Criminal Law Enforcement Against E-Commerce Fraud: A Case Study at the East Java Regional Police

Jessyca Dea Welhelmindo Bua Hetady[1*], Jonaedi Efendi[2]
[1]jessycadea@gmail.com, [2]jonaediefendi@ubhara.ac.id
Universitas Bhayangkara Surabaya

ABSTRACT

This study aims to examine the efforts and challenges faced by the East Java Regional Police in enforcing the law against e-commerce fraud, which has become increasingly prevalent in the digital era. The research employs a qualitative method with a juridical-empirical approach and a descriptive research type, by collecting primary data through direct interviews with the Head of the Cyber Unit at the East Java Regional Police and victims of fraud, as well as secondary data from legislation such as the Indonesian Penal Code (KUHP) and Law No. 19 of 2016 on Electronic Information and Transactions (ITE Law), supplemented by secondary and tertiary legal materials from various relevant literature and sources. The data analysis was conducted using triangulation by combining various data sources to enhance the validity of the findings. The results show that the East Java Police have made systematic efforts to enforce the law on e-commerce fraud, including digital data analysis, cyber forensic involvement, and coordination with financial authorities such as OJK and Bank Indonesia. However, the effectiveness of these efforts is hindered by technological limitations, a lack of skilled human resources, low digital literacy among the public, and suboptimal regulatory support and collaboration with e-commerce platforms. Therefore, strengthening institutional capacity and inter-agency synergy is essential to address the growing challenges of digital crime.

Keywords: *Cybercrime, E-Commerce Fraud, East Java Police, ITE Law, Law Enforcement*

Penegakan Hukum Tindak Pidana Terhadap Penipuan Berbasis E-Commerce: Studi Kasus Di Polda Jatim

ABSTRAK

Penelitian ini bertujuan untuk mengetahui bagaimana upaya serta kendala yang dihadapi oleh Kepolisian Daerah Jawa Timur dalam menegakkan hukum terhadap tindak pidana penipuan berbasis e-commerce yang kian marak terjadi di era digital. Penelitian ini menggunakan metode kualitatif dengan pendekatan yuridis empiris dan tipe penelitian deskriptif, melalui pengumpulan data primer berupa wawancara langsung dengan Kepala Unit Cyber Polda Jatim dan korban penipuan, serta data sekunder dari peraturan perundang-undangan seperti KUHP dan UU No. 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, ditambah dengan bahan hukum sekunder dan tersier dari berbagai literatur dan sumber relevan. Analisis dilakukan secara triangulatif dengan menggabungkan berbagai sumber data untuk meningkatkan validitas temuan. Hasil penelitian menunjukkan bahwa Polda Jatim telah melakukan berbagai upaya penegakan hukum terhadap penipuan e-commerce secara sistematis, termasuk penggunaan analisis data digital, pelibatan forensik siber, dan koordinasi dengan OJK serta BI. Namun, efektivitasnya masih terkendala oleh keterbatasan teknologi, kurangnya SDM ahli, rendahnya literasi digital masyarakat, serta belum optimalnya dukungan regulasi dan kerja sama dengan platform e-commerce. Oleh karena itu, diperlukan peningkatan kapasitas kelembagaan dan sinergi antarinstansi untuk menghadapi tantangan kejahatan digital yang terus berkembang.

Kata kunci: *Kejahatan Siber, Penegakan Hukum, Penipuan E-Commerce, Polda Jatim, UU ITE*

INTRODUCTION

The advancement of information and communication technology has driven significant digital transformation, including the emergence of a paperless era in which the use of paper continues to decline. Economic activities such as transactions, coordination, trade agreements, and proof of payment are now widely conducted in digital form through electronic mail, instant messaging, and electronic payment systems. These developments have improved efficiency, reduced waste, and supported environmental conservation efforts. Such convenience has further accelerated the rapid growth of electronic commerce, which has become increasingly prevalent in society. Technology-based companies play a substantial role in providing innovative and accessible e-commerce platforms for consumers.

Kotler and Armstrong state that e-commerce is an online platform used by business actors and consumers via computers to carry out business activities and information searches.[1] Wong further notes that e-commerce encompasses sales and marketing transactions of products and services through electronic media such as the internet, computers, radio, and television.[2] This transformation has fundamentally altered the way people shop, making it more practical and contemporary.[3]

E-commerce delivers considerable positive effects in fulfilling human needs, particularly with regard to time effectiveness and efficiency. Through e-commerce platforms, individuals are able to conduct buying and selling transactions without the necessity of direct meetings, thus removing barriers of time and location. Another advantage of e-commerce lies in its capacity to build trust through product review systems, seller reputation mechanisms, and consumer protection features provided by digital platforms. By means of these various mechanisms, electronic transactions can proceed smoothly, securely, and conveniently for both parties involved.[4]

Nonetheless, e-commerce also carries certain drawbacks, particularly concerning the absence of direct interaction between sellers and buyers. The lack of face-to-face engagement may give rise to doubts regarding product quality and the credibility of business actors. To address this issue, Indonesia has a legal framework in the form of Consumer Protection Law Number 8 of 1999, which provides protection for consumers in buying and selling transactions, including those conducted online. Among the consumer rights guaranteed under this law are the right to accurate and clear information, the right to receive goods in accordance with agreed terms, and the

[1] Principles of Marketing, Philip Kotler, Gary M. Armstrong (2017)
[2] Internet Marketing for Beginners, Jony Wong (2013)
[3] Setiawan, dkk "Tindak Pidana Penipuan Pada Transaksi E-Commerce Dimasa Pandemi Covid-19," Era Hukum: Jurnal Ilmiah Ilmu Hukum 19 (2021): 183–202.
[4] Dedi Riswandi and Transaksi On-Line, "Transaksi On-Line (E-Commerce): Peluang Dan Tantangan Dalam Perspektif Ekonomi Islam," Jurnal Econetica 1, no. 1 (2019): 1–13.

right to return goods or obtain compensation in the event of a violation. This regulation is essential in balancing technological progress with the protection of consumer rights.[5]

Surveys indicate that public understanding in Indonesia regarding online fraud schemes remains suboptimal, with only 54 percent of respondents demonstrating awareness of such methods. Paradoxically, approximately 21 percent of those respondents had already become victims of online fraud, and 28 percent had experienced fraud conducted under the guise of e-commerce platforms. The most frequently used methods involve the Telegram and WhatsApp applications, with fraud patterns consisting of prize lottery schemes (55 percent) and shopping vouchers (37 percent). This situation underscores the critical importance of improving digital security education within society. Digital literacy is urgently needed to enable the public to recognize signs of fraud and take preventive measures when conducting online transactions, including verifying the authenticity of accounts, hyperlinks, and offers received.[6]

Within the jurisdiction of the East Java Regional Police, e-commerce fraud cases have continued to display a concerning trend. In 2020, three major cases were recorded, namely bicycle purchase fraud involving losses of Rp30,500,000, garlic purchase fraud involving 1.5 tonnes of goods with losses of Rp14,835,090, and face mask sales fraud involving losses of up to Rp160,330,000 marketed through Instagram. In 2021, reports of online fraud cases increased to 176 cases, yet only 60 cases were successfully resolved, with the remainder still under investigation or left unresolved. Although the number of reported cases declined to 29 in 2022, this figure does not necessarily reflect an improvement in case handling, but may instead be attributed to a decrease in public willingness to file reports.[7][8]

The weakness of law enforcement against online fraud constitutes one of the primary reasons for the recurring nature of this crime. Many cases are treated as ordinary offences and therefore not handled with sufficient seriousness, despite the fact that the financial losses incurred are substantial and affect a large number of victims. Legal instruments such as Article 378 of the Criminal Code and Article 28 paragraph (1) of the Electronic Information and Transactions Law (UU ITE) are already available to prosecute perpetrators. Article 378 regulates fraud committed through deception or false pretences to obtain unlawful gain, carrying a maximum penalty of four years' imprisonment. Article 28 paragraph (1) of the UU ITE, meanwhile, prohibits the

[5] Agustanti, Dika, and Setiawan, "Tindak Pidana Penipuan Pada Transaksi E-Commerce Dimasa Pandemi Covid-19."
[6] Harianto Rantesalu and Penanggulangan Kejahatan, "Penanggulangan Kejahatan Penipuan Belanja Online Di Wilayah Kepolisian Daerah Jawa Timur," Janaloka Jurnal 1, no. 2 (2022): 70–94
[7] Ibid., 70–94.
[8] T Y Rahmanto, "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik," Jurnal Penelitian Hukum DE JURE 19, no. 1 (2019): 31–52

dissemination of false information that causes harm to consumers in electronic transactions. However, without firm law enforcement and officials who understand the complexity of digital crime, these regulations have yet to produce a sufficient deterrent effect.[9]

Each of the three prior studies makes important contributions individually, yet collectively they leave significant gaps unresolved. Akbar, Kamal, and Badaru examined the effectiveness of the role of the police in online fraud law enforcement, but their discussion remains general in scope and does not specifically address the East Java jurisdiction.[10] Suarno, Puluhuwa, and Wantu investigated the effectiveness of criminal law regulations pertaining to cybercrime, yet their study is normative in character and does not empirically examine the specific inhibiting factors in the handling of cyber fraud cases.[11] Meanwhile, the research by Shona Azi et al. constructs a normative argument regarding the role of the UU ITE in e-commerce regulation, but stops at the regulatory level without examining how law enforcement officials in the field implement the regulation or the obstacles they encounter in its application.[12]

Accordingly, three principal gaps remain unaddressed by prior research. First, no study has specifically examined e-commerce fraud law enforcement at the operational level of a Regional Police institution, in particular the East Java Regional Police. Second, the overlapping application of Article 378 of the Criminal Code and Article 28 paragraph (1) of the UU ITE in the handling of e-commerce fraud cases in the field has never been examined in depth using empirical data obtained directly from investigators handling these cases. Third, the preventive and repressive dimensions as two approaches to law enforcement have never been studied simultaneously within a single, comprehensive, empirically grounded case study. This research is presented to address all three of those gaps.

