

THE EFFECTIVENESS OF LAW ENFORCEMENT AGAINST ONLINE FRAUD CRIMES AT THE CRIMINAL INVESTIGATION UNIT OF THE DENPASAR CITY POLICE

I Nyoman Wiranata¹
Universitas Mahendradatta

Ni Ketut Wiratny²
Universitas Mahendradatta

Sobandi³
Universitas Mahendradatta

Correspondence : I Nyoman Wiranata (nyomanwiranata68@gmail.com)

Abstract

The rapid development of information technology has significantly transformed various aspects of social and economic activities, particularly through electronic transactions. However, these advancements have also contributed to the increasing prevalence of cybercrime, especially online fraud. The sophisticated modus operandi, use of fake identities, fraudulent bank accounts, and digital platforms have complicated criminal investigations and law enforcement efforts. This study aims to analyze the implementation of law enforcement against online fraud by the Criminal Investigation Unit of Denpasar Metropolitan Police and to identify factors affecting its effectiveness. The research employs an empirical legal method with an empirical juridical approach. Primary data were collected through interviews with investigators, while secondary data were obtained from legislation, legal literature, and scientific journals. Data were analyzed qualitatively. The findings indicate that law enforcement has generally been implemented in accordance with the Indonesian Criminal Code, the Criminal Procedure Code, Law Number 1 of 2024 concerning the Second Amendment to the Electronic Information and Transactions Law, and Law Number 2 of 2002 concerning the Indonesian National Police. Nevertheless, its effectiveness is constrained by difficulties in tracing perpetrators, limited digital forensic facilities, inadequate public digital literacy, and the complexity of electronic evidence. Improving investigators' competence, strengthening digital forensic infrastructure, enhancing inter-agency cooperation, and increasing public awareness are essential to improve the effectiveness of law enforcement against online fraud.

Keywords: Law Enforcement, Online Fraud, Cybercrime, Legal Effectiveness.

INTRODUCTION

Developments in information technology have transformed societal patterns across various sectors, including communication, commerce, payment systems, and public services. The internet has become a primary necessity, facilitating various community activities through electronic systems. While these advancements have significantly boosted Indonesia's digital economy, they have simultaneously given rise to new forms of crime that exploit information technology as a medium for criminal activity. Cybercrime—criminal acts utilizing information technology—has proliferated alongside the increasing use of electronic media. One of the most prevalent forms of cybercrime is online fraud. Such fraud is perpetrated via social media, instant messaging apps, online marketplaces, and other digital platforms, with the aim of unlawfully obtaining profit through deceitful schemes or the use of false identities.

Online fraud schemes are evolving rapidly. Common methods include the sale of non-existent goods, illegal investment schemes, fraudulent online loans, prize scams, social media account impersonation, and phishing. Perpetrators exploit low levels of digital literacy among the public and weaknesses in electronic transaction verification systems, resulting in substantial financial losses for victims. Indonesia has established a legal framework to combat fraud through the Criminal Code and has strengthened regulations via Law Number 1 of 2024 concerning the Second Amendment to the Law on Electronic Information and Transactions. Furthermore, the criminal law reform enacted through Law Number 1 of 2023 (the new Criminal Code) has reinforced protections for the public against various forms of digital crime.

Despite the existence of a legal framework, law enforcement efforts regarding online fraud continue to face various obstacles. Perpetrators frequently employ tactics such as using false identities, nominee accounts, unverified prepaid SIM cards, Virtual Private Networks (VPNs), and offshore servers, all of which complicate the processes of identification and establishing proof. Furthermore, handling electronic evidence requires digital forensic procedures that demand both technical expertise and adequate facilities. Data from the Criminal Investigation Unit of the Denpasar City Police (Polresta Denpasar) indicates that online fraud remains a prevalent criminal offense, with reports continuing to emerge annually. This situation demonstrates that the effectiveness of law enforcement depends not only on the existence of regulations but is also influenced by the professionalism of law enforcement officers, the availability of digital forensic resources, inter-agency cooperation, and the level of public legal awareness. Therefore, this research is essential to analyze the effectiveness of law enforcement regarding online fraud within the jurisdiction of the Denpasar City Police Criminal Investigation Unit.

METHOD

This study is an empirical legal study employing a socio-legal (juridical-empirical) approach. This approach involves examining applicable laws and regulations alongside field research to understand the implementation of law enforcement regarding online fraud. Data sources comprise both primary and secondary data. Primary data were obtained through interviews with investigators from the Criminal Investigation Unit (Satreskrim) of the Denpasar City Police (Polresta Denpasar) who handle online fraud cases. Meanwhile, secondary data were gathered through a literature review covering primary legal materials (laws and regulations), secondary legal materials (books, scholarly journals, and research findings), and tertiary legal materials (legal dictionaries and encyclopedias). Data collection was conducted via interviews, observation, and literature review. Finally, the data were

analyzed qualitatively by correlating normative provisions with empirical facts to draw conclusions regarding the effectiveness of law enforcement against online fraud at the Denpasar City Police Criminal Investigation Unit.

RESULTS AND DISCUSSION

Law Enforcement Implementation Regarding Online Fraud Crimes at the Criminal Investigation Unit of the Denpasar City Police

Advancements in information technology have transformed conventional crime patterns into digital-based crimes (cybercrime). One of the most frequently reported offenses to law enforcement agencies is online fraud. Such fraud is perpetrated via social media, online marketplaces, messaging apps, and other digital platforms, utilizing fake identities, anonymous accounts, and bank accounts that are difficult to trace. This phenomenon requires law enforcement agencies to adapt their enforcement mechanisms to the increasingly complex nature of digital crime. Law enforcement actions regarding online fraud by the Criminal Investigation Unit of the Denpasar City Police are conducted in accordance with the Criminal Procedure Code (KUHP), Law No. 2 of 2002 concerning the Indonesian National Police, the Criminal Code (KUHP), and Law No. 1 of 2024 regarding the Second Amendment to Law No. 11 of 2008 concerning Electronic Information and Transactions. These regulations collectively serve as the legal basis for investigators to carry out preliminary inquiries, formal investigations, evidence gathering, suspect designation, and the eventual handover of case files to the public prosecutor.

Based on the research findings in this thesis, the case handling mechanism begins with the receipt of a police report filed by the victim. Upon receipt, investigators conduct an initial clarification regarding the sequence of events, the victim's identity, and preliminary evidence—such as conversation screenshots, transfer receipts, website addresses, phone numbers, and the social media accounts used by the perpetrator. This stage serves as the basis for determining whether there is a suspected criminal offense as defined by applicable laws and regulations. If a criminal event is identified, investigators issue a Letter of Order for Preliminary Investigation. During this preliminary investigation phase, information is gathered to ascertain the perