the form of dictionaries, encyclopedias, and other supporting reference materials. Data collection was conducted through field observations, unstructured interviews with respondents, and a literature review of literature and laws and regulations related to the research problem.

Data were analyzed qualitatively by systematically describing the results of interviews, observations, and document studies, then connecting them with legal provisions and law enforcement theory to answer the research questions. Conclusions were drawn using an inductive method, namely drawing conclusions from specific facts obtained through field research to general conclusions regarding the implementation of law enforcement, obstacles, and efforts to handle triangular fraud crimes at the Riau Regional Police.

RESULT AND DISCUSSION

A. Implementation of law enforcement in the crime of triangular fraud in the jurisdiction of the Riau Regional Police

The development of information technology has changed the patterns of interaction among people in conducting economic activities, including the sale and purchase of goods and services. Transactions that previously required sellers and buyers to meet in person can now be conducted through social media, messaging apps, and e-commerce platforms. This convenience offers benefits in terms of time efficiency, cost savings, and marketing reach. However, the ease of communication without physical meetings also creates opportunities for individuals to commit crimes by exploiting people's ignorance, trust, and limited ability to verify the identities of transacting parties. Maskun explained that the development of information technology not only provides convenience in people's lives but also gives rise to new forms of crime with characteristics that differ from conventional crimes, primarily because perpetrators can utilize communication networks and disguise their identities in the

digital space.(Maskun, 2022).

One type of crime that exploits this situation is the triangle fraud. This type of fraud involves three main parties: the perpetrator acting as a fake intermediary, the actual seller of the goods, and the potential buyer who becomes the victim. The perpetrator exploits the communication relationship between the seller and the buyer by creating the impression that he or she has a legitimate relationship or authority in the transaction. However, the perpetrator does not have the legal relationship to act as an intermediary or owner of the goods. The goal of this act is to control the transaction process so that payment or delivery of goods occurs based on deliberately manipulated information.

In practice, fraudsters typically seek out genuine sellers' product advertisements published on social media or online shopping apps. Photos, specifications, prices, and other information about the items are then reused without the owner's consent to create new advertisements. Fraudsters may offer items at lower prices to attract potential buyers. When buyers contact fraudsters, they pose as the owner of the item or a party related to the seller. Simultaneously, fraudsters contact the genuine seller, claiming to be the prospective buyer or the party who will arrange the transaction. Thus, each party receives different information and is unaware that their communications are actually controlled by the same person.

This situation makes the transaction appear to be proceeding normally, even though the identity and true intentions of the perpetrator are manipulated. The buyer believes they have made payment to the rightful recipient, while the seller believes the goods have been delivered to the actual purchaser. After the goods are delivered and the money is received into the perpetrator's designated account, the perpetrator cuts off communication and eliminates any trace. As a result, the buyer loses money, while the seller may lose the goods or face lawsuits from the buyer because the payment received does not correspond to the actual transaction.

Triangle fraud is not simply a failed transaction, but rather a pattern of behavior that can be designed to control another party's assets through a series of lies. R. Soesilo (1995) in his explanation of the crime of fraud explains that fraud is related to the act of persuading someone to hand over goods, create debt, or write off receivables with the intention of obtaining illegal profits through the use of false names, false circumstances, tricks, or lies. This idea is relevant to understanding triangle fraud because the perpetrator builds trust through false identities and information so that the victim is willing to hand over money or goods.

Judging from the structure of the act, there are several important characteristics of triangle fraud. First, there is a relationship between three parties with different interests, but not all of them are aware of the existence and roles of the others. Second, the perpetrator uses false identities, positions, or information to build trust. Third, there is communication manipulation aimed at controlling the decisions of sellers and buyers. Fourth, there is the diversion of payments or goods through a pre-planned mechanism. Fifth, the perpetrator has the intent to gain unlawful profit.

Thus, the term "triangular fraud" is more accurately understood as a modus operandi or method of committing a crime, rather than as a separate crime with specific criminal formulations. Determining criminal liability must still be based on applicable criminal law and proving the elements of the act, culpability, and intent of the perpetrator. The use of intermediary services in buying and selling transactions is not prohibited as long as it is conducted legally, transparently, and based on the consent of the parties involved.

Triangle fraud is an act that can cause harm to a person's legal interests, particularly their right to property. Therefore, its handling must be based on criminal law provisions that prohibit the unlawful acquisition of profit through deception or a series of lies. In the Indonesian criminal law system, the primary basis for assessing such acts is the provisions

concerning the crime of fraud in Law Number 1 of 2023 concerning the Criminal Code.

Article 492 of the National Criminal Code regulates the actions of a person who, with the intention of unlawfully benefiting themselves or another person, uses a false name, false position, deception, or a series of lies to induce another person to hand over goods, grant a loan, acknowledge a debt, or write off a receivable. This provision provides the basis for assessing whether the series of actions carried out in a triangular fraud fulfills the elements of the crime of fraud.

When associated with triangle fraud, using the identity of the goods owner, intermediary, or authorized recipient of payment can be part of the use of a false name or position. Similarly, the use of fake advertising, false product information, and payment account arrangements can be part of a ruse or series of lies. However, investigators must still prove that the act was committed with the intent to gain unlawful gain and actually persuaded the victim to hand over the money or goods.

