Journal of Law Science
Volume 7, No. 3, 2025
e-ISSN 2684-9658 pp. 496-502
www.iocscience.org/ejournal/index.php/JLS

Law enforcement against online fraud on e-commerce platforms based on law no. 19 of 2016

Nurani Sofiyana[1], Rina Arum Prastyanti[2]
[1,2]*Program Studi Hukum, Universitas Duta Bangsa, Surakarta. Email: nuranisofiyana571@gmail.com*

ARTICLE INFO

Keywords:

E-Commerce Platforms;
Electronic Transactions;
ITE Law;
Law Enforcement;
Online Fraud.

Article history:

Received May 12, 2025;
Revised Jun 3, 2025;
Accepted Jun 24, 2025;
Online Jul 30, 2025.

ABSTRACT

The rapid spread of information and communication technology, particularly e-commerce, has changed the way economies transact around the world, expand markets, and make it easier. However, along with these advances, a new problem has arisen in the form of increasing cases of online fraud that are detrimental to consumers. Online fraud, especially those that occur on e-commerce platforms, is one of the main problems that threatens consumer trust in companies (Hartanto, 2016). *This qualitative study was carried out with normative juridical methods. This method looks at laws and regulations, case studies, and academic research. The study found different types of online fraud, ranging from sending goods that don't fit the description or counterfeit goods to using the wrong payment system. Despite the fact that the ITE Law provides a strong legal basis for cracking down on fraudsters, there are several challenges in implementing it* (ZAHRA, 2025). *These include constraints with digital forensic human resources and difficulties in identifying and tracking perpetrators. Additionally, the lack of digital literacy makes the situation worse because consumers are more vulnerable to fraud. As a result, this study suggests increasing the technical capacity of law enforcement officials, cross-sector collaboration between the government and the public, and better digital literacy programs to create a safe, fair, and trustworthy e-commerce ecosystem (Andreaningrum et al., 2024).*

Corresponding Author:

Nurani Sofiyana,
Business and Law Faculty,
Universitas Duta Bangsa,
Jl. Ki Mangun Sarkono No.20, Nusukan, Banjarsari, Surakarta, Jawa Tengah, 57135, Indonesia
Email: nuranisofiyana571@gmail.com

1. Introduction

Aspects of human life have changed due to advances in information and communication technologies, including trade. With ease of access, process speed, and wide market coverage, e-commerce is now one of the main means for people to make transactions to buy and sell goods and services online. E-commerce offers many benefits for consumers and business actors. However, behind this convenience, there is a new risk in the form of many online fraud crimes that harm the community. This issue is very important because the number of fraud cases continues to rise, indicating a gap between regulations and law enforcement, despite the existence of regulations (Sanusi, 2024).

However, there are new challenges behind the ease, especially the increase in online fraud cases. Fraud can be carried out in a variety of ways, such as using a fake identity, sending goods that don't match the description, delivering goods after payment, or tampering with the payment system. This action undermines public trust in the electronic commerce system in Indonesia, in addition to harming consumers financially (Dianta, 2023).

The development of information technology has changed the way people transact, especially through e-commerce platforms that make online transactions easier and more efficient. Platforms such as Tokopedia, Shopee, and Bukalapak are increasingly popular among Indonesians of various demographics. However, this increase allows cybercriminals to commit various types of fraud, such as identity forgery, the sale of counterfeit goods, and the misuse of personal data. The situation has worsened due to several factors, including the lack of digital literacy among some consumers and the lack of verification of business actors on digital platforms (Hukum & Pasundan, 2024).

The data shows a huge increase in online fraud cases from 2014 to 2022. There were 62 cases recorded in 2014, and this number continues to increase until it reaches 191 cases in 2022. This shows that this threat is increasingly real and serious. This increase shows an increase in the number of internet and e-commerce users as well as weaknesses in consumer protection systems and limited law enforcement efforts. Therefore, online fraud on e-commerce platforms should be considered a legal and social issue that requires serious attention from governments, law enforcement, platform providers, and society itself. It's not just a technical problem (Purnama Ramadani Silalahi et al., 2022).

The Government of Indonesia passed Law Number 11 of 2008 concerning Electronic Information and Transactions (ITE Law) to create a clear legal basis for electronic activities. Law Number 19 of 2016 improves several provisions in the ITE Law, especially those related to clearer definitions, regulations on the implementation of electronic systems, strengthening people's rights in using the internet, and stricter regulations (Fathurrachman & Dian Alan Setiawan, 2022).

