Analysis of Online Fraud Crimes With Cashback and Commission Offer Modes Through Online Media

Restika Ndruru, Muhammad Arif Sahlepi

Abstract
This study aims to analyze online fraud crimes with the mode of offering cashback and commissions through social media, including legal arrangements, victim protection, and obstacles in law enforcement. The method used is normative juridical with literature studies, reviewing laws and regulations, legal literature, and related documents. The results of the study showed that the crime of fraud was regulated in Article 378 of the Criminal Code for conventional fraud as well as Article 28 and Article 45A of the ITE Law (Law No. 11 of 2008 and Law No. 19 of 2016) for online fraud, providing a criminal threat of up to six years in prison and/or a maximum fine of Rp1 billion. Legal protection for victims includes the right to material compensation through compensation and restitution, supported by a professional judicial process, and preventive efforts through digital literacy and public education. Online fraud modes include phishing, scams, and shared card info, while obstacles to disclosure of perpetrators include the use of fake identities, complex banking bureaucracy, low professionalism of investigators, and limited digital investigation support facilities. The implications of the research emphasize the need to strengthen the capacity of law enforcement officials, optimize ITE Law regulations, and increase public digital literacy and awareness as preventive measures in dealing with the diversification of online fraud modes.

Keywords: *Online Fraud*, *Cashback*, Social Media, ITE Law, Legal Protection

Restika Ndruru
Master of Laws Study Program, Universitas Pembangunan Panca Budi, Indonesia
E-mail: restikandruru7@gmail.com

Muhammad Arif Sahlepi
Master of Laws Study Program, Universitas Pembangunan Panca Budi, Indonesia
e-mail: arifsahlepi@dosen.pancabudi.ac.id
2nd International Conference on Islamic Community Studies (ICICS)
Theme: History of Malay Civilisation and Islamic Human Capacity and Halal Hub in the Globalization Era
https://proceeding.pancabudi.ac.id/index.php/ICIE/index

Introduction

The development of digital technology in recent years has had a significant impact on the pattern of people's activities, including in internet-based transaction and communication activities. These advances bring a variety of conveniences, but at the same time trigger an increasingly diverse increase in cybercrime. One of the most common forms of crime is online fraud, which is an action carried out through online media to deceive victims with the aim of obtaining financial benefits and personal data illegally. Online fraud is defined as the use of internet services or internet-based software to manipulate, take personal data, or make false transactions that can harm victims both materially and morally.

Juridically, online fraud in Indonesia is regulated in Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE) as amended by Law Number 19 of 2016 and Law Number 1 of 2024. Article 28 paragraph (1) of the ITE Law prohibits everyone from spreading false and misleading news that can cause consumer losses in electronic transactions. Furthermore, Article 45A paragraph (1) of the ITE Law provides provisions for criminal sanctions in the form of imprisonment for a maximum of six years and/or a maximum fine of Rp1,000,000,000, for perpetrators of violations of this article [1]. This provision is the main legal basis in handling online fraud crimes in Indonesia, including those that use the *Cashback*, commissions, and fake prizes.

In recent years, online fraud modes have been growing and taking advantage of users' weaknesses in understanding the flow of digital transactions. One of the modes that is often used is *offering cashback* and commissions through online media, which provides the lure of instant profits to victims. This pattern is usually carried out through cell phones, short messages, messaging applications, and social media by disguising themselves as official parties such as marketplaces, delivery services, or certain companies. This mode has proven to be effective in ensnaring victims because the perpetrator creates a convincing communication atmosphere, supported by evidence of fake transactions, fake website links, and messaging groups featuring fictitious members to strengthen the victim's belief.

Online fraud with the mode of luring rewards or commissions is one form of digital crime that has shown a rapid increase in recent years. Perpetrators usually use psychological manipulation techniques through an intensive interpersonal approach so that the victim feels confident and finally willing to follow all the instructions given by the perpetrator [2]. Social media is the most dominant means in the spread of the reward fraud mode because of its ability to reach many users quickly and widely, while providing space for perpetrators to build convincing fictitious identities [3]. This condition is exacerbated by the low digital literacy of the community, which makes many individuals more easily influenced by offers of financial benefits that seem rational even though they are misleading. Therefore, the importance of adaptive and responsive regulation is becoming increasingly urgent, especially to deal with the diversification of digital crime modes that continue to grow [4].