R. Soesilo (1995) emphasized that in a criminal act of fraud, there must be an intention to gain profit by unlawful means and an act of persuading the victim through fraudulent means as defined in the crime formulation. Based on this understanding, the element of intent and the relationship between the deception and the transfer of assets are important elements in the proof. It is not enough to simply prove that someone received money from the victim; a connection must be found between the misleading act and the victim's decision to transfer their assets.

In addition to the National Criminal Code, the use of electronic means in triangular fraud also needs to be analyzed based on Law Number 11 of 2008 concerning Electronic Information and Transactions as last amended by Law Number 1 of 2024. Article 28 paragraph (1) regulates the prohibition on distributing and/or transmitting electronic information or electronic documents containing false notifications or misleading information that results in material losses for consumers in electronic transactions. The criminal provisions are contained in Article 45A paragraph (1).

In the context of triangular fraud, these provisions may be considered if the perpetrator disseminates false advertisements or misleading information through electronic media and all the elements specified in the article are met. However, the application of these provisions must be carried out carefully. Not every fraud using WhatsApp, Facebook, Instagram, or buying and selling applications automatically meets the elements of Article 28 paragraph (1). The victim's status as a consumer, the nature of the information disseminated, the element of intent, and material losses must be proven based on the circumstances of the case.

In their study on law enforcement against electronic fraud, I Gusti Made Jaya Kesuma, Ida Ayu Putu Widiati, and I Nyoman Gede Sugiartha (2020) explained that electronic fraud essentially shares elements with conventional fraud, but utilizes electronic technology as a means of carrying out the act. The study also emphasized the importance of aligning criminal provisions with the proven elements of the act. This understanding demonstrates that the use of technology does not eliminate the fundamental character of fraud as a crime against property, but rather adds complexity to the evidence and investigation of perpetrators.

Furthermore, criminal liability for the parties involved must be determined based on their roles and culpability. In a triangle fraud, not all parties involved in the transaction can be directly categorized as perpetrators. The account holder who receives the money, for example, must be questioned regarding their knowledge and involvement in the criminal act. If someone intentionally provides the account, controls the receipt of money, or assists the perpetrator in diverting the proceeds of crime, their involvement can be analyzed under the provisions of participation or assistance in the National Criminal Code. Conversely, someone whose account is used without knowledge and intent cannot be held accountable simply because their name is listed as the account holder.

Therefore, the application of criminal law to triangular fraud must prioritize individual evidence against each individual suspected of involvement. This approach is necessary so that law enforcement can not only successfully identify the recipients of the funds but also uncover those who planned, controlled, and profited from the crime.

Law enforcement against the triangle fraud crime within the Riau Regional Police jurisdiction is part of the police's responsibility to protect the public from crimes that exploit advances in information technology. Law enforcement in this case involves not only applying criminal provisions to the perpetrators but also encompasses the officers' ability to identify the modus operandi, gather evidence, uncover the relationships between the parties, and provide legal certainty to the victims.

In fact, the Riau Regional Police have raised concerns about the triangle fraud scheme by warning the public about the risks of online transactions. An official Riau Police report on July 19, 2025, illustrated the perpetrator's modus operandi, exploiting a genuine seller's vehicle advertisement and then offering the item to potential buyers at a lower price. The perpetrator then manipulates communication between the two parties so that payment is made based on information controlled by the perpetrator.(Maskun, 2022). This report can be used as a description of the modus operandi that has attracted police attention in Riau Province, but it cannot be treated as statistical data on the number of cases handled.

In its implementation, law enforcement against triangular fraud needs to be viewed through several interrelated stages as follows.

1. Receipt of reports and identification of criminal incidents

   The initial stage of law enforcement begins with receiving reports from members of the public who feel they have been harmed by a purchase or sale transaction suspected of being fraudulent. Victims can report the incident to the police by providing initial evidence, such as email conversations, screenshots of advertisements, proof of transfers, account numbers, telephone numbers, and the identity of the account used in the transaction.

   At this stage, officers must obtain detailed information regarding the initial transaction, the communication between the parties, the party providing the account number, the amount transferred, and the circumstances after payment. The initial investigation should be directed at determining whether a third party is controlling communication between the seller and buyer.

   Handling reports of triangle fraud requires careful attention because the reporting party may not fully understand who the actual perpetrator is. For example, a buyer may report a legitimate seller because they believe they have transferred the money, while the legitimate seller may feel they haven't received the legitimate payment. In such circumstances, investigators need to examine both parties equally to determine whether they are both victims of the perpetrator manipulating the transaction.

2. Investigation into alleged criminal acts

   After receiving the report, the police conducted an investigation to obtain clarity regarding the incident. The investigation focused on identifying the parties involved, the accounts used, communication history, and the relationship between the transactions and the victim's losses.

   Investigations also serve to distinguish acts that truly involve elements of fraud from civil matters. Failure to fulfill a contractual obligation does not automatically constitute a criminal offense. Facts must be established that demonstrate deception, deception, or the use of a false identity with the intent to gain unlawful gain.