This study aims to empirically analyse the implementation of law enforcement against e-commerce fraud offences by the Special Criminal Investigation Cyber Unit (Siber Reskrimsus) of the East Java Regional Police, encompassing the application of Article 378 of the Criminal Code and Article 28 paragraph (1) of the UU ITE within both preventive and repressive approaches, while simultaneously identifying the

[9] S Yulianto, *Regulasi Dan Kebijakan Dalam Menanggulangi Kejahatan Siber Di Indonesia* (Jakarta: Universitas Indonesia Press, 2024)

[10] Akbar, M.A., Kamal, M., & Badaru, B. (2024)
"Efektivitas Peran Kepolisian Terhadap Penegakan Hukum Tindak Pidana Penipuan Online Di Dunia Maya" Journal of Lex Philosophy (JLP), Vol. 5 No. 2, hlm. 877–893

[11] Mohamad Suarno Nur, Fenty Puluhuwa, & Fence M. Wantu (2023)
"Kebijakan Penegakan Hukum dalam Upaya Menangani Cyber Crime yang Dilakukan oleh Polri Virtual di Indonesia" Jurnal Ilmu Hukum the Juris, Vol. 7 No. 2, hlm. 464–470. DOI: 10.56301/juris.v7i2.1122 STIH Awang Long, Samarinda

[12] Shona Azi, dkk. (2024) "Peran UU ITE dalam Regulasi E-Commerce di Era Digital" Jurnal Ilmu Hukum, Humaniora dan Politik (JIHHP), Vol. 5 No. 1, hlm. 258–267. DOI: 10.38035/jihhp.v5i1.2900.

inhibiting factors faced by field officers, including dimensions of regulation, limitations in digital forensic technology, human resources, and inter-agency coordination, with the objective of producing a comprehensive overview as a basis for policy recommendations toward more effective and adaptive law enforcement in response to the development of cybercrime in Indonesia.

LITERATURE REVIEW

Law Enforcement Theory

The term "law," etymologically speaking, derives from an Arabic word meaning "rule" or "decision," and is known in Latin as *rectum* or *ius*, both of which are rooted in the concepts of governance and justice.[13] Law does not constitute merely a system of technical rules, it also carries moral, ethical, and symbolic dimensions that are deeply embedded in humanistic perspectives and social structures. Accordingly, law is not simply a written norm but rather a reflection of the values of justice and harmonious social order.[14]

Van Apeldoorn asserts that no single definition of law is entirely satisfactory given its complex and dynamic nature. In general terms, however, law may be understood as a set of binding rules of conduct that aim to create order, peace, and justice within society. Soerojo Wignjodipoero defines law as a body of commands, prohibitions, and permissions that regulate human behavior in order to achieve harmonious communal life. Within this context, law functions not only as an instrument of social control but also as an expression of fundamental human values directed toward achieving a life that is orderly, just, and balanced, both at the individual and collective levels.[15]

Theory of Legal Effectiveness

The theory of legal effectiveness represents an approach within legal scholarship that emphasizes the importance of public compliance with legal norms as a measure of the success of a legal system.[16] Law is viewed not merely as text or regulation, but as a living social system within society. Legal effectiveness reflects the extent to which law is capable of achieving its primary objectives, namely justice and social order. For this reason, law will not function optimally if it is positioned solely as a normative symbol without the active support of those who apply it in practice.

---

[13] S Laurensius Arliman and Penegakan Hukum Dan Kesadaran, "Penegakan Hukum Dan Kesadaran Masyarakat," 2015
[14] Ibid.
[15] Pengantar Ilmu Hukum (1981), Soerojo Wignjodipoero
[16] S Soekanto, Faktor-Faktor Yang Mempengaruhi Penegakan Hukum (Jakarta: RajaGrafindo Persada, 1983).