In the case of online fraud, Article 28 paragraph (1) of the updated ITE Law emphasizes that: "Everyone deliberately and without the right to spread false and misleading news that results in consumer losses in Electronic Transactions." The act is criminally threatened based on Article 45A paragraph (1) of Law 19/2016, which states: "Every person who deliberately and without the right spreads false and misleading news as referred to in Article 28 paragraph (1) shall be sentenced to imprisonment for a maximum of 6 (six) years and/or a maximum fine of Rp1,000,000,000.00 (one billion rupiah)."

Law Number 19 of 2016 also explains several important things about electronic transactions. First, Article 26 establishes the responsibility of the Electronic System Operator (PSE) to protect user data, stating that the use of data must be based on the consent of the individual concerned. Second, Article 40 paragraphs (2a) and (2b) regulate the removal of unlawful content, including content related to fraud, which the state authorities decide. Third, this law also includes more detailed provisions on the procedure for investigating cybercrimes. This is done to clarify the authority of investigators in handling violations in the digital field. Fourth, to protect consumers from various forms of online crime, consumer rights are strengthened in electronic transactions (Suharto, 2024).

Given this situation, law enforcement efforts to combat online fraud on e-commerce platforms cannot rely on existing laws. A comprehensive strategy is needed that includes strengthening law enforcement officials, cross-sectoral collaboration between the government, e-commerce platforms and the community, and prevention efforts through digital literacy and education. It is hoped that the electronic commerce ecosystem in Indonesia will become safer, more transparent, and more reliable for all parties involved if all parties work well together (Annastasyia Mukrimah Yusuf, Ma'ruf Hafidz, 2024).

2. Method

This study uses a qualitative approach. This method aims to analyze the law as a standard that governs public behavior, especially in terms of law enforcement Law Number 19 of 2016 against online fraud that occurs on e-commerce platforms. There are three main approaches: the legal approach, the case approach, and the conceptual approach. Primary legal materials are laws and court decisions, secondary legal materials are scientific literature and journals, and tertiary legal materials are legal dictionaries and encyclopedias. The data collection method consists of studying regulations, academic literature, and relevant court decisions. This normative juridical method is chosen to study the doctrinal interpretation of digital legal provisions. On the other hand, the conceptual method contextualizes the modus operandi of fraud within legal theory (Trisnawati, 2023).

The applicable legal provisions are described, their application in specific cases, and the obstacles to online fraud law enforcement are identified through a descriptive-qualitative analysis of the data obtained. This research not only tracks actual conditions but also offers solutions to improve legal protection for consumers in electronic transactions in the digital age. It is hoped that this research will make a theoretical and practical contribution to the development of cyber law and consumer protection in Indonesia (Rodriguez de las Heras Ballell, 2017).

3. Analysis and Results

3.1. Forms and Modes of Online Fraud that occur on E-Commerce Platforms

Fraud that occurs online on e-commerce platforms is now an increasingly complicated and difficult problem to overcome. The fraud modes used by perpetrators are increasingly diverse and sophisticated along with the rapid development of digital technology. Fraud like this threatens public trust in e-commerce platforms that are supposed to be convenient and safe for transactions.(Albert, 2002) They also take consumer money. Online scams that often occur on e-commerce platforms are as follows:

a) Shipping Goods Not Up To Description: This is one of the mostcommon modes of fraud. Actors usually offer very interesting product descriptions, either in terms of quality, price, or features. Consumers are swayed by seductive information and then pay. However, when customers receive the product, they find that it does not meet the promised description of the quality, color, size, or even the type of product itself. For example, people buy electronic devices with certain specifications, but the ones they receive turn out to have much lower specifications or even counterfeit goods. The existence of ambiguity in product descriptions or the lack of strict control procedures on e-commerce platforms are the two main factors causing this mode (Eka Putri & Kartika Wati, 2024).

b) Fictitious Goods: Thieves sell items that are not real or do not exist at all. Advertisements for products that seem to be real and at very attractive prices are made by the perpetrators. The promised goods are not delivered until the consumer is interested and pays. Offenders typically use fake identities or easy-to-delete accounts to avoid recognition and protect themselves from legal action. Because fraudsters often delete accounts or change their digital identities after committing fraud, it is difficult for consumers or authorities to track the whereabouts of these unreal items (Streel & Husovec, 2020).

c) Not Delivering Goods After Payment: In this mode, the perpetrator makes a transaction that initially appears legitimate. The perpetrator offers the object that appears attractive to the consumer, but after they pay, the perpetrator disappears without delivering the item in question. After the transaction is completed, the perpetrator usually simply disappears, so the customer only receives a fake notification or no delivery confirmation at all. This

mode is increasingly popular on e-commerce platforms that do not have sufficient verification or consumer protection systems. Additionally, some perpetrators use fake accounts, which are often altered or deleted to avoid further searches (Setyawan et al., 2023).

