Juridical Analysis of Transaction Fraud Crime Online in North Lampung Regency

Resa Septia, Nisa Fadhilah,
Universitas Muhammadiyah Kotabumi
Email: resaseptia9900@gmail.com,nisa.fadhilah@umko.ac.id,

Abstract

The rapid development of digital technology has increased online transactions within society while simultaneously giving rise to various forms of cybercrime, including online fraud. This study aims to analyze the application of legal provisions to online transaction fraud in North Lampung Regency and to identify the challenges faced by law enforcement in handling such cases. This research employs an empirical juridical method by examining the relevant provisions of the Indonesian Criminal Code (KUHP), the Electronic Information and Transactions Law (UU ITE), and empirical data regarding patterns of online fraud occurring in the region. The findings indicate that online fraud generally fulfills the elements of Article 378 of the Criminal Code, while the provisions of the ITE Law serve as additional instruments when offenders use electronic media to deceive victims or disguise their identities. However, the effectiveness of law enforcement remains hindered by difficulties in tracing offenders who utilize fake accounts, the limited availability of digital evidence preserved by victims, and the lack of technical capacity among investigators in managing electronic evidence. These conditions demonstrate that cybercrime cannot be addressed solely through normative regulation, but also requires adequate infrastructure and enhanced human resource capabilities. This study emphasizes the urgency of strengthening law enforcement through improved cyber-investigation skills, the provision of technological support systems, and increased digital literacy among the public. Such efforts are essential to ensuring more effective legal protection and fostering a safer digital transaction environment in North Lampung Regency.

Keywords: *online fraud, electronic transactions, Criminal Code, Electronic Information and Transactions Law, North Lampung.*

Introduction

The development of information technology has brought major changes in people's lives, including in buying and selling activities which are now widely carried out through digital media.[1] People in North Lampung Regency are increasingly accustomed to using social media, *marketplaces*, and communication applications as a means of daily transactions. This change in behavior patterns does offer convenience and efficiency, but at

[1] Danang Rifai et al., "The Development of the Digital Economy Regarding the Behavior of Social Media Users in Making Transactions The Development of the Digital Economy Regarding the Behavior of Social Media Users in Making Transactions," n.d.

the same time increases the risk of criminal acts that take advantage of technological loopholes. One of the most common forms of crime is fraud in online transactions, which results in material losses while lowering the level of public trust in the security of digital transactions.[2]

Fraud in *online* transactions basically has different characteristics from conventional fraud.[3] If in traditional fraud the perpetrator and victim interact directly, then in online transactions the relationship between the two is mediated by technology. Perpetrators often take advantage of fake identities, untraceable account numbers, or use digital application features to disguise their existence.[4] Forms of fraud that often appear include the sale of fictitious goods, the use of fake transfer receipts, the sending of malicious links *(phishing),* and the creation of fake *marketplace* accounts. This condition not only causes economic losses, but also reduces public trust in the use of the internet as a safe transaction medium.

Juridically, fraud has been regulated in Article 378 of the Criminal Code, which emphasizes that a person can be convicted if with the intention of unlawfully benefiting himself or others, he uses trickery, a series of lies, or influences others to hand over an item. This provision emphasizes the existence of malicious intent *(mens rea)* and deceptive acts *(actus reus).*

However, when fraud is committed using electronic means, the provisions of the Criminal Code cannot stand alone. In the context of digital crime, law enforcement officials must also refer to Article 28 paragraph (1) of Law Number 19 of 2016 (Amendment to the ITE Law) which prohibits everyone from spreading false and misleading news that causes losses in electronic transactions. This provision is strengthened by Article 45A paragraph (1) which stipulates criminal threats for the party who commits the act. Thus, the combination of Article 378 of the Criminal Code and the articles in the ITE Law provides a more complete legal basis for dealing with online fraud, especially those that utilize electronic media as the main instrument

Various previous studies have discussed the problem of criminal acts related to information technology, but the focus raised is different. The research conducted by Muhammad Ilman Nafian, for example, focuses more attention on the importance of protecting the public against the risks of using digital media and emphasizes the need for caution in interacting through electronic platforms.[5] Meanwhile, another study by Muhammad Arif Sahlepi discusses the social and legal dynamics arising from technological developments, but the study does not specifically highlight the form of criminal liability in online transactions or the pattern of its handling by local law enforcement officials.[6]

[2] Jason Aaron et al., "Analisis Tindak Pidana Penipuan Online Dalam Konteks Hukum Pidana Cara Menanggulangi Dan Pencegahannya" 4, no. 2 (2024): hlm. 281–94.