Lawrence M. Friedman proposed that legal effectiveness is measured across three dimensions: legal substance, legal structure, and legal culture. Legal substance refers to the quality and relevance of the content of the law in relation to the needs of society. Legal structure encompasses the institutions and law enforcement apparatus responsible for applying those rules. Legal culture, in turn, reflects the values, attitudes, and behaviors of society in relation to the law.[17] All three dimensions must operate in a synergistic manner for law to function optimally. In this context, the theory of legal effectiveness serves as a bridge between normative law and social reality, while simultaneously functioning as an analytical tool for identifying weaknesses within an existing legal system.[18]

In its application, this theory calls for legal inquiry that is both empirical and multidisciplinary in orientation. When law fails to correspond with social values or cannot be applied in a practical manner, its effectiveness diminishes. In Indonesia, the challenges to legal effectiveness are considerably complex, ranging from weak law enforcement and overlapping regulations to a low culture of legal compliance within society. Improving legal effectiveness therefore requires comprehensive legal reform, including the strengthening of official integrity, broader public participation, and more equitable legal education across all segments of society.[19]

RESEARCH METHODOLOGY

This study employs a qualitative method with a juridical-empirical approach and a descriptive research type to examine law enforcement against e-commerce fraud offences at the East Java Regional Police. Through direct interviews, observation, and library research, this study seeks to understand the practical and factual implementation of law based on Law Number 19 of 2016 and Law Number 8 of 1981.

Data were collected from three categories of legal materials, namely primary materials consisting of interviews and statutory regulations, secondary materials consisting of books, articles, and academic journals, and tertiary materials consisting of legal dictionaries and encyclopedia. Data collection was conducted through both field studies and library research. The data were then analyze using triangulation techniques and a qualitative descriptive method.

The analysis process was carried out through the sequential stages of selection, classification, systematization, and inductive conclusion drawing based on the facts obtained in the field. This research was conducted at the East Java Regional Police,

[17] L M Friedman, The Legal System: A Social Science Perspective (New York: Russell Sage Foundation, 1975)
[18] Rahardjo, Penegakan Hukum: Suatu Tinjauan Sosiologis
[19] J Habermas, Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy (Cambridge: MIT Press, 1996)

located at Ahmad Yani Road Number 116, Surabaya, commencing on 23 March 2024 and continuing until the completion of the study.

RESULT AND DISCUSSION

Legal Framework for Law Enforcement Against E-Commerce Fraud at the East Java Regional Police

Fraud is an act carried out with the intention of deceiving or misleading another person in order to obtain personal gain or to cause harm to another party. Under the Criminal Code (KUHP) as stipulated in Law Number 1 of 2024, fraud is categorised as a criminal offence pursuant to Article 378. This article provides that any person who intentionally deceives another by furnishing false information, using a fabricated identity, or misrepresenting a situation in order to obtain unlawful benefit may be subject to criminal sanctions in the form of imprisonment and/or a financial penalty.[20]

In practice, perpetrators of fraud frequently exploit the negligence, trust, or ignorance of victims in order to execute their schemes. The consequences of such fraud may include financial losses as well as psychological harm to the victim. In more serious cases where fraud is carried out on a large scale, involves a syndicate, or causes significant harm to victims, perpetrators may be subject to heavier sanctions as provided under Article 379b of Law Number 1 of 2024.[21]

As technology continues to advance, the forms of fraud have become increasingly varied and frequently exploit digital media. E-commerce fraud represents one form of cybercrime that has grown progressively widespread alongside the expansion of electronic commerce. Common methods employed in this type of fraud include the sale of fictitious goods, theft of personal data, and fraudulent investment schemes disguised as marketplace platforms.[22]

Beyond fictitious goods schemes, e-commerce fraud may also occur in the form of financial information theft, such as the acquisition of credit card numbers or electronic wallet account credentials belonging to victims. Techniques such as phishing and malware are frequently used to deceive users into surrendering their personal data. In certain cases, perpetrators pose as customer service representatives of e-commerce platforms in order to solicit sensitive information from victims. Such conduct falls within the category of electronically-based fraud as regulated under Article 379c and may be subject to heavier criminal sanctions when carried out in an organized manner.[23]

---

[20] R Sudjana, Kriminalitas Ekonomi Dan Penipuan di Indonesia (Bandung: Penerbit Universitas Padjadjaran, 2020).
[21] A Nasution, Tindak Pidana Penipuan: Kajian Hukum Dan Implementasinya di Indonesia (Medan: Universitas Sumatera Utara Press, 2024)
[22] H Riyanto, E-Commerce Fraud: Fenomena, Dampak, Dan Strategi Pencegahan (Yogyakarta: Penerbit UII, 2021).
[23] "Pasal Penipuan Online."

In response to the growing prevalence of e-commerce fraud, the government and digital platforms have continued their efforts to strengthen security systems and to educate the public on how to conduct safe transactions over the internet. Among the preventive measures available to users are verifying the reputation of sellers, using secure payment methods, and avoiding transactions conducted outside official platforms. Furthermore, Article 379d of Law Number 1 of 2024 implicitly grants law enforcement authorities the power to investigate suspicious electronic transactions and to block accounts or websites that are proven to have been used for fraudulent activities.