d) Payment System Manipulation: This category includes fraud committed by individuals who use errors or flaws in payment systems available on e-commerce platforms. For example, perpetrators may redirect transactions from secure payment systems to personal accounts or ask customers to pay through platforms that are more vulnerable to fraud. In some cases, the perpetrator may also request payment through unprotected methods, such as direct transfers to personal bank accounts or using third-party apps that don't have clear security guarantees. Since transactions are not recorded on the e-commerce platform in question, this mode often causes customers to lose their money without the goods received (Anderson et al., 2012).

e) Use of Fake Identities: This type of fraud involves people using fake identities or accounts to manipulate consumers. On e-commerce platforms, perpetrators often create profiles that appear to be very legitimate. They can impersonate well-known sellers or merchants, or even fake positive reviews and ratings to attract customers' attention. After making a transaction, the perpetrator then deceives the customer in a similar way to other methods, such as sending an inappropriate product or even not delivering the item at all. Consumers feel deceived because they think they are transacting with people who are supposed to be trustworthy (Porter, 2021).

This mode of online fraud not only harms customers financially but also damages public trust in e-commerce platforms. Consumer trust relies heavily on the assurance that e-commerce platforms can conduct safe and reliable transactions. As scams like this continue to occur, customers become more vigilant and may avoid online transactions. As a result, the development of the digital economy can be hampered. Additionally, consumers can experience loss of money, time, and even personal data that is misused.

Overall, this diversity of fraud modes shows that online fraudsters are increasingly adept at exploiting the weaknesses of existing e-commerce systems. This shows that while e-commerce platforms offer a lot of convenience, they also need to be more proactive in building secure and transparent systems. Online fraud can be reduced with the strict application of laws and increased public awareness of the security of digital transactions (Izazi et al., 2024).

3.2. Law Enforcement against Online Fraud Based on Law No. 19 of 2016

To handle and take strict action against fraudulent practices that harm consumers, especially in the rapidly growing world of electronic commerce, Law Number 19 of 2016 concerning Electronic Information and Transactions (ITE Law) provides a clear legal framework to deal with the problem of online fraud that often occurs on e-commerce platforms. The presence of this law is increasingly important to ensure that users of e-commerce services are safe and secure as online transaction activities increase (Ramli et al., 2020).

Article 28 paragraph (1) of the ITE Law has one of the most important provisions related to the control of online fraud. A person can be subject to criminal penalties if "Everyone knowingly and without rights spreads false and misleading news resulting in consumer losses in electronic transactions." This provision is intended to prevent fraudsters from deceiving customers by using electronic media. This scam is usually done by displaying counterfeit goods, selling inappropriate items, or telling potential buyers false promises (Afriani & Hidayati, 2024).

Article 45A paragraph (1) of the ITE Law stipulates that perpetrators who are proven to have committed acts as mentioned in Article 28 paragraph (1) can be sentenced to imprisonment for a maximum of six years or a maximum fine of Rp1,000,000,000.00. These sanctions show that the state takes the crime of fraud in electronic transactions seriously and seeks to punish the

perpetrators. It is hoped that this strict provision will increase people's sense of security when transacting electronically and reduce the rate of online fraud (Tuju et al., 2025).

Law No. 19 of 2016 regulates the protection of user data in addition to the provisions of false information. Article 26 requires Electronic System Operators (PSEs) to maintain the confidentiality, integrity, and security of user data. PSE can also only use such data with the user's consent. This is an important component of e-commerce transactions, where the security of customer data must be maintained so that irresponsible parties do not misuse it (Nurlaili Janati et al., 2023).

Article 40 paragraphs (2a) and (2b) of the ITE Law add to consumer protection by requiring e-commerce platforms to remove content or electronic information that contains unlawful content, including content related to fraud. In other words, PSEs are obliged to remove or terminate access to such content in cases where counterfeit products or fake offers are sold on their platform. The goal is to avoid further losses for customers (Indonesia, 2024).

The law enforcement process against online fraud cases still faces many challenges even though a fairly complete legal framework is available. One of the main problems is that it is difficult to find and supervise fraudsters who often use fake accounts and fake identities and use technologies such as VPNs to disguise their existence. The process of investigating, arresting, and prosecuting cybercriminals is hampered by this circumstance (Simanungkalit et al., 2024).

These various obstacles show that the handling of online fraud cases is highly dependent on the strength of laws such as the ITE Law and how the law is applied in the field. There is a need for increased technical capacity of the apparatus, more cooperation between e-commerce platforms and law enforcement officials, and broader digital literacy programs throughout the community. To create a safe, fair, and trustworthy e-commerce environment for all users, effective law enforcement must be combined with systematic prevention efforts. ITE has more specific sanctions for online fraud compared to the Criminal Code and the Consumer Protection Law, but digital evidence and identification issues complicate enforcement.

4. Conclusion

Along with the rapid use of digital technology in trading transactions, online fraud is on the rise on e-commerce platforms. Consumers have been harmed and lost trust in e-commerce platforms due to various fraudulent modes, including shipping goods that do not match descriptions, counterfeit goods, and payment system manipulation. Law Number 19 of 2016 (ITE Law) regulates law enforcement against internet fraud perpetrators. However, there are some obstacles in its implementation, such as difficulties in identifying perpetrators and lack of digital forensic resources. Therefore, governments, e-commerce platforms, and the public must work together to better protect consumers through better law enforcement and broader digital literacy training. E-commerce fraud not only requires legislation but also better investigations and proactive cooperation between regulators and platforms.

Acknowledgments

From the beginning of the report's creation to its conclusion, the author has benefited greatly from the advice and help of numerous people. The author would like to use this opportunity to thank the, Almighty God for His unending grace, which allowed him to finish writing this report. Professor Dr. Rina Arum Prastyanti, S.H., M.H., who has offered guidance, critiques, and inspiration in addition to motivation. The writer's parents, who are a constant source of guidance and encouragement. The writer's friends, who have consistently accompanied and assisted the writer.

References

Afriani, A. A., & Hidayati, M. N. (2024). Analisis Pelanggaran Pasal UU ITE dalam Praktik E-Commerce di Indonesia (Studi Kasus Pada Grab Toko Indonesia). *Innovative: Journal Of Social Science Research*, *4*(3), 14700–14711.

Albert, M. R. (2002). E-buyer beware: Why online auction fraud should be regulated. *American Business Law Journal*, *39*(4), 575–644. https://doi.org/10.1111/j.1744-1714.2002.tb00306.x

Anderson, R., Barton, C., Boehme, R., Clayton, R., Van Eeten, M. J. G., Levi, M., Moore, T., & Savage, S. (2012). Measuring the Changing Cost of Cybercrime. *The Economics of Information Security and Privacy*, 1–32. https://weis2019.econinfosec.org/wp-content/uploads/sites/6/2019/05/WEIS_2019_paper_25.pdf

Andreaningrum, K. I., Thelma, K., & G, M. O. (2024). Penegakan Hukum terhadap Tindak Pidana Penipuan terhadap Konsumen dalam Usaha Jual Beli Online di Kota Kupang. *Jurnal Hukum, Politik Dan Ilmu Sosial (Jhpis)*, *3*(3).

Annastasyia Mukrimah Yusuf, Ma'ruf Hafidz, H. K. (2024). Journal of Lex Philosophy (JLP). *Journal of Lex Philosophy (JLP)*, *5*(1), 260–275.

Dianta, D. (2023). Urgensi Penegakan Hukum E-Commerce di Indonesia: Sebuah Tinjauan Yuridis. *Arus Jurnal Sosial Dan Humaniora*, *3*(1), 1–14. https://doi.org/10.57250/ajsh.v3i1.173

Eka Putri, N. A., & Kartika Wati, R. (2024). Law Enforcement of Thrifting Practices Through Overseas Online Thrift Shops with Instagram Applications. *Jurnal Indonesia Sosial Teknologi*, *5*(8), 3787–3796. https://doi.org/10.59141/jist.v5i8.1319

Fathurrachman, F., & Dian Alan Setiawan. (2022). Pertanggungjawaban Pidana Bagi Pelaku Affiliator terhadap Korban Trading Binary Option Ditinjau dari UU Nomor 19 Tahun 2016 tentang Perubahan Atas UU Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. *Bandung Conference Series: Law Studies*, *2*(2), 1011–1017. https://doi.org/10.29313/bcsls.v2i2.2536

Hartanto, O. D. J. K. S. (2016). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan Lewat Jual Beli Online (E-Commerce) dan Perlindungan Hukum Terhadap Korbannya (Studi Di Wilayah Hukum Polresta Surakarta). *Universitas Muhammadiyah Surakarta*, *01*(19), 1–23. https://eprints.ums.ac.id/118408/

Hukum, F., & Pasundan, U. (2024). *Rewang Rencang : Jurnal Hukum Lex Generalis. Vol.5. No.8 (Agustus 2024) Tema/Edisi : Hukum Pemerintahan (Bulan Kedelapan) https://jhlg.rewangrencang.com/*. *5*(8), 1–15.