The phenomenon of online fraud with *cashback* and commission modes does not only occur in general in society, but is also experienced directly by authors, who in 2025 get a prize offer, then directed to join certain groups of applications and websites, follow the instructions of the perpetrator, and make transactions that lead to significant financial losses. This case shows that the mode makes use not only of social engineering, but also of the structure of organized organized crime, involving fake accounts, fictitious identities, and reward systems designed to build the trust of victims. This fact reinforces the urgency of research on how this mode works, how the legal framework governs it, and how the forms of protection should be applied to prevent the recurrence of similar cases.

Social media provides a huge stage for scammers to expand their networks and exploit people online. They can quickly connect with more people and easily create fake profiles as well as use unauthorized identities to commit fraud. Online fraud can be done through a variety of means, such as fraud via email, SMS, or chat apps. These online scams can be identity fraud,

financial fraud, or information fraud. In recent years, online fraud has increased significantly, and it has become a major concern for governments and other organizations [5].

The scientific novelty in this study lies in the focus of analysis on online fraud modes that combine *cashback* offering, commission, and reward techniques as a systematically structured crime strategy. Although much research on cybercrime has been conducted, specific studies on *cashback* and commission fraud patterns through online media are still limited, especially from the perspective of criminal law and consumer protection. This study seeks to fill this gap by providing an in-depth analysis of operational patterns, criminal responsibility of perpetrators, and legal implications for victims.

Based on this description, the research problems in this article are directed at legal arrangements, modus operandi, and obstacles in law enforcement against online fraud crimes with the mode of *offering cashback* and commission through online media, as follows:

1. What is the law that regulates the crime of fraud?
2. What is the legal protection for victims and efforts to prevent online fraud on social media?
3. What are the modes and obstacles faced in exposing perpetrators of online fraud crimes on social media?

This research aims to gain a comprehensive understanding of online fraud crimes with the mode of *offering cashback* and commissions through online media. In particular, this study aims to examine the legal provisions that are the basis for regulating these criminal acts, explain the forms of legal protection and prevention efforts that can be provided to victims, and analyze the modus operandi and obstacles faced by law enforcement officials in uncovering and taking action against online fraud perpetrators with *cashback* and commission modes.

Literature Review

Online fraud is a crime committed through the internet or digital platforms with the aim of obtaining illegal profits through the act of deceiving victims [6]. The modus operandi of online fraud varies, including *Phishing*, social engineering, and financial lure schemes such as *Cashback* or commission. This fraud not only causes financial losses but also has the potential to access the victim's personal data, increasing the risk of identity theft [7]. The literature shows that the complexity of online fraud modes is increasing as digital technologies and *E-commerce platform*.

Offer *Cashback* And commissions are one of the modes of online fraud that has emerged as a new phenomenon. Perpetrators set up formal-looking mechanisms, such as social media groups or dedicated websites, to show evidence of fake transactions and convince victims to transfer funds with the promise of greater returns [8]. This mode utilizes the victim's psychology through social pressure and false social evidence so that the victim is encouraged to follow the perpetrator's instructions. This shows that this kind of scheme falls under the category *Investment scam* and *Social Engineering* which has the potential to deceive many users.

Online fraud in Indonesia is regulated through Article 378 of the Criminal Code concerning fraud and Law Number 11 of 2008 concerning Information and Electronic Transactions which has been updated through Law Number 19 of 2016 and Law Number 1 of 2024. Article 28 paragraph (1) of the ITE Law prohibits the dissemination of misleading information that harms consumers in electronic transactions while Article 45A paragraph (1) establishes criminal sanctions for violations. Although the legal framework is in place, law enforcement implementation faces the challenges of digital proof, the use of fake identities, and complex cross-jurisdictional transactions [9].

Legal protection for victims of online fraud includes preventive and repressive measures. Preventive measures include digital literacy, public education, and platform security policies. Repressive measures include case reporting, digital forensic investigations, freezing of holding accounts, and asset recovery. Synergy between victims, digital platforms, banks, PPATK, and

law enforcement officials is needed to accelerate asset recovery and increase the effectiveness of law enforcement [10].

Law enforcement against online fraud faces obstacles in the form of the use of fake identities, third-party accounts, servers outside the jurisdiction, and rapid movement of funds. Empirical studies state that effective mitigation strategies include increasing the digital forensic capacity of the apparatus, cross-agency and international cooperation, and the development of an efficient and victim-friendly reporting system. The implementation of this strategy has been proven to increase the effectiveness of prevention and enforcement against online fraudsters [11].