In East Java, a number of e-commerce fraud cases have been reported by law enforcement authorities in recent years. The following are cases of e-commerce fraud that occurred in East Java between 2021 and 2024:

1. Fake Online Stores[24]

   One prominent case involved a fraud scheme using fake online stores operating through social media platforms. Perpetrators offered electronic products at discounted prices to attract potential buyers. Once victims had transferred funds, the perpetrators severed all communication and disappeared without delivering the promised goods. Such conduct falls within the general category of fraud prosecutable under Article 378 of Law Number 1 of 2024.[25]
2. Phising

   Another case occurring in this jurisdiction involved phishing fraud targeting users of popular marketplace platforms. Perpetrators sent fraudulent hyperlinks resembling official e-commerce websites, prompting users to enter personal data such as email addresses, passwords, or banking information. Upon obtaining access to the victim's account, the perpetrators rapidly redirected funds or conducted unlawful transactions in the victim's name. Such conduct may be prosecuted under Articles 379c and 379d of Law Number 1 of 2024 on the grounds of exploiting technology to commit criminal acts.[26]
3. Online Scamming syndicates

   In addition, the Directorate of Special Criminal Investigation (Ditreskrimsus) of the East Java Regional Police has previously uncovered an e-commerce fraud syndicate network operating across multiple provinces. The perpetrators used false identities and fictitious bank account numbers to carry out transactions. In an operation conducted in 2023, police successfully apprehended several suspects and seized various items of evidence including electronic devices, ATM cards, and forged documents used in the fraudulent activities.[27] Given that these acts were carried out on a large scale and involved

[24] Rantesalu, H. (2022). Penanggulangan Kejahatan Penipuan Belanja Online di Wilayah Kepolisian Daerah Jawa Timur. Janaloka Jurnal, 1(2), 70–94.
[25] "Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan Online."
[26] "Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan Online."
[27] Susanto, Pencegahan Dan Penanganan Kejahatan Siber: Peran Pemerintah Dan Swasta

a syndicate, the perpetrators may be charged under Article 379b of Law Number 1 of 2024, which governs organized fraud causing significant harm.

Efforts and Obstacles in Law Enforcement Against E-Commerce Fraud at the East Java Regional Police

Law enforcement against e-commerce fraud offences presents a distinct challenge for law enforcement authorities in the current digital era. The East Java Regional Police, through the Special Criminal Investigation Cyber Unit (Siber Reskrimsus), has implemented various strategic measures in addressing this form of cybercrime, though their execution has not been without a number of complex obstacles. The following section outlines the efforts, obstacles, and solutions undertaken in the enforcement of e-commerce fraud law at the East Java Regional Police.

1. Law Enforcement Efforts by the Special Criminal Investigation Cyber Unit (Siber Reskrimsus) of the East Java Regional Police

   In addressing the growing prevalence of e-commerce fraud, the Special Criminal Investigation Cyber Unit (Siber Reskrimsus) of the East Java Regional Police has implemented structured and technology-based legal measures.

   The initial step involves the application of Article 378 of the Criminal Code concerning fraud and Article 28 paragraph (1) of Law Number 11 of 2008 on Electronic Information and Transactions (UU ITE), which governs the dissemination of misleading information that causes harm to consumers. The combined application of these provisions furnishes a strong legal basis for prosecuting perpetrators who commit crimes through digital platforms. The East Java Regional Police also conducts perpetrator profiling and pattern analysis of victim reports in order to uncover connections between cases and broader fraud networks. In an interview, the Head of Section II of Sub-Directorate II of the Cyber Criminal Investigation Directorate of the East Java Regional Police, Rio Armando S.H., S.Psi, affirmed that *"Article 28a paragraph (1) of the UU ITE is used for online-based fraud, while Article 378 of the Criminal Code is still applied to more conventional cases."* The combined use of both provisions affords investigators legal flexibility to adapt their application to the specific characteristics of each case, whether entirely digital or conventional in nature but involving technological elements.

   The subsequent step involves the collection of intelligence materials (Pulbaket), which encompasses not only physical items but also digital data such as communication trails, online transaction records, and perpetrator identities traced through fraudulent accounts. The informant stated, *"Our first step is to profile the perpetrator, we gather whatever information is related to*

the perpetrator, then we summon the victim for a detailed examination of the chronology of events."

Given the numerous obstacles encountered in case handling, *Reskrimsus* of the East Java Regional Police collaborates with digital forensic experts and relevant agencies. The informant further stated that coordination is conducted with several parties including banks and social media administrators, with the aim of obtaining information on financial flows or suspicious account activity in the context of cyber fraud. Intensive coordination is also conducted with the Financial Services Authority (OJK), Bank Indonesia (BI), and the Attorney General's Office to ensure that legal proceedings proceed smoothly and accurately.

The case presentation stage serves as the concluding step to determine whether a case will proceed to formal investigation or be discontinued due to insufficient evidence. The handling of e-commerce fraud is oriented not only toward punishment but also toward protecting the public from increasingly complex digital crime. This approach demonstrates that the East Java Regional Police operates not merely in a reactive capacity but also in a preventive and adaptive manner in responding to the evolving methods of fraud. The *Reskrimsus* unit serves as the frontline in maintaining digital security, continuously updating its strategies in line with technological developments and the evolution of cybercrime.