Indonesia, D. I. E. S. (2024). *TERHADAP PELAKU USAHA DALAM TRANSAKSI ONLINE SECARA CASH ON DELIVERY (COD)*. https://doi.org/10.55551/jip.v5i2.142

Izazi, F. S., Sajena, P., Kirana, R. S., & Marsaulina, K. (2024). Perlindungan Hukum Terhadap Konsumen dalam Transaksi E-Commerce Melalui Undang-Undang Nomor 8 Tahun 1999 Tentang Perlindungan Konsumen dan Peraturan Pemerintah (PP) Nomor 80 Tahun 2019 Tentang Perdagangan Melalui Sistem Elektronik. *Leuser: Jurnal Hukum Nusantara*, *1*(2), 8–14. https://journal.myrepublikcorp.com/index.php/leuser/article/view/73

Nurlaili Janati, Delima Afriyanti, & Ficha Melina. (2023). Perlindungan Konsumen Pada Platform Belanja Online Perspektif Hukum Ekonomi Islam. *Syarikat: Jurnal Rumpun Ekonomi Syariah*, *6*(1), 134–147. https://doi.org/10.25299/syarikat.2023.vol6(1).13839

Porter, J. (2021). Commentary: Inefficiencies in Digital Advertising Markets: Evidence from the Field. *Journal of Marketing*, *85*(1), 30–34. https://doi.org/10.1177/0022242920970133

Purnama Ramadani Silalahi, Aisy Salwa Daulay, Tanta Sudiro Siregar, & Aldy Ridwan. (2022). Analisis Keamanan Transaksi E-Commerce Dalam Mencegah Penipuan Online. *Profit: Jurnal Manajemen, Bisnis Dan Akuntansi*, *1*(4), 224–235. https://doi.org/10.58192/profit.v1i4.481

Ramli, T. S., Ramli, A. M., Permata, R. R., Ramadayanti, E., & Fauzi, R. (2020). ASPEK HUKUM PLATFORM e-COMMERCE DALAM ERA TRANSFORMASI DIGITAL. *Jurnal Studi Komunikasi Dan Media*, *24*(2), 119. https://doi.org/10.31445/jskm.2020.3295

Rodriguez de las Heras Ballell, T. (2017). The Legal Anatomy of Electronic Platforms: A Prior Study to Assess the Need of a Law of Platforms in the EU. *The Italian Law Journal*, *3*(1), 149–176.

Sanusi, M. F. (2024). *Perlindungan Hukum Terhadap Korban Tindak Pidana Penipuan Yang Dilakukan Oleh Pelaku Usaha E-Commerce Berbasis Transaksi Elektronik*. *5*(November), 171–178.

Setyawan, A., Setyabudi, C. M., & Nita, S. (2023). Strategy To Build Public Awareness In Preventing Online Fraud Crimes In The Jurisdiction Of The Cimahi Police. *International Journal of Social Service and Research*, *3*(10), 2641–2649. https://doi.org/10.46799/ijssr.v3i10.563

Simanungkalit, J. A. R., Hertadi, R., & Hosnah, A. ul. (2024). Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya. *AKADEMIK: Jurnal Mahasiswa Humanis*, *4*(2), 281–294. https://doi.org/10.37481/jmh.v4i2.754

Streel, A. De, & Husovec, M. (2020). *Requested by the IMCO committee The e-commerce Directive as the*

cornerstone of the Internal Market. *May*.

Suharto, A. (2024). *ONLINE PERSPEKTIF UNDANG- UNDANG INDONESIA INFORMASI ELEKTRONIK (STUDI PADA*. *September*.

Trisnawati, D. (2023). Tinjauan Yuridis Terhadap Tindak Pidana Penipuan Secara Onlineberdasarkan Undang-Undang Nomor 11 Tahun 2008 Jo Undang-Undang Nomor 19 Tahun 2016 Tentang Informasi Dan Transaksi Elektronik. *Jurnal Ilmu Sosial*, *2*(9), 1991–2006.

Tuju, M. C., Ramadani, S., & Nasution, C. (2025). *Penegakan Hukum Terhadap Tindak Pidana Cyber dalam Kasus Penipuan Jual Beli Online dalam Perspektif Kriminologi*. *5*, 1763–1776.

ZAHRA, Y. I. (2025). *Analisis Yuridis Perlindungan Hukum Terhadap Anak*. 411–418.