   In this regard, Budi Suhariyanto (2012) explains that the development of information technology crimes presents new challenges for law enforcement because criminal acts can be committed through electronic systems, while the perpetrator and

victim are not always in the same location. Therefore, investigations into triangle fraud need to consider the relationship between digital activities and the transfer of money or goods.

3. Investigation and collection of evidence

   If a suspected crime is discovered, investigators will conduct an investigation in accordance with the applicable Criminal Procedure Code (KUHAP). The purpose of the investigation is to shed light on the criminal incident and identify those who can be held criminally responsible.

   In a triangle scam, investigators must gather evidence that explains how the perpetrators construct a series of lies, control communications, determine payment accounts, and profit from the transactions. Electronic evidence plays a crucial role because most of the perpetrators' actions are conducted via communication devices and the internet.

   In his study of telematics law, Edmon Makarim positions electronic information and documents as a crucial part of the legal relationships evolving through the use of information technology. This demonstrates the need to understand the nature of digital information in the evidentiary process so that the evidence obtained can be properly assessed based on the law.(Suhariyanto, 2012). Forms of evidence that can be collected in triangular fraud cases include:

   a. A conversation between a seller and a buyer containing an offer of goods and payment instructions.
   b. Conversation between the perpetrator and the original seller showing the identity disguise.
   c. Original ads and imitation ads that use the same photos and product descriptions.
   d. Proof of transfer and financial transaction documents.
   e. Phone numbers, social media accounts, email addresses, and digital identities used.
   f. Information from the buyer, original seller, account owner, and other witnesses.
   g. The results of the digital forensic examination relating to the devices, accounts, and communications used by the perpetrator.

   Evidence collection must consider authenticity, integrity, relevance, and the validity of the method of acquisition. Screenshots should not be considered direct proof of the perpetrator's identity, as accounts or phone numbers can be used by others. Therefore, digital evidence must be verified and linked to witness statements and transaction documents.

4. Account and cash flow tracking

   Tracing the flow of funds is a crucial part of uncovering triangle fraud. Perpetrators often don't use accounts in their own names, but instead use other people's accounts to receive money from victims. Investigators must determine who owns the account, who controls access to the account, who directs the payments, and where the money is diverted once received.(Maskun, 2022).

   Investigators need to distinguish between individuals who are merely registered account holders and those who are knowingly involved in criminal activity. Investigations can focus on transaction history, communications regarding account use, the relationship between the account holder and the perpetrator, and the profits each party obtained. Banking information requests must be conducted in accordance with applicable legal authorities and procedures.

   From a law enforcement perspective, tracing the flow of funds is necessary not only to identify the initial recipient but also to uncover the possibility of a network of interconnected recipients. If money is transferred to multiple accounts, investigators must trace the connection of each transaction to the crime under investigation.

5. Examination of witnesses and determination of the roles of each party

   Witness examination is crucial in uncovering the triangle fraud scheme. The genuine seller can provide information regarding their communication with the party claiming to be the buyer. The buyer can explain the bidding process, the reason for the payment, and the account provided. Meanwhile, the account holder needs to be questioned regarding the origin of the transaction and their relationship with the party directing the payment.(Maskun, 2022).

   The parties' statements must then be compared with electronic evidence and transaction documents. Investigators must establish a consistency between the communication sequence, the movement of funds, and the delivery of goods. A thorough investigation can help determine whether both the seller and the buyer were victims of the fraud.

   Determining each person's role is also necessary to prevent misrepresentation of suspects. Someone who receives money is not necessarily the mastermind of the fraud. Conversely, someone who does not directly receive money can still be held accountable if proven to have intentionally committed or assisted in the commission of a crime under criminal law.
6. Case filing and coordination with the public prosecutor

   After obtaining the necessary evidence and information, investigators compile a case file in accordance with criminal procedure law. The file must systematically explain the acts committed, the identities of the parties being questioned, the relationship between the evidence, the elements of the crime applied, and the consequences for the victim.(Kesuma et al., 2020).

   Coordination with the public prosecutor is necessary to ensure that the case construction and application of the articles align with the facts. In triangular fraud cases, thorough filing is crucial because there may be more than one party involved with different roles. Investigators must be able to explain the rationale for applying Article 492 of the National Criminal Code and, where relevant, the provisions of the ITE Law based on the fulfillment of each element.
7. Protection and recovery of losses for victims

   Law enforcement is not only aimed at imposing penalties on perpetrators, but must also consider the interests of victims. Victims of triangle fraud have the right to receive good service, certainty regarding the progress of their reports, and information regarding available recovery mechanisms.(Soesilo, 1995).

   Restitution of losses can be achieved through available legal mechanisms based on the circumstances of the case and applicable provisions. However, returning money to the victim does not automatically eliminate criminal liability if the elements of the crime have been met. Therefore, the interests of victim restitution and the criminal accountability process must be balanced.

Based on this description, law enforcement against triangle fraud within the Riau Regional Police jurisdiction requires a comprehensive approach. The success of a case is measured not only by receiving a report or naming a suspect, but also by the investigator's ability to identify the perpetrators controlling the scheme, prove the involvement of each party, and provide legal protection to the victim.

To analyze the implementation of law enforcement against triangular fraud crimes in the jurisdiction of the Riau Regional Police, the theory of law enforcement effectiveness proposed by Soerjono Soekanto (2014) can be used. This theory explains that the success of law enforcement is influenced by five factors: legal factors, law enforcement factors, facilities or infrastructure factors, community factors, and cultural factors. These five factors are interrelated and cannot be separated in assessing the effectiveness of a law enforcement

system.

a. Legal factors

Legal factors relate to the substance of the laws and regulations that serve as the basis for handling criminal acts. In the triangle fraud, Article 492 of the National Criminal Code provides a basis for assessing acts that use false identities, deception, or a series of lies to obtain unlawful benefits. Meanwhile, the provisions of the Electronic Information and Transactions Law can be applied if the act fulfills the elements of disseminating false or misleading information that results in material losses for consumers in electronic transactions.

The issue that needs attention is not simply the availability of regulations, but rather the accuracy of authorities in applying legal provisions based on the facts found. Investigators must be able to distinguish between fraud, breach of contract, and other possible criminal acts that arise in a single sequence of events. Implementing articles that do not align with the facts can create legal uncertainty and hinder the evidentiary process.

b. Law enforcement factors

Law enforcement factors relate to the quality of the human resources carrying out the law enforcement process. In triangular fraud cases, investigators require the ability to understand criminal law, criminal procedure, electronic transactions, digital evidence examination, and fund flow tracing.

These skills are necessary because perpetrators don't always use their real identities and can control communications through multiple accounts. Investigators must be able to link electronic evidence with witness statements and financial transactions. In addition to technical skills, professionalism, integrity, thoroughness, and objectivity are also crucial factors in ensuring case handling avoids errors in determining who is responsible.

c. Facilities and infrastructure factors

Facilities and infrastructure factors include the availability of technological devices, digital forensic laboratories, information systems, expert personnel, and supporting facilities for the investigation process. Handling triangular fraud requires the ability to secure and analyze electronic data from various sources.

Limited digital auditing capabilities and equipment can impact the speed of case resolution. Therefore, improving information technology facilities and digital analysis capabilities is a crucial requirement for the police, especially when handling cases involving multiple accounts, phone numbers, and interconnected accounts.

d. Community factors

The public plays a crucial role in assisting the law enforcement process, whether as victims, witnesses, or information providers. The public's willingness to report crimes and preserve evidence of communications will help investigators obtain the information they need.

However, some people still don't report incidents immediately due to embarrassment, fear, or the perceived insignificance of the loss. Some victims also erase communication with the perpetrator, making it difficult to obtain initial evidence. Therefore, it is necessary to increase public awareness of the importance of reporting and securing evidence from the onset of a suspected crime.

e. Cultural factors

Cultural factors relate to a society's customs, values, and behavioral patterns in transactions. The habit of making payments based on trust without verifying the identity of the seller, the recipient, or the authenticity of the goods can open up opportunities for fraud.

The public needs to develop more cautious and responsible transaction habits. Trust in buying and selling relationships remains essential, but it must be accompanied by

identity verification and certainty about the recipient of payment. These changes in behavior can help reduce opportunities for perpetrators to exploit vulnerabilities in electronic transactions.

Based on these five factors, the effectiveness of law enforcement against triangle fraud in the Riau Regional Police region must be viewed holistically. Adequate regulations will not yield optimal results without the support of competent officers, technological facilities, public participation, and a strong legal culture. Therefore, Soerjono Soekanto's theory provides the analytical basis that improving law enforcement cannot be achieved simply by implementing criminal sanctions but must be accompanied by improvements.

Optimizing law enforcement against triangle fraud within the Riau Regional Police jurisdiction must be implemented through an integrated approach that combines enforcement, strengthening digital evidence, institutional coordination, and prevention. The success of law enforcement is measured not only by the number of perpetrators prosecuted, but also by the authorities' ability to identify the main perpetrators, mitigate public losses, and provide certainty and legal protection to victims.

B. Obstacles in implementing law enforcement in the crime of triangular fraud in the jurisdiction of the Riau Regional Police

Law enforcement against triangular fraud crimes within the jurisdiction of the Riau Regional Police faces various obstacles related to developments in information technology, communication patterns between parties, the use of false identities, and financial transaction mechanisms. Triangle fraud differs from conventional fraud in that the perpetrators do not always have direct contact with the victims. Instead, the perpetrators exploit the relationship between the seller and the buyer to create the appearance of a legitimate transaction. As a result, the injured party cannot always identify the actual perpetrator.

This problem presents a challenge for investigators because uncovering a crime is not sufficient simply by identifying the recipient of the money or the delivery of the goods. Investigators must be able to identify the individuals who devised the fraud scheme, controlled communications, directed payments, and profited from the act. Maskun (2022) explains that cybercrime has specific characteristics, including the use of information technology as a means of committing the crime, the disguise of identity, and the possibility of criminal acts that transcend geographical boundaries.