2. Inhibiting Factors in Law Enforcement Against E-Commerce Fraud at the East Java Regional Police

   Alongside the various efforts that have been undertaken, law enforcement against e-commerce fraud offences at the East Java Regional Police is not without a number of significantly inhibiting factors. These obstacles encompass various dimensions, ranging from limitations in resources and technology and low levels of public digital literacy to the complexity of transnational cybercrime syndicate networks. The following section outlines the inhibiting factors faced by *Siber Reskrimsus* of the East Java Regional Police in handling e-commerce fraud cases.

   a. Limitations in Resources and Technology

      Perpetrators of fraud employ sophisticated methods such as social engineering and software that is difficult to trace. Law enforcement officers face obstacles due to a lack of adequate digital forensic technology and limited human resources, particularly when perpetrators are located abroad. This impedes the effectiveness of the investigative process. In an interview, an informant disclosed that "*The challenge is that perpetrators are more observant, faster, and more precise in executing their methods; we face difficulties in conducting investigations because of our standard operating procedures, especially*

when perpetrators are not within Indonesian jurisdiction." These limitations include a lack of adequate digital forensic equipment as well as human resources with specialized expertise in cybercrime investigation.

b. Low Levels of Public Digital Literacy

Members of the public who are not yet technologically literate, particularly elderly individuals and those from lower economic backgrounds, constitute easy targets. They are susceptible to deception by fraudulent advertisements and implausible offers due to insufficient understanding of the risks associated with online transactions. In the interview, it was disclosed that "Indeed, this lack of understanding plays the primary role; people who are technologically illiterate are easily victimized by online fraud." The informant further added that victims who frequently fall prey to cyber fraud tend to come from elderly and middle-income groups, and that based on reports received, many of them had taken out loans and consequently suffered losses twice over.

c. Regulatory Obstacles

Although legal regulations already exist governing criminal offences, namely Article 378 of the Criminal Code addressing fraud in general terms whether offline or online, and Article 28 paragraph (1) of the UU ITE addressing the dissemination of misleading information on digital media and electronic transactions that harm consumers, their implementation has not been optimal. The law frequently fails to keep pace with the rapid evolution of fraud methods, whereby conventional cases may transition into digital ones. Law enforcement officials stated that *"Article 28 paragraph (1) of the UU ITE is used for false or misleading information, but sometimes cases shift from conventional to ITE cases due to the use of the internet as a medium of fraud."* This reflects the absence of a coherent and focused legal framework.

d. Tracing Difficulties

The continuous advancement of technology has simultaneously been exploited by cybercriminals to obstruct the tracing process. The use of fake accounts, virtual private networks (VPNs), and overseas servers is employed to prevent their activities from being detected by national monitoring systems. Fictitious identities and digital data that can be easily deleted complicate the evidentiary process and prolong legal proceedings. Regarding the tracing difficulties encountered at the East Java Regional Police, an informant stated that *"The evidentiary challenge lies in digital data that can be quickly deleted and information that is deliberately made fictitious,"* adding that *"intermediary perpetrators can also be used when fictitious information is known by*

proxy actors." The informant further explained that the use of technology such as VPNs and overseas servers also complicates tracing, since perpetrators using VPNs are effectively outside Indonesian legal jurisdiction, meaning that law enforcement authorities no longer hold the authority to act. This situation demonstrates that the obstacles to tracing perpetrators are not merely technical in nature but also touch on jurisdictional dimensions that require cross-border handling.

e. Insufficient Coordination with E-Commerce Platforms and Financial Institutions

E-commerce platforms and financial institutions are in principle cooperative and fully supportive of investigative processes; however, requests for information must be submitted through administrative channels. This is carried out by sending formal letters to the relevant e-commerce platform or financial institution, which naturally requires a longer processing time and results in delays in law enforcement response beyond what the situation warrants. The East Java Regional Police explained that *"There are several cooperative arrangements, but all must go through a formal information request letter,"* and that *"They support us by providing all the information we need."* This indicates that the obstacle lies not in the unwillingness of the relevant parties to cooperate, but rather in the slow bureaucratic process that requires every step to be communicated in writing and formally. In the handling of cyber fraud cases that demand rapid response, the time lag resulting from this administrative process may lead to the loss of digital evidence or the escape of perpetrators. This underscores the need for a more efficient system of communication and data exchange between institutions.

f. Cybercrime Syndicates

Cyber fraud is no longer carried out on an individual basis but has evolved into criminal activity conducted by organized networks operating across regions and even across national borders. Methods such as phishing and fraudulent applications are frequently employed, while extradition treaties with certain countries where perpetrators are located have yet to be established. An informant stated that *"The trend of e-commerce fraud increases every year and is largely carried out by extensive networks,"* and that *"The use of fraudulent applications, phishing, and the sending of malicious links causes enormous losses as all funds in the victim's account disappear."* The situation becomes more complex when perpetrators are located outside Indonesian legal jurisdiction. The absence of extradition treaties with a number of

countries in which perpetrators take refuge constitutes a genuine obstacle in the law enforcement process, since Indonesian law enforcement authorities do not have direct authority to arrest or prosecute perpetrators who fall under the jurisdiction of another state. This situation illustrates that the handling of cybercrime syndicates requires an approach that transcends the boundaries of national law.