Research Methodology

This research uses a normative juridical approach, which is legal research that examines legal materials as a basis for studying legal problems. This approach views law as a norm that applies in society and is used as a reference to assess the right or wrong of an action.

The data collection technique is carried out through library *research* by tracing and reviewing laws and regulations, legal documents, and literature relevant to the research topic. Literature studies aim to identify, classify, and analyze existing legal norms.

The types of legal materials used include:

1. Primary legal materials are binding legal sources, such as the Criminal Code, ITE Law Number 11 of 2008 and its amendments through Law Number 19 of 2016, and Consumer Protection Law Number 8 of 1999.
2. Secondary legal materials are legal literature, legal expert books, scientific articles, journals, research results, and legal expert opinions.
3. Tertiary legal materials are legal dictionaries, encyclopedias, and legal indexes to understand technical terms.

The collected data is analyzed objectively to answer the legal problems raised, through relevant legal approaches, cases, and legal theories. The analysis is carried out systematically to produce conclusions that are in accordance with the applicable legal norms.

Research Results

4.1 Laws Governing the Crime of Fraud

The crime of fraud has a clear legal basis both in terms of normative and information technology regulations. In general, Article 378 of the Criminal Code (KUHP) stipulates that fraud is an act committed by deception, a series of lies, the use of a false name, or false circumstances with the intention of unlawfully benefiting oneself. Perpetrators who are proven to have committed fraud can be sentenced to a maximum prison sentence of four years. This provision confirms that national criminal law has long recognized and sanctioned fraudulent practices as a form of unlawful acts that harm other parties.

In the digital era, fraudulent practices are no longer limited to face-to-face interactions, but rather expand through electronic media. The Electronic Information and Transaction Law (ITE Law), which has been revised through Law No. 1 of 2024, provides a special legal umbrella for fraud committed online. Article 28 of the ITE Law prohibits the dissemination of false information through electronic systems, while Article 45A regulates criminal threats of up to six years in prison and/or a maximum fine of Rp 1 billion for perpetrators. These regulations not only strengthen the legal foundation against traditional fraud, but also provide relevant legal protections in the context of increasingly complex and evolving cybercrime.

Online fraud is carried out through various *platform* social media or *Marketplace*, with a mode such as *Phishing*, *Scamming*and *Social Engineering*. Scams can also take advantage of the spread of fake news to harm others or benefit oneself. According to Pratiwi & Fernando, emphasizing that law enforcement only on the Criminal Code without the ITE Law is still weak in dealing with online fraud [12]. Meanwhile, according to Amelia, the integrated application

of the Criminal Code and the ITE Law provides a stronger legal basis to crack down on online fraudsters [13].

4.2 Legal Protection and Online Fraud Prevention Efforts on Social Media

Legal protection aims to provide rights and security guarantees for individuals to avoid losses, including as a result of online fraud. According to C.S.T. Kansil, legal protection is an act that respects the freedom, dignity, and dignity of individuals. Technological developments, especially social media, have a positive impact such as facilitating communication, access to information, business, education, and health. However, social media also has the potential to be used as a means of crime, one of which is online fraud, which is included in the category *Cybercrime* Because of using the internet network to commit criminal acts [14].

Legal protection for victims of online fraud has been regulated through Law No. 11 of 2008 concerning Information and Electronic Transactions which was updated with Law No. 19 of 2016 (ITE Law). The ITE Law serves as a legal umbrella to ensure legal certainty for the public in conducting electronic transactions. Materially, Article 28 paragraph (1) of the ITE Law gives the victim the right to claim material damages. Based on Stephen Schafer's concept, compensation can be in the form of compensation (from the community or government) and restitution (from the perpetrator as a form of criminal liability). Online fraud can also be subject to criminal sanctions according to Article 378 of the Criminal Code with a maximum threat of 4 years in prison. This research emphasizes that effective legal protection requires the implementation of a good criminal justice system, starting from the investigation stage to the implementation of court decisions, so that victims obtain legal certainty and recover the losses experienced.