[3] Berbasis Transaksi Elektronik, Tony Yuri Rahmanto, and Badan Penelitian, "De Jure De Jure" 19, no. 30 (2019): hlm.31–52.

[4] Marselino Clifer Tuju, Suci Ramadani, and Chairuni Nasution, "Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli Online Dalam Perspektif Kriminologi" 5 (2025): hlm.1763–76.

[5] Article Information, "Transaksi Elektronik, Penipuan, Perlindungan Hukum" 4, no. 6 (2024).

[6] Muhammad Arif Sahlepi, "Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik" 3 (2023): 1402–12.

Mahendra and colleagues' research pays attention to the criminal act of fraud in the realm of electronic transactions by emphasizing the protection aspect of consumers and business actors, but has not reviewed how law enforcement is carried out concretely at the local level and how laws and regulations are applied in cases that occur in the community.[7]

From the three studies, it can be seen that the study of technology-based crime has developed quite a bit, but there are still gaps that have not been touched, especially related to the juridical analysis of fraud in online transactions that occur specifically in North Lampung Regency. Each region has different social characteristics, patterns of technology use, and dynamics of handling cases. Therefore, research that focuses on the local context is important to provide a more concrete picture of how the rules of law, both the Criminal Code and the Electronic Information and Transaction Law, are applied in dealing with cases of rampant online fraud.

The novelty of this study arises from an effort to combine normative analysis of criminal regulations with empirical data on law enforcement practices in North Lampung. This research not only discusses the elements of fraud in electronic transactions, but also describes how police and prosecutors handle public reports, obstacles that arise in the investigation process, and the forms of modes that are developing in the region. Thus, this research presents a new perspective that has not been raised by previous research, while contributing to the development of technology-based criminal law studies at the regional level. In addition, the novelty of this research is also the incorporation of normative analysis of Article 378 of the Criminal Code and Article 28 paragraph (1) jo. Article 45A paragraph (1) of the ITE Law with empirical data regarding the handling of online fraud cases in North Lampung. This research not only describes the elements of criminal acts based on the provisions of the law, but also photographs law enforcement practices, investigation constraints, and variations in fraud modes that develop in society. This study is expected to provide a new perspective that can enrich the literature on electronic crime, especially at the regional level.

Method

This study uses a normative juridical method because the focus of the study is on the analysis of the legal rules that govern fraud in online transactions and their application based on official documents and other legal materials. This approach was chosen to examine in depth how the provisions in the Criminal Code and the Electronic Information and Transaction Law are used in ensnaring digital-based fraudsters.

The data sources in this study are all from legal materials, both primary and secondary. Primary legal materials include relevant laws and regulations, such as the Criminal Code, the ITE Law, and court decisions related to online fraud crimes. Secondary legal materials are obtained from scientific literature, criminal law books, accredited journal articles, previous research results, and other documents that can support the analysis of the

[7] Gelar Ali Ahmad, "Analisis Yuridis Tindak Pidana Penipuan Transaksi Jual Beli Online Terhadap Pelaku Usaha Sebagai Korban," 2008.

elements of criminal acts and the application of legal provisions in the context of electronic transactions. Data collection is carried out through literature studies by studying, identifying, and classifying legal sources that are in accordance with the research problem.

Discussion

Rules Governing Online Transaction Fraud and Overview of Online Transaction Fraud in North Lampung Regency

Fraud in *online* transactions is basically a form of fraud committed by utilizing electronic means as the main medium.[8] Juridically, this act is still based on the general provisions regarding fraud as stipulated in Article 378 of the Criminal Code, which emphasizes that a person can be convicted if he deliberately uses trickery, a series of lies, or takes advantage of the trust of others to obtain an unlawful advantage so that the victim hands over goods or provides a benefit. The element of fraud contained in the Criminal Code can still be applied in the case of *online transactions* because the nature of fraud, namely the existence of misleading actions that cause losses, has not changed even though the medium is different.

However, when these acts are carried out through electronic devices, the regulation is not enough to depend only on the Criminal Code. The state provides additional legal instruments through the Electronic Information and Transactions Act. Article 28 paragraph (1) of Law Number 19 of 2016 prohibits everyone from spreading false and misleading information that can cause losses in electronic transactions, while Article 45A paragraph (1) provides a criminal threat for violations of these provisions. This article emphasizes that the dissemination of false information through electronic platforms such as social media, *marketplaces,* or messaging applications is prohibited and punishable. Thus, the Criminal Code and the ITE Law are complementary to each other: the Criminal Code confirms the existence of an element of fraud, while the ITE Law emphasizes that the act is carried out through electronic means.

In practice, *online* fraud is carried out through various actions aimed at falling into victims. Perpetrators often use fake identities or anonymous accounts to obscure the trail, then offer goods or services that never actually existed. To convince victims, perpetrators often send fake proof of transfers, forged delivery receipts, or misleading messages that appear to indicate that the transaction is being processed. It is not uncommon for perpetrators to persuade victims with a series of stories made up to encourage victims to make payments immediately, or send fake links that can steal personal data. After the victim transfers a certain amount of money, the perpetrator usually disappears by blocking the contact or deleting the account. These various modes essentially show that perpetrators use technology to hide identities, convey misleading information, and gain profits illegally.

[8] Marselinus Goa and Hudi Yusuf, "Analisis Penipuan Online Melalui Media Sosial Dalam Kasus Kejahatan Belanja Online Di Wilayah Jawa Timur" 3, no. 3 (2025).

Through the combination of Article 378 of the Criminal Code and Article 28 paragraph (1) jo. Article 45A paragraph (1) of the ITE Law, law enforcement has sufficient grounds to ensnare perpetrators *of online fraud.* This arrangement not only looks at the actions of perpetrators from the perspective of conventional fraud, but also pays attention to the characteristics of digital crimes that require proof related to electronic footprints, false information, and misleading online activities. Thus, the legal regulation of online transaction fraud reflects the adaptation of criminal law to technological developments and the increasingly complex patterns of crime in the digital era.

The development of digital activities in North Lampung Regency in recent years has shown a significant increase. People from various age groups, especially the younger generation and housewives, are increasingly actively using social media such as Facebook, WhatsApp, TikTok and Instagram to buy and sell everyday goods. This is influenced by several factors, such as the ease of internet access, the increasing use of gadgets, and the rise of local sellers who market goods online.[9] However, these changes are not always followed by the ability of the public to recognize the threat of digital crime, so the number of online fraud in this region continues to increase.

In North Lampung, *the pattern of online* fraud is generally related to the sale of fictitious goods, such as clothes, shoes, gadgets, and various electronic products. The mode that is often used is to offer goods at a much cheaper price than the market, then convince the victim to make a full payment in advance. The perpetrator usually gives reasons that seem reasonable, such as limited stock, goods running out quickly, or there is a special promo. After the victim transfers the money, the perpetrator disappears, blocks communication, or changes his digital identity.

Most of these transactions are done through local buying and selling groups on Facebook or unofficial *marketplaces*. The characteristics of victims are generally those who are tempted by low prices and are less careful in verifying the identity of the seller.[10] Meanwhile, perpetrators often use fake accounts created specifically to deceive, complete with profile photos and uploads that appear to show normal buying and selling activities. The perpetrator's ability to manipulate this condition makes it even more difficult for victims to distinguish which is the real seller and which is the fraudulent account.