In the context of law enforcement, these obstacles need to be analyzed based on five factors that influence the effectiveness of law enforcement as stated by Soerjono Soekanto (2014): legal factors, law enforcement, facilities, society, and culture. These five factors can be used to identify issues that have the potential to hinder the handling of triangular fraud crimes in the jurisdiction of the Riau Regional Police. Forms of Obstacles in the Implementation of Law Enforcement

1. Difficulty in Revealing the Identity of the True Perpetrator

   The first obstacle is the difficulty of identifying the perpetrator. In triangle fraud, the perpetrator often uses different identities when communicating with the seller and the buyer. The perpetrator may claim to be the owner of the goods to the buyer, while simultaneously posing as a potential buyer to the original seller. Using these identities prevents each party from knowing they are dealing with the same person.

   Furthermore, perpetrators can use phone numbers not registered to their real identities, fake social media accounts, profile photos belonging to others, and specially created email addresses to conduct transactions. After successfully obtaining money or goods, perpetrators can delete accounts and cease communication, making tracking more difficult.

This issue requires investigators to conduct a thorough examination of the digital identities used. Tracing cannot be based solely on account names or phone numbers, but must also be linked to device information, communication history, transaction activity, and statements from the parties involved. Budi Suhariyanto (2012) explains that the characteristics of information technology crimes allow perpetrators to disguise their identities and exploit electronic systems, requiring investigative skills that are in line with technological developments.

2. The Difficulty of Obtaining and Proving Electronic Evidence

Another obstacle is the difficulty in obtaining complete and legally accountable electronic evidence. Most triangular fraud schemes take place through messaging apps, social media, and online shopping platforms. The only evidence victims typically have is screenshots of conversations, photos of items, sales advertisements, and proof of transfers.

Problems arise when the perpetrator's account has been deleted, chat messages have been deleted, or the phone number used is no longer active. This situation can make it difficult for investigators to reconstruct communication between the perpetrator, seller, and buyer. This communication is crucial for proving the existence of deception and a series of lies.

Edmon Makarim (2003) explains that developments in information technology have given rise to legal issues concerning the validity, authenticity, and evidentiary power of electronic information and documents. Therefore, the examination of electronic evidence must consider aspects of authenticity, integrity, and its relevance to the legal event being examined.

In triangle fraud cases, screenshots alone are not sufficient to assess the content of the conversation. Investigators also need to verify the source of the information, the relationship between the account and the person using it, the timing of the communication, and how the evidence matches the financial transactions. If electronic evidence is not obtained and carefully examined, there is a risk that the perpetrator's actions cannot be fully proven.

The use of third-party bank accounts is a significant obstacle in uncovering triangle fraud. Perpetrators often don't use their own accounts, but instead use other people's accounts to receive payments from victims. These accounts can be obtained through borrowing, renting, purchasing, or using them without the account holder's knowledge.

This situation makes it difficult to determine who should be held criminally responsible. The name listed on the account may not necessarily be the person controlling the transaction or orchestrating the fraud. In fact, the account holder may not even be aware that their account is being used to receive proceeds of crime.

Therefore, investigators need to investigate who controls the account, who issues payment instructions, who makes withdrawals or transfers, and who benefits from the transaction proceeds. Investigations should also focus on the communication between the account holder and the party using the account.

Budi Suhariyanto (2012) explains that the development of information technology-based crimes raises evidentiary issues that are not only related to the perpetrator's actions in the digital space, but also the relationship between electronic activities and their consequences in real life. In triangular fraud, this can be seen in the relationship between electronic communications, recipient accounts, and the delivery of goods to unauthorized parties.

Tracing the flow of funds becomes a particular challenge when the money received from the victim is immediately transferred to another account or withdrawn through a banking facility. The perpetrator may split the funds across multiple accounts to make it

difficult to trace the origin of the funds. In certain circumstances, the money may also be transferred through other electronic transaction services.

Investigators must be able to establish a link between the initial transfer evidence and subsequent transactions. Examination of the initial recipient's account must be followed by tracing subsequent transactions to identify who controls and benefits from the proceeds of crime.

Obstacles can arise if transaction information requires a formal request from a banking institution or financial services provider. Data requests must be executed based on applicable authorities and procedures, so investigators cannot obtain all information freely. If coordination and data request processing require time, disclosing the flow of funds can be lengthy.

R. Soesilo (1995) explains that the crime of fraud involves the intention to gain unlawful gain and the use of certain means to persuade another person to hand over goods or assets. Therefore, investigators must identify whether deception was used from the outset to induce the victim to hand over money or goods, rather than simply observing the failure to fulfill transaction obligations.

3. Limited Human Resource Capabilities of Investigators

Handling triangular fraud crimes requires investigators with an understanding of criminal law and technical skills in information technology. This is because solving cases involves more than just witness examinations and physical documents, but also requires analysis of electronic devices, communication histories, account identities, and digital transactions.

Not all investigators possess the same level of technical expertise in conducting digital forensic examinations. Such examinations require knowledge of how to secure data, extract information, analyze metadata, and verify the authenticity of electronic evidence. If these skills are limited, the examination process may rely on the assistance of specific personnel or experts, requiring additional time.

Research by Muhammad Safei, Sandra Dewi, and Olivia Anggie Johar (2025) on the use of digital evidence in online fraud law enforcement within the Riau Regional Police jurisdiction identified limited technical capacity and digital forensic tools as issues affecting the effectiveness of evidence. The research findings are relevant as a description of the challenges of handling electronic-based fraud in Riau, although they do not specifically measure all triangular fraud cases.