Online fraud prevention efforts depend not only on regulations and law enforcement, but also on the active participation of the public. Digital awareness, education about the use of social media, and vigilance against suspicious links or files are effective preventive measures. Law enforcers must act professionally and with integrity from the investigation stage, including the fulfillment of initial evidence and the discovery of digital evidence in accordance with the provisions of Article 183 of the Criminal Code. With optimal implementation, legal protection and online fraud prevention efforts can run synergistically, minimize the risk of public losses, and ensure legal certainty for victims.

According to Swangga Prabhaswara, the application of Article 378 of the Criminal Code and Article 28 of the ITE Law still needs to be strengthened to deal with increasingly complex fraud modes [15]. Ihsan & Burhayan pointed out that there are obstacles to investigations, such as false identities of perpetrators and limited law enforcement facilities, which have the potential to reduce the effectiveness of legal protection [15]. Meanwhile, Utomo et al, highlighted the importance of people's digital literacy as the main preventive step, especially in dealing with the mode of fraud based on part-time job vacancies on social media [16]. This comparison shows that this study is consistent with previous literature, but at the same time emphasizes the need for stronger collaboration between governments, law enforcement officials, and the public in preventing online fraud

4.3 Modes and Obstacles in Disclosure of Online Fraud Perpetrators on Social Media

Fraud that occurs through social media utilizes various modus operandi that are increasingly diverse and adaptive to technological developments and social behavior. Among them, *Phishing* i.e. sending a link that appears legitimate to steal the victim's data; *scam*, with chat or phone fraud techniques that trick victims into obtaining money; and *Shared Card* info, namely the theft of the victim's card information through the mode of contacting the victim by disguising himself as a bank or official agency and then asking for approval that seems trivial but leads to the draining of account funds. These findings are in line with studies in Indonesia

that show that online fraudsters often use social engineering techniques (*Social Engineering*) such as *Phishing* and *Spoofing* as the main mode [17].

Although legal frameworks such as the Electronic Information and Transaction Law (UU ITE) have been put in place to tackle online fraud, enforcement of fraud crimes through social media faces fundamental obstacles that hinder the effectiveness of investigation and disclosure of perpetrators. First, the difficulty of tracking the identity of the perpetrator, because the perpetrator often uses fake identities, mobile phone numbers registered in the name of other people, or bank accounts that are controlled in a hidden manner. This condition is in accordance with the findings that the complexity of proving and tracing perpetrators is the main obstacle in the enforcement of online fraud laws [18].

A number of structural obstacles aggravate the disclosure process, such as long bureaucracy in opening access to perpetrators' accounts, lack of cooperation between competent parties, low professionalism of law enforcement (investigators), and lack of facilities and infrastructure to support digital investigations. Empirical studies state that law enforcement agencies in Indonesia have limitations in terms of technological resources, personnel capacity and coordination between institutions, making the handling of online fraud cases less than optimal [19].

Conclusion

The crime of fraud is normatively regulated in Article 378 of the Criminal Code for conventional fraud as well as in Article 28 and Article 45A of the ITE Law (Law No. 11 of 2008 and Law No. 19 of 2016) for online fraud, providing a clear legal basis along with a criminal threat of up to six years in prison and/or a maximum fine of Rp 1 billion for the perpetrator. Legal protection for victims includes the right to claim material compensation through compensation or restitution, supported by the implementation of professional criminal justice and the integrity of law enforcement officials, as well as prevention efforts through digital literacy and public education in using social media. Online fraud modes include *phishing, scams*, and *shared card* info, while obstacles in the disclosure of perpetrators include the use of fake identities, complex banking bureaucracy, low professionalism of investigators, and limited digital investigation supporting infrastructure. The implications of these findings show the need to strengthen the capacity of law enforcement officials, optimize ITE Law regulations, and increase public digital literacy and awareness as preventive measures, with further research development can focus on evaluating the effectiveness of the implementation of the ITE Law in various types of online fraud modes that continue to develop.

Bibliography

[1] Law Number 1 of 2024 concerning the Second Amendment to Law Number I1 of 2oo8 concerning Information and Electronic Transactions.

[2] N. F. Azzahra, K. Ahmad, and Y. Adha, "Legal Protection for Victims of Online Fraud Due to Prize Draws," vol. 1, no. 1.

[3] N. Kumalasari and S. H. B. Wijaya, "Information Manipulation on Love Scamming Victims on Social Media: A Case Study on Information Manipulation on Women Love Scamming Victims in Semarang City," vol. 17, no. 2, 2024.