This phenomenon is increasingly evident with several cases that have been handled by local law enforcement officials. One of the cases that became an example was when a Kotabumi resident became a victim of fraud through a mobile phone purchase transaction. The perpetrator offered a branded phone at a very low price through social media, and the victim was asked to transfer a certain amount of money as a sign of completion. After the payment is made, the perpetrator no longer responds to the victim's message. The investigation later found that the account used by the perpetrator borrowed the identity of

[9] Role Effectiveness et al., "Journal of Lex Philosophy (JLP)" 5 (2024).
[10] Anakletus Rumlus et al., "Legal Responsibility of Perpetrators of Online-Based Fraud Thesis," 2023.

another person and the account number used was a holding account belonging to a third party.[11]

This example shows that online fraud in North Lampung is not a stand-alone event, but is part of a broader social phenomenon, where the use of technology is not always balanced with an understanding of digital security. This situation confirms the need for serious attention not only from law enforcement officials, but also from the public who need to increase vigilance and ability to recognize fraud patterns. In addition, this condition suggests that the study of online fraud requires a more comprehensive approach in order to understand how the mechanisms of this crime take place and how legal protection can be provided effectively.

Online Transaction Fraud Mode in North Lampung Regency

Digital-based fraud in North Lampung Regency shows a variety of modes that are growing along with the increasing use of social media and online transaction platforms. Although each case has different characteristics, the common pattern that is often found is the use of digital space as a means to disguise the identity of the perpetrator, expand the reach of potential victims, and take advantage of digital security loopholes that are not fully understood by the public.

One of the most common modes is the offering of fictitious goods through social media. Actors usually create new accounts with convincing-looking identities, complete with profile photos, product uploads, and fake testimonials, at prices that appear to be much cheaper than the market price. Huge profits in a short time became an attraction that tempted many victims. When potential buyers begin to put their trust, the perpetrator then encourages the payment to be made in full at the beginning on the grounds of limited stock or a certain time promo. After the money was successfully transferred, communication was immediately cut off and the perpetrator's account disappeared.

Another mode is the use of fake transfer receipts to make the victim believe that the perpetrator has made a payment or delivery of goods.[12] This technique is commonly used in two-way buying and selling transactions, where the perpetrator sends an image of the original proof of transfer, even though the actual transaction never happened. The existence of a transaction proof editor application makes it easier for perpetrators to manipulate it. Victims who do not understand the characteristics of digital transfer proof are usually easy to trust and hand over the goods or make a follow-up payment.

[11] Tribrata News, "Spesialis Pelaku Penipuan Diamankan Polsek Kotabumi Kota," 2024, https://tribratanews-reslampungutara.lampung.polri.go.id/detail-post/spesialis-pelaku-penipuan-diamankan-polsek-kotabumi-kota.

[12] Aulia Anjani Nurdin, Axara Alejendra Anjani, and Fiqih Dien Alamsyah, "Indonesian Legal Media (MHI) Analysis of Online Fraud through Social Media in the Criminology Perspective of Indonesian Legal Media (MHI)" 2, no. 2 (2024): hlm. 74–82.

There is also a mode of fraud through the creation of a fake account that imitates official stores or trusted sellers. The perpetrator took advantage of the store's reputation to attract buyers' trust. The victim thought he was transacting with the right store, even though the account was completely fake. A similar pattern was found in the form of sending malicious links *(phishing),* which were directed to take personal data or trick victims into transferring a sum of money to the perpetrator's account. In some cases in North Lampung, the perpetrator also took advantage of loan accounts or accounts of other people who did not know that their identities were being used for criminal activities. These kinds of accounts make it difficult to track because the flow is not directly connected to the main actor. After the transaction was successful, the perpetrator immediately withdrew funds and stopped contact with the victim.

These various modes show that *online fraud* in North Lampung Regency does not only depend on technological sophistication, but also on the ability of perpetrators to take advantage of public negligence. The pattern always relies on false identities, misleading information, and efforts to eliminate digital traces after the victim has suffered a loss. The pattern that is developing in this region illustrates that *online* fraud is not only a technological problem, but also a social problem related to low digital literacy and high public trust in fast transactions through digital platforms.

The phenomenon of the development of fraud mode illustrates that digital crime in North Lampung is no longer random, but has shown a structured pattern. Perpetrators understand the tendency of people who easily believe in low prices, fake testimonials, or promos that seem profitable. By utilizing the digital space as the main medium, actors can carry out their actions with little risk and high mobility. This condition makes digital-based fraud one of the serious challenges for law enforcement in the region.

Law Enforcement Against *Online* Fraud in North Lampung Regency

The application of legal provisions to online transaction fraud cases in North Lampung Regency basically still adheres to two main instruments, namely the Criminal Code and the Information and Electronic Transactions Law (UU ITE). The two instruments are used simultaneously because the perpetrator's actions not only include deception as formulated in Article 378 of the Criminal Code, but also involve the use of electronic means as a medium to commit lies. This situation puts law enforcement officials in the position of having to interpret both provisions simultaneously so that the law enforcement process can run effectively. The process of proving in *online* fraud is the most decisive aspect in the application of legal provisions.[13]

[13] Efektivitas Pencegahan et al., "Journal of Lex Philosophy (JLP)" 5 (2024).

The handling of fraud cases in *online transactions* in North Lampung Regency basically follows the mechanism of criminal law enforcement in general, but has special characteristics because the acts are carried out through electronic means. The law enforcement process at the regional level shows that the authorities not only assess the elements of fraud, but also must understand the patterns of technology use and digital footprints left by the perpetrators.

Stages of Research and Investigation

Case handling usually begins with a community report. At the investigation stage, the police collected preliminary information to confirm the existence of an alleged criminal act. Because the majority of perpetrators use fake identities or accounts that are easily deleted, investigators must trace transaction conversations, communication history, social media accounts, and fund transfer flows. After it was found that there were acts that led to fraud, the process was continued to an investigation.

At the investigation stage, the authorities began to corroborate the evidence by asking for information from the victim, witnesses, and tracing the account number used by the perpetrator. Investigators also work with banks, digital platform providers, or mobile operators to obtain data that can identify the perpetrators. The challenge that often arises is that the perpetrators are outside the North Lampung area or use accounts borrowed from other parties, so the investigation requires cross-regional coordination. However, investigators are still trying to compile a case construction based on the flow of electronic transactions and communication that takes place.

Digital Evidence

In *the case of online fraud, the* evidence used by the police is mostly in the form of electronic evidence. This evidence includes screenshots of conversations, chat history on messaging applications, call recordings, photos of goods or advertisements used by the perpetrator, social media account links, and transaction track records recorded in the banking system. In addition, evidence in the form of account mutations, proof of original transfers from banks, IP addresses, and phone number owner data are also used to strengthen the evidence. The electronic evidence is a valid basis according to the law because the ITE Law recognizes electronic information as evidence that has the same evidentiary power as conventional evidence. With digital evidence, investigators can trace the relationship between the perpetrator, the electronic means used, and the losses suffered by the victim

Application of Article

In online fraud cases, investigators in North Lampung generally apply a combination of articles to strengthen the legal construction. Article 378 of the Criminal Code is used to ensnare deceptive acts through a series of lies that cause the victim to hand over money or

goods. This article is the general basis for the unlawful nature of the perpetrator's actions. In addition to the Criminal Code, investigators also use provisions in the ITE Law, especially Article 28 paragraph (1) which prohibits the dissemination of false and misleading information that harms the public in electronic transactions. Violations of this article are subject to criminal sanctions as stipulated in Article 45A paragraph (1). With the application of these two legal instruments, the actions of the perpetrators are not only seen as ordinary fraud, but also as the misuse of electronic means that are specifically protected by the ITE Law. The combination of the application of this article is important because the mode of online fraud involves two aspects at once: the element of lying as regulated by the Criminal Code and the dissemination of misleading electronic information as regulated in the ITE Law. This provides space for investigators to draft stronger charges and provide legal certainty for victims.

Obstacles in Law Enforcement against Online Transaction Fraud

Law enforcement against online transaction fraud in North Lampung Regency is inseparable from various obstacles or obstacles that arise both in technical and non-technical aspects. These obstacles are interrelated and have a direct effect on the effectiveness of the investigation, proof, and case settlement process. One of the main obstacles that is most often encountered is the difficulty in identifying the perpetrator. Many perpetrators take advantage of fake identities, non-permanent social media accounts, and disposable phone numbers to carry out their mode. This digital identity forgery makes it difficult for perpetrators to track and slows down the investigation process, especially when the account used has been deleted or deactivated.