4. High Potential for Unreported Cases

Another obstacle to consider is the possibility of fraud cases not being reported to the police. Victims who experience losses may choose to resolve the issue privately, contact the account recipient, or simply file a complaint via social media without proceeding to a formal report.

This situation can result in the actual number of fraud incidents not being fully recorded in police case handling data. As a result, law enforcement officials may not obtain a complete picture of the patterns, frequency, and development of the triangle fraud scheme.

Research by Muhammad Safei, Sandra Dewi, and Olivia Anggie Johar (2025) differentiates between public complaints and police reports, which serve as the basis for investigations. The study recorded 840 online fraud complaints in 2024 and 793 complaints from January to November 2025 at the Riau Regional Police. These figures represent general online fraud complaints, not specific cases of triangular fraud. This distinction is important to prevent misuse of the research data.

Obstacles to law enforcement against triangular fraud crimes in the jurisdiction of the Riau Regional Police can be analyzed using Soerjono Soekanto's theory of factors influencing

law enforcement. This theory explains that the success of law enforcement is influenced by five interrelated factors: legal factors, law enforcement, facilities, society, and culture.(Safei et al., 2025).

First, legal factors. Obstacles to legal factors relate to the appropriate application of criminal provisions to the perpetrator's actions. Triangle fraud is a modus operandi that can involve several forms of conduct, so investigators must determine the qualifications of the crime based on proven facts and elements of the offense. The use of the National Criminal Code and the provisions of the ITE Law must be carried out carefully to avoid errors in determining the basis for criminal liability.(Simarmata, 2013).

Second, law enforcement factors. This obstacle relates to the limited technical capabilities of investigators in examining digital evidence and tracing electronic transactions. Uncovering triangle fraud requires the ability to identify perpetrators using false identities and establish the link between electronic communications and the transfer of money or goods. Therefore, improving investigator competency is a crucial requirement in handling these cases.(Safei et al., 2025).

Third, the infrastructure and facilities factor. Limited digital forensic equipment, examination software, evidence storage facilities, and expert personnel can slow down the investigation process. Yet, electronic evidence is crucial in uncovering the relationship between the perpetrator and the victim. The availability of adequate facilities will support the process of securing and analyzing evidence more accurately.(Soekanto, 2014).

Fourth, societal factors. Obstacles to societal factors are evident in the limited understanding of reporting procedures and the importance of preserving digital evidence among some victims. People who fail to report promptly or retain evidence of communication can make it difficult for investigators to construct a criminal case.

Fifth, cultural factors. Cultural factors relate to the societal habit of conducting transactions based on trust without verifying the identities of the parties. The habit of making payments without verifying the name of the account recipient matches the name of the party entitled to receive the payment can be exploited by perpetrators to carry out triangle fraud.(Najwa et al., 2026).

Based on these five factors, the obstacles to law enforcement against triangle fraud cannot be resolved solely by increasing the application of criminal sanctions. Improved officer capacity, enhanced technological facilities, strengthened institutional coordination, and increased public legal awareness are required. This will allow law enforcement to be more targeted in identifying the main perpetrators and providing protection to victims.

C. Efforts to overcome obstacles in implementing law enforcement in the crime of triangular fraud in the jurisdiction of the Riau Regional Police

To address these various problems, planned and sustainable steps are needed to ensure effective law enforcement. Based on these obstacles, targeted efforts are needed to ensure effective law enforcement against triangular fraud within the Riau Regional Police jurisdiction. These efforts need to be tailored to the characteristics of triangular fraud, which involve identity theft, the use of third-party accounts, electronic communications, and the possibility that victims may not report their experiences. Possible efforts include the following.

1. Optimizing the Tracing of the Perpetrator's Identity and Disclosure of the Network Involved

   The first step that needs to be taken is to optimize the identity tracing of the perpetrator by examining all information related to electronic transactions and communications. Riau Police investigators need to link social media accounts, telephone numbers, email addresses, communication devices, recipient accounts, and conversation

histories between the perpetrator, seller, and buyer. This examination aims to establish the connection between the parties involved so that it can be determined who actually controlled the communication and orchestrated the transaction.

Furthermore, investigators need to conduct a thorough examination of the statements of the victim, the original seller, and the account holder used to receive the payment. Each party's statement must be matched with evidence of communication and financial transactions to determine each person's role in the chain of events. Therefore, case management should not only focus on the party named on the account but also aim to uncover the main perpetrator and any other parties who knowingly assisted or were involved in the crime (Maskun, 2022).

2. Improving Investigator Capabilities and Optimizing Security and Examination of Electronic Evidence

   The second effort is to improve the human resource capabilities of investigators through education and training related to handling electronic-based crimes. Investigators need to have the skills to secure electronic devices, examine digital conversations, trace account identities, analyze metadata, and understand digital forensic examination procedures. Improving these skills is crucial for investigators to identify and link electronic evidence to the criminal incidents being handled.