3. Causative Factors Behind E-Commerce Transaction Fraud Offences

In addition to the inhibiting factors in law enforcement, there are also underlying factors that contribute to the prevalence of fraud offences in e-commerce transactions within society. These factors are interconnected, ranging from social, economic, and technological dimensions to the weakness of existing regulations. The following section outlines the causative factors behind e-commerce transaction fraud offences as identified in this study.

a. Insufficient Public's Digital Literacy

Fraud in e-commerce transactions occurs frequently due to low levels of digital literacy within society. Many victims come from groups that do not understand the risks of online transactions and readily trust offers of prizes or discounts without verification. This is reinforced by the statement of the Public Relations Division of the East Java Regional Police that *"Public understanding of the paradigm of online fraud cases is necessary; it is frequently technologically illiterate individuals or the elderly who are affected,"* and that *"This lack of understanding plays the primary role; technologically illiterate individuals are easily victimized by online fraud, they lack sufficient understanding and their devices are not adequately protected."*

b. Weak Oversight of Personal Data Security

Personal data breaches provide an opening for criminal actors to execute fraud schemes. One method identified by the East Java Regional Police is phishing, whereby victims are directed to fraudulent websites and perpetrators subsequently gain free access to the victim's personal data. The Public Relations Division stated *that "Victims are usually provided with a link after being contacted, then their phone hangs after the link is clicked, after which the victim is asked to transfer a small amount of funds, but thereafter all funds in the victim's account disappear as a result of hacking."* The informant further added that some perpetrators are known to continue carrying out their activities from within correctional facilities, as seen in a case at the Madiun Correctional Institution where a perpetrator was still able to access communication devices illegally.

The issue of personal data security is not solely the responsibility of users but must also be a matter of concern for platform

providers. Inadequately secured systems, weak two-step verification, and carelessness in sharing information through social media or messaging applications heighten the risk. When digital security systems are not continuously improved, perpetrators can easily infiltrate and steal data. Moreover, the fact that inmates are able to access digital devices demonstrates that internal oversight within correctional facilities remains lax, creating continued opportunities for perpetrators to carry out their activities.

c. High Levels of Unemployment

The economic situation also serves as a trigger for the increase in this type of criminal offence. Many victims are drawn in by promises of instant financial returns from investment schemes or fraudulent cooperative savings groups. In an interview, law enforcement officials stated that *"The form is usually bait promising reciprocal benefits,"* and that *"It predominantly targets technologically illiterate individuals, the elderly, and those facing economic hardship; many have even reported taking out loans and suffering losses twice over."*

High unemployment rates and economic difficulties render the public more susceptible to enticing offers that promise large returns in a short period of time. Schemes such as online cooperative savings fraud or fraudulent investment schemes exploit the economic vulnerability of victims seeking a way out of financial hardship. Regrettably, rather than obtaining financial gain, victims suffer losses twice over: both materially and psychologically. This situation is exacerbated by the ease with which perpetrators can disseminate fraudulent promotions through social media and messaging applications with minimal oversight.

d. Weak Regulations and Law Enforcement Systems

The East Java Regional Police acknowledges that inaccuracies persist in the application of regulations, as the type of online fraud may overlap between the Criminal Code and the UU ITE. It was explained that *"The basic legal instrument used is Article 28 paragraph (1) of the UU ITE, while for other matters the Criminal Code is used for general fraud cases; Article 378 remains relevant."* The informant further conveyed that the UU ITE and the Criminal Code are still being deliberated upon so that criminal law in cyber fraud cases may be regulated with greater clarity.

e. Increasingly Sophisticated Fraud Methods

Continuous technological innovation brings not only benefits but also serves as a vehicle for cybercriminals to develop digital fraud methods, ranging from prize offers and fraudulent applications to social *engineering techniques such as pretexting. An informant explained that*

"The form is usually bait that promises reciprocal benefits, and it is not merely a one-time approach but is systematized." The informant also identified emerging trends in cyber fraud, including the use of fraudulent applications for phishing purposes, illegal access to websites, and the disruption of the victim's device for several seconds after a malicious link is clicked.

f. Insufficient Public Education and Outreach by Authorities

Public education efforts are considered to have not yet reached an optimal level, despite the fact that vulnerable groups such as the elderly and members of the general public are greatly in need of guidance on how to conduct safe online transactions. This was emphasized by the informant serving as the Public Relations representative of the East Java Regional Police, who stated *that "The public needs to understand the paradigm of online fraud."* Large-scale public outreach remains a significant responsibility yet to be fully discharged by government agencies.