In addition to identity issues, the use of a holding bank account that does not belong to the perpetrator is also a big obstacle. In a number of cases, the perpetrator takes advantage of accounts borrowed from other people, or accounts that are deliberately provided as a means of fraud. This condition makes the authorities have to conduct multiple checks, ranging from account owners to banks, before they can confirm the actual involvement of the perpetrators. The coordination process with the bank takes time, especially when the account used is in a different area from where the victim reported.

Another obstacle lies in the availability and quality of digital evidence. Many victims do not keep important evidence such as conversations, transaction history, or proof of transfer in a complete format. There are also victims who only report after a long time has passed so that electronic evidence that should be accessible through applications or digital systems is no longer available. In online fraud , digital evidence is a crucial component that determines whether the elements of the crime can be proven. The incompleteness of the evidence is a serious challenge for investigators to build a legal construction that can be accounted for.

In addition to technical obstacles, the readiness of law enforcement officials in dealing with technology-based crimes is also an important factor. Online fraud requires special competence in understanding digital communication patterns, procedures for securing

electronic evidence, and identity tracking techniques in cyberspace. Not all investigators have adequate training or experience in the field. This shortcoming causes the process of handling cases to take longer than conventional fraud. Some cases even have to be coordinated with *cybercrime units* at the provincial or central level when regional investigators face limited technical capacity.

In addition to internal factors of the apparatus, the level of digital literacy of the community also plays a big role in the emergence of law enforcement obstacles. Many victims only become aware of the scam after the loss has occurred, but at that time they often don't understand what evidence to keep or what steps to take. Low vigilance in online transactions, especially on offers at unreasonable prices, makes the public an easy target for perpetrators. When the report was submitted to the authorities, the victim's position of not being ready to present evidence made the legal process more complicated.

Another obstacle that also affects is the scope of jurisdiction. Online fraud perpetrators are often not located in the North Lampung area, some are even outside the province. The difference in location between the victim and the perpetrator requires coordination between regions, both between the police and with cyber units at a higher level. This coordination process does not always run quickly because it depends on workload, administrative distance, and data request procedures to digital service providers or banks.

Overall, these various obstacles illustrate that *handling online* fraud requires a more comprehensive approach than conventional fraud. Law enforcement does not only depend on criminal provisions, but also requires technical competency support, digital infrastructure readiness, and increased public awareness. Without overcoming these obstacles, *handling online fraud* in North Lampung will continue to face the same obstacles and it will be difficult to achieve optimal results.

Looking at the development of online transaction fraud cases in North Lampung Regency, it is increasingly clear that the handling approach that has been carried out so far is not fully adequate to answer the complexity of digital crime. Fraud carried out through electronic media is not only developing in terms of mode, but also increasingly structured and taking advantage of weaknesses in security systems and low public awareness in protecting personal data and ensuring the legitimacy of transactions. This condition shows the importance of strengthening measures, both in the realm of law enforcement and in improving people's digital literacy.

In terms of law enforcement, increasing the capacity of the apparatus is an urgent need. Online fraud requires technical skills in managing digital evidence, understanding electronic communication patterns, and tracing the digital footprint of perpetrators who often use fake accounts or temporary phone numbers. Limited technical skills can hamper the investigation process, especially when perpetrators utilize more advanced technology or switch platforms.[14] Therefore, special training on cybercrime investigations needs to be

[14] Rewang Rencang et al., "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol. 5. No.7 (2024) Theme/Edition : Criminal Law (Seventh Month) Https://Jhlg.Rewangrencang.Com/" 5, no. 7 (2024): 1–16.

strengthened, so that officials at the regional level are able to handle cases quickly and accurately without having to always rely on *cybercrime units* at the provincial or central level.