   In addition to improving personnel capabilities, securing electronic evidence needs to be implemented from the initial receipt of a report. Victims should be instructed to save conversations, transfer receipts, account links, phone numbers, sales advertisements, and other information related to the transaction. Investigators must then ensure that this evidence is obtained, reviewed, and documented with attention to authenticity and integrity. If a more in-depth technical examination is required, investigators can coordinate with experts or digital forensic laboratories with the competencies appropriate to the case (Safei et al., 2025).

3. Strengthening Coordination with Banks and Digital Service Providers to Trace Fund Flows

   The third effort is to strengthen coordination between Riau Police investigators and banks, payment service providers, and digital platform operators. This coordination is necessary to obtain information related to recipient accounts, transaction history, account holder identities, and account data used in communications and transactions. Information requests must be made through official procedures in accordance with applicable laws and regulations.

   When handling third-party accounts, investigators need to trace the flow of funds from the moment they are received from the victim to the party making the withdrawal or transfer. This investigation must be accompanied by an analysis of communications and payment instructions to determine whether the account holder is merely being used as an intermediary, is aware of the use of their account, or is knowingly assisting in the commission of the crime. Through continuous coordination and transaction tracing, investigators are expected to identify those controlling and benefiting from the proceeds of crime (Suhariyanto, 2012).

4. Improving Reporting Services, Socialization, and Public Legal Awareness

   The fourth effort is to improve public services while expanding outreach regarding the methods and dangers of triangle fraud. The Riau Regional Police need to make it easier for victims to submit reports or complaints, obtain information on case handling procedures, and receive guidance on the necessary evidence. Officers also need to clearly explain the differences between consultations, complaints, and police reports so the public understands the legal steps they can take when they experience fraud.

Outreach can be conducted through social media, direct outreach, collaboration with local governments, and community education activities. Outreach materials should emphasize the importance of verifying the seller's identity matches the account holder's name, avoiding payments to accounts with unclear links to transactions, and retaining all evidence of communication and payment. It is hoped that this increased awareness will encourage the public to be more cautious in their transactions and encourage victims to report crimes (Soekanto, 2014).

CONCLUSIONS

Law enforcement in the triangular fraud crime within the jurisdiction of the Riau Regional Police is carried out through the stages of receiving reports or public complaints, investigation, inquiry, evidence collection, examination of witnesses and involved parties, tracing accounts and cash flow, and resolving the case in accordance with applicable law. Handling this case requires a thorough examination because the perpetrators use different identities to connect the seller and buyer, so that the party receiving the money or delivering the goods is not necessarily the main perpetrator. Therefore, law enforcement needs to be directed at uncovering the chain of actions, communication relationships, and the role of each party in the crime.

Obstacles to law enforcement in the triangular fraud case within the jurisdiction of the Riau Regional Police include difficulties in identifying the perpetrators, obtaining and verifying electronic evidence, the use of third-party bank accounts, and difficulties in tracing the flow of funds from the crime. Furthermore, limited human resource capacity for digital forensic investigations and the potential for unreported cases by victims also impact the process of uncovering the crime. These obstacles require time, technical expertise, and coordination with various parties to accurately prove the perpetrators' involvement.

Efforts to overcome obstacles in the implementation of law enforcement in the crime of triangular fraud in the jurisdiction of the Riau Regional Police are carried out through optimizing the tracing of the perpetrator's identity and revealing the parties involved, improving the capabilities of investigators and securing and examining electronic evidence, strengthening coordination with banks and digital service providers to trace the flow of funds, and improving reporting services, socialization, and public legal awareness. These efforts need to be implemented in an integrated manner so that case handling does not only focus on the party receiving the money, but also can uncover the perpetrators who planned and controlled the crime and those who consciously helped carry it out.

REFERENCES

Akbar, M. N. T., Alimuddin, H., Arumahi, H. L., & Syahird, A. (2026). Analisis yuridis perlindungan hukum terhadap korban kejahatan siber dalam penipuan jual beli online dengan modus segitiga di Kota Makassar. *Jurnal Pustaka Cendekia Hukum dan Ilmu Sosial, 4*(2).

Alif Agung Samudra, R., & Widarto, B. (2024). Penegakan hukum tindak pidana penipuan dalam jual beli mobil bekas (Studi kasus di Polsek Duren Sawit). *Lex Progressium: Jurnal Kajian Hukum dan Perkembangan Hukum, 1*(1).

Arief, B. N. (2017). *Bunga rampai kebijakan hukum pidana*. Kencana.

Arifin, R. (2019). Penegakan hukum tindak pidana penipuan secara online berdasarkan Pasal 378 KUHP. *Dinamika: Jurnal Ilmiah Ilmu Hukum, 25*(4).

Arizoni, D., Ashibly, & Rosmanila. (2024). Penegakan hukum terhadap penipuan triangle scheme pada transaksi kendaraan bekas di platform digital. *Jurnal Jendela Hukum dan Keadilan, 10*(1).

Bastari, R. G., Junaidi, A., & Ismiyanto. (2024). Perlindungan hukum terhadap tindak pidana penipuan dalam situs jual beli online di Indonesia. *Ranah Research: Journal of Multidisciplinary Research and Development, 7*(1).

Chazawi, A. (2011). *Kejahatan terhadap harta benda*. Bayumedia Publishing.

Darmayanti, D. M. P., & Suardita, I. K. (2017). Kajian terhadap tindak pidana penipuan melalui jual-beli online. *Kertha Wicara: Journal Ilmu Hukum, 6*(1).

Fauzi, S. N., & Primasari, L. (2017). Tindak pidana penipuan dalam transaksi di situs jual beli online (e-commerce). *Recidive: Jurnal Hukum Pidana dan Penanggulangan Kejahatan, 6*(3).

Hamzah, A. (2016). *Hukum acara pidana Indonesia*. Sinar Grafika.

Kesuma, I. G. M. J., Widiati, I. A. P., & Sugiartha, I. N. G. (2020). Penegakan hukum terhadap penipuan melalui media elektronik. *Jurnal Preferensi Hukum*, *1*(2).

Kesuma, I. G. M. J., Widiati, I. A. P., & Sugiartha, I. N. G. (2020). Penegakan hukum terhadap penipuan melalui media elektronik. *Jurnal Preferensi Hukum, 1*(2).

Makari, E. (2003). *Kompilasi hukum telematika*. RajaGrafindo Persada.

Mappaselleng, N. F. (2024). Analisis kriminologis tindak pidana penipuan melalui transaksi online. *Indonesian Journal of Legality of Law, 6*(2).

Maskun. (2022). *Kejahatan siber (cyber crime): Suatu pengantar*. Kencana Prenada Media Group.

Miss, J. S., Rumapea, M. S., Wijaya, A., Manurung, B. M., & Lionggodinata, W. (2019). Upaya penanggulangan tindak pidana penipuan situs jual beli online di Indonesia. *Jurnal Hukum Samudra Keadilan, 14*(1).

Moeljatno. (2015). *Asas-asas hukum pidana*. Rineka Cipta.

Najwa, N., Makkuasa, A., & Hidjaz, M. K. (2026). Penegakan hukum terhadap penipuan digital antara ketersediaan regulasi dan keterbatasan implementasi. *Legal Dialogica*, *1*(2).

Pajriansyah, D., Moresikani, K., Nadhila, M., Patoni, R., & Haza, Z. E. (2023). Penegakan hukum dalam tindak pidana dalam transaksi jual beli online. *Consensus: Jurnal Ilmu Hukum, 1*(3).

Panjaitan, A. Y. (2021). Analisis putusan Nomor 194/Pid.Sus/2019/PN MNK tentang tindak pidana penipuan terhadap transaksi elektronik. *Novum: Jurnal Hukum, 4*(4).

Rahmadhani, E., Saipuddin, L., & Amin, I. (2026). Penegakan hukum terhadap tindak pidana penipuan berbasis online di Polresta Mataram. *Parhesia, 4*(1).

Rauf, A., Idy, M. Y., Suryani, & Hardi. (2022). Tindak pidana penipuan dalam transaksi jual beli secara online. *SISITI: Seminar Ilmiah Sistem Informasi dan Teknologi Informasi, 11*(1).

Rimbawa, I. M. A., Pradnyana, I. W. A. N., Fajar, N. M. A. P., Priscyllia, F., & Dewi, C. I. D. L. (2025). Pelaksanaan penegakan hukum dalam tindak pidana penipuan (378 KUHP): Penelitian di wilayah hukum Polres Karangasem. *Jurnal Yustitia, 19*(2).

Rizal, S., & Matondang, T. M. (2024). Analisis yuridis pertanggungjawaban e-commerce terhadap tindak pidana penipuan dalam transaksi jual beli online. *Ilmu Hukum Prima (IHP), 7*(1).

Safei, M., Dewi, S., & Johar, O. A. (2025). Implementasi pada alat bukti jejak digital dalam penegakan hukum tindak pidana penipuan online. *Collegium Studiosum Journal*, *8*(2).

Salsabila, V. D., Putera, A., & Jannah, M. (2026). Tinjauan yuridis tindak pidana penipuan jual beli barang melalui online. *Legal Dialogica, 1*(2).

Santoso, L. L. A., & Apriani, R. (2023). Perlindungan hukum terhadap tindak pidana penipuan di masa pandemi. *Jurnal Justitia: Jurnal Ilmu Hukum dan Humaniora, 6*(2).

Simarmata, B. Hambatan dalam penyidikan tindak pidana penipuan melalui internet. *Fiat Iustitia: Jurnal Hukum*, *1*(1).

Soekanto, S. (2014). *Faktor-faktor yang mempengaruhi penegakan hukum*. Rajawali Pers.

Soesilo, R. (1995). *Kitab Undang-Undang Hukum Pidana (KUHP) serta komentar-komentarnya lengkap pasal demi pasal*. Politeia.

Suhariyanto, B. (2012). *Tindak pidana teknologi informasi (cybercrime): Urgensi pengaturan dan celah hukumnya*. RajaGrafindo Persada.

Suharto, A. (2024). Upaya perlindungan terhadap tindak pidana penipuan jual beli online perspektif Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik (Studi pada platform OLX). *IBLAM Law Review, 4*(3).

Zabidin. (2021). Analisis penegakan hukum tindak pidana penipuan online di Indonesia. *Spektrum Hukum, 18*(2).