[4] M. Reza Pradana, Basir, and S. Nita, "The Phenomenon of Online Fraud and the Level of Digital Literacy of the Community as a Form of Social Change," *Journal Of Social Science Research*, vol. 4, no. 1, 2024, doi: https://doi.org/10.31004/innovative.v4i1.7863.

[5] F. N.N, N. Z, and R. R. M, "Public Awareness in Using Social Media to Avoid Online Fraud Mode," *Proceedings of the National Seminar on Education*, vol. 1, no. 1, pp. 96–103, 2024.

[6] I. T. Bakti, "Analysis of Potential Fraud in Obtaining Cashback on the Tokopedia Online Buying and Selling Application," vol. 2, no. Vol. 2 No. 2 (2023): JEKMA Journal, October 2023, 2023.
[7] T. May Lesari and N. Jane Onoyi, "Potential Analysis *Fraud* In Procurement *Cashback* On Sales *Mobile* in the App *Online* Tokopedia," vol. 15, no. 1, p. 3, 2025, doi: https://doi.org/10.37776/zuang.v15i1.1871.
[8] S. Mirfandaresky, A. Kaimuddin, and P. Prajna Paramita, "Digital Forensics in the Investigation of Fraud Crimes *Online* (Case Study in the Jurisdiction of the Ponorogo Resort Police)," *Faculty of Law, Islamic University of Malang*, vol. 28, no. 10, 2022.
[9] S. R. A. Prasad, "Legal Implications for Consumer Protection in Online Fraudulent Transactions," *Journal of Law and Citizenship*, vol. 15, no. 7, 2025, doi: Prefix%20doi.org/10.3783/causa.v2i9.2461.
[10] H. Thalib, Adrianto, and M. Ilyas, "Law Enforcement Against Online Fraud Crimes," *Journal of Lex Philosophy (JLP)*, vol. 5, no. Vol. 5 No. 2 (2024): Journal of Lex Philosophy (JLP), 2024.
[11] A. Sahfitri and R. Rosmalinda, "Digital Fraud Through Links *Phishing*," *JDH*, vol. 6, no. 2, Dec 2024, doi: 10.36859/jdh.v6i2.2881.
[12] Wiwit Pratiwi and Zico Junius Fernando, "Law Enforcement of Online-Based Fraud Crimes in Review from the Electronic Information and Transaction Law (ITE Law)," *Justice Magazine*, vol. 211, no. 2, 2021, doi: https://doi.org/10.32663/mkfh. v21i2.2378.
[13] A. Amelia, "Legal Study of the Crime of Fraud *Online*," *Global Innovation Journal*, vol. 1, no. 1, pp. 14–25, Nov 2023, doi: 10.58344/ jig.v1i1.3.
[14] Annisa Hesti Kurniawati, Dara Pustika Sukma, and Yulio Iqbal Cahyo Arsetyo, "Legal Protection for Victims of Online-Based Fraud Crimes Based on Law Number 19 of 2016 concerning Information and Electronic Transactions by Victimology," *JCI*, vol. 2, no. 9, pp. 3465–3474, May 2023, doi: 10.53625/ jcijurnalcakrawalacientífica.v2i9.5661.
[15] S. Prabhaswara, "Juridical Analysis of Fraud in the Use of Social Media," *Journal Findings*, vol. 01, no. 03, 2023.
[16] F. W. Utomo, D. R. Mauludin Insana, and E. C. Mayndarto, "The mechanism of digital fraud in society in the 5.0 era (a case study of online fraud based on part-time job vacancies that spread in society)," *WUNY Scientific Journal*, vol. 6, no. 1, pp. 32–41, Mar 2024, doi: 10.21831/jwuny.v6i1.72257.
[17] Muh. A. F. Syahril dan A. Aris, "Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act," *JLJ*, vol. 2, no. 3, pp. 198–205, Nov 2024, doi: 10.33506/jlj. v2i3.3711.
[18] Muh. A. F. Syahril dan A. Aris, "Strategies and Dynamics of Online Fraud in Indonesia: Tracing the Effectiveness of the Implementation of the Electronic and Transaction Information Act," *JLJ*, vol. 2, no. 3, pp. 198–205, Nov 2024, doi: 10.33506/jlj. v2i3.3711.
[19] Luh Putu Yeyen Karista Putri, "Online Fraud Law in Indonesia: Enforcement Challenges and Future Solutions," *National Education University of Denpasar*, vol. 12, no. 2, 2022.