In addition to strengthening human resources, law enforcement supporting infrastructure also needs to be improved. Handling electronic evidence requires digital verification tools, tracking devices, and other supporting systems capable of processing large amounts of data. The availability of this facility will help the authorities build a stronger proof construction. Cooperation with third parties such as digital service providers, banks, and telecommunication operators is also an important aspect to speed up the process of tracing the identity of perpetrators and the flow of financial transactions involved in *online fraud.*

On the other hand, increasing people's digital literacy is no less important. Many victims of *online fraud* appear due to ignorance in distinguishing between real and fake accounts, not understanding the characteristics of valid digital transaction proofs, or being easily tempted by promotions and prices that are much cheaper than market value.[15] Providing education on how to transact safely, the importance of verifying information before making payments, and being aware of unreasonable offers must be a program that is continuously carried out by local governments, educational institutions, and communities.

This educational effort not only serves as a preventive measure, but also helps the public understand the rights and legal steps that can be taken when becoming a victim. People who are more aware of digital security will be better prepared to collect and store evidence when fraud occurs, making it easier for the authorities in the proof process. Understanding the reporting procedure can also speed up law enforcement response and minimize losses suffered by victims.

The urgency of strengthening law enforcement and digital literacy reflects the fact that *online* fraud cannot be handled with a normative approach alone. Although regulations are available, their effectiveness depends on the readiness and ability of the parties involved, both law enforcement officials and the public as users of digital services. Without comprehensive measures that combine legal, technological, and educational aspects, handling *online* fraud will continue to face the same obstacles and potentially become a bigger threat as the use of technology increases in North Lampung.

Conclusion

Online transaction fraud in North Lampung Regency shows that technological developments have changed the pattern of crime, from being carried out directly to digital-based by utilizing social media, *marketplaces,* and other electronic means. Although the form and mode have changed, the elements of fraud as stipulated in Article 378 of the Criminal Code are still fulfilled, because the perpetrator uses trickery and a series of lies to encourage

[15] Juwita Sari et al., "INCREASING DIGITAL AWARENESS THROUGH HAZARD SOCIALIZATION Information Article" 01, no. September (2024): 21–27.

the victim to hand over a sum of money. The provisions in the ITE Law then serve as an additional basis to ensnare perpetrators who actively use electronic systems as a tool in committing fraud.

The application of the law against *online fraud* in practice still faces various obstacles, ranging from difficulties in tracking the identity of perpetrators who often use fake accounts, switching platforms, to utilizing other parties' holding accounts. Another challenge arises from the evidentiary aspect, where digital evidence is often not properly stored by victims or has been lost due to time constraints on access. In addition, the technical capabilities of the apparatus in managing electronic evidence and tracing digital footprints still need to be strengthened so that the investigation process can be carried out effectively.

Seeing these conditions, handling *online* fraud in North Lampung requires strategic steps that not only focus on law enforcement, but also on improving people's digital literacy. Strengthening the capacity of the apparatus in the field of cyber investigation, providing adequate legal infrastructure, and educating the public on how to transact safely in the digital space are very important aspects. This effort must be carried out on an ongoing basis so that the community is not only protected, but also able to play an active role in preventing similar criminal acts from occurring.

Overall, this study confirms that *online fraud* is a form of crime that can be handled with existing legal instruments, but its effectiveness is greatly influenced by the readiness of human resources, technological support, and public awareness. By strengthening these three aspects, it is hoped that law enforcement against online transaction fraud in North Lampung Regency can run more optimally, provide better legal protection for the community, and encourage the creation of a safer digital ecosystem.

Bibliography

Aaron, Jason, Riado Simanungkalit, Raihan Hertadi, and Universitas Pakuan. "Analisis Tindak Pidana Penipuan Online Dalam Konteks Hukum Pidana Cara Menanggulangi Dan Pencegahannya" 4, no. 2 (2024): 281–94.

Ahmad, Gelar Ali. "Analisis Yuridis Tindak Pidana Penipuan Transaksi Jual Beli Online Terhadap Pelaku Usaha Sebagai Korban," 2008.