The absence of sustained educational campaigns and outreach regarding digital security leaves the public without the foundational knowledge required to recognize potential fraud. The role of government institutions, law enforcement agencies, and e-commerce platforms is of considerable importance in educating the public through various media, both online and offline. Without continuous and strategic educational efforts, the openings for fraud will persist. Education should reach down to the smallest community level, with content that is easy to comprehend, particularly for groups that are most vulnerable to victimization.

CONCLUSION

Based on the research findings outlined in the preceding discussion, it can be concluded that law enforcement against e-commerce fraud offences at the East Java Regional Police is carried out through a systematic and technology-based approach. *Reskrimsus* of the East Java Regional Police applies Article 378 of the Criminal Code and Article 28 paragraph (1) of the UU ITE as the primary legal foundations, combined with proactive digital crime pattern mapping through data analysis and the monitoring of suspicious online activity. The collection of digital evidence is conducted in collaboration with cyber forensic experts to ensure the admissibility of evidence, while coordination with the Financial Services Authority (OJK) and Bank Indonesia is maintained to close the financial loopholes that are frequently exploited by perpetrators.

Notwithstanding these efforts, law enforcement activities continue to face a number of considerably significant obstacles. Limitations in technology and the shortage of human resources with competence in cyber investigation constitute

fundamental barriers, further compounded by low levels of public digital literacy that render the public vulnerable to continuously evolving fraud methods. From a regulatory standpoint, existing provisions have not yet been fully capable of reaching perpetrators who operate using false identities, while the limited obligation placed upon e-commerce platforms to support investigations makes it difficult for law enforcement authorities to obtain the necessary data. Insufficient coordination among law enforcement agencies, e-commerce platforms, and financial institutions further slows the response to case handling. Beyond this, the presence of cybercrime syndicates operating across regions and even across national borders adds considerable complexity to law enforcement efforts, owing to the jurisdictional limitations held by domestic authorities.

REFERENCES

Agustanti, Rosalia, Dika, dan Ahmad Setiawan. "Tindak Pidana Penipuan Pada Transaksi E-commerce Dimasa Pandemi Covid-19." Era Hukum: Jurnal Ilmiah Ilmu Hukum 19 (2021): 183–202.

Habermas, Jürgen. Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy. Cambridge: MIT Press, 1996.

Hasil wawancara dengan Panit II Subdit II Ditreskrimsus Polda Jatim, Rio Armando, S.H., S.Psi., pada 13 Juni 2025.

Laurensius Arliman, S. Penegakan Hukum Dan Kesadaran Masyarakat. Jakarta: [Nama penerbit tidak dicantumkan], 2015.

Nasution, A. Tindak Pidana Penipuan: Kajian Hukum Dan Implementasinya Di Indonesia. Medan: Universitas Sumatera Utara Press, 2024.

Rahardjo, Satjipto. Penegakan Hukum: Suatu Tinjauan Sosiologis. Yogyakarta: Genta Publishing, 2009.

Rahmanto, T. Y. "Penegakan Hukum Terhadap Tindak Pidana Penipuan Berbasis Transaksi Elektronik." Jurnal Penelitian Hukum DE JURE 19, no. 1 (2019): 31–52.

Rantesalu, Harianto. "Penanggulangan Kejahatan Penipuan Belanja Online Di Wilayah Kepolisian Daerah Jawa Timur." Janaloka Jurnal 1, no. 2 (2022): 70–94.

Riyanto, H. E-commerce Fraud: Fenomena, Dampak, Dan Strategi Pencegahan. Yogyakarta: Penerbit UII, 2021.

Riswandi, Dedi. "Transaksi On-Line (E-commerce): Peluang Dan Tantangan Dalam Perspektif Ekonomi Islam." Jurnal Econetica 1, no. 1 (2019): 1–13.

Soekanto, Soerjono. Faktor-Faktor Yang Mempengaruhi Penegakan Hukum. Jakarta: RajaGrafindo Persada, 1983.

Sudjana, R. Kriminalitas Ekonomi Dan Penipuan Di Indonesia. Bandung: Penerbit Universitas Padjadjaran, 2020.

Susanto, Budi. Pencegahan Dan Penanganan Kejahatan Siber: Peran Pemerintah Dan Swasta. Jakarta: Gramedia Pustaka Utama, 2021.

Yulianto, S. Regulasi Dan Kebijakan Dalam Menanggulangi Kejahatan Siber Di Indonesia. Jakarta: Universitas Indonesia Press, 2024.

"Cara Menentukan Pasal Untuk Menjerat Pelaku Penipuan Online." Hukumonline. 2024. https://www.hukumonline.com.

"Pasal Penipuan Online." Hukumonline. 2024. https://www.hukumonline.com.