Daniel, Albert, Hamonangan Tampubolon, and Uyan Wiryadi. "Tindak Pidana Pencurian Data Elektronik Ditinjau Berdasarkan Undang-Undang ITE," 2025, 4621–30.

Elektronik, Berbasis Transaksi, Tony Yuri Rahmanto, and Badan Penelitian. "De Jure De Jure" 19, no. 30 (2019): 31–52.

Goa, Marselinus, and Hudi Yusuf. "Analisis Penipuan Online Melalui Media Sosial Dalam Kasus Kejahatan Belanja Online Di Wilayah Jawa Timur" 3, no. 3 (2025).

Information, Article. "Transaksi Elektronik, Penipuan, Perlindungan Hukum" 4, no. 6 (2024).

Lubis, Muhammad Ridwan, Gomgom T P Siregar, Cut Nurita, and Venny Fraya Hartin. "Bulletin of Community Engagement" 3, no. 2 (2023).

Nurdin, Aulia Anjani, Axara Alejendra Anjani, and Fiqih Dien Alamsyah. "Media Hukum Indonesia (MHI) Analisis Penipuan Online Melalui Media Sosial Dalam Perspektif Kriminologi Media Hukum Indonesia (MHI)" 2, no. 2 (2024): 74–82.

Pencegahan, Efektivitas, Dan Penanggulangan, Tindak Pidana, and Jual Beli Online. "Journal of Lex Philosophy (JLP)" 5 (2024).

Peran, Efektivitas, Kepolisan Terhadap, Penegakan Hukum, Pidana Penipuan, Online Di, and Dunia Maya. "Journal of Lex Philosophy (JLP)" 5 (2024).

Rencang, Rewang, Jurnal Hukum, Lex Generalis, Hukum Pidana, Bulan Ketujuh, Universitas Islam, and Kalimantan Mab. "Rewang Rencang : Jurnal Hukum Lex Generalis. Vol. 5. No.7 (2024) Tema/Edisi : Hukum Pidana (Bulan Ketujuh) Https://Jhlg.Rewangrencang.Com/" 5, no. 7 (2024): 1–16.

Rifai, Danang, Sania Fitri, Irma Nirmala Ramadhan, and Rizky Ramadan. "Perkembangan Ekonomi Digital Mengenai Perilaku Pengguna Media Sosial Dalam Melakukan Transaksi Perkembangan Ekonomi Digital Mengenai Perilaku Pengguna Media Sosial Dalam Melakukan Transaksi," n.d.

Rumlus, Anakletus, Program Studi, Magister Ilmu, Universitas Islam, and Sultan Agung. "Tanggung Jawab Hukum Pelaku Tindak Pidana Penipuan Berbasis Online Tesis," 2023.

Sahlepi, Muhammad Arif. "Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Online Di Tinjau Dari Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan

Transaksi Elektronik" 3 (2023): 1402–12.

Sari, Juwita, Rahma Mahmudah, Muhamad Uut Suprianto, and Iim Khairunnisa. "MENINGKATKAN KESADARAN DIGITAL MELALUI SOSIALISASI BAHAYA Informasi Artikel" 01, no. September (2024): 21–27.

Sinambela, Rut Afentina, Salsabila Fayza, Bunga Ananda, Zaki Edi Saputra, Alawiyah Matondang, Fakultas Ekonomi, and Universitas Negeri Medan. "ETIKA EKONOMI DI ERA EKONOMI DIGITAL DALAM STUDI KASUS PENIPUAN LAYANAN JASA TITIP (JASTIP) DAN DAMPAKNYA TERHADAP" 13 (2025): 313–22.

Tribrata News. "Spesialis Pelaku Penipuan Diamankan Polsek Kotabumi Kota," 2024. https://tribratanews-reslampungutara.lampung.polri.go.id/detail-post/spesialis-pelaku-penipuan-diamankan-polsek-kotabumi-kota.

Tuju, Marselino Clifer, Suci Ramadani, and Chairuni Nasution. "Penegakan Hukum Terhadap Tindak Pidana Cyber Dalam Kasus Penipuan Jual Beli Online Dalam Perspektif Kriminologi" 5 (2025): 1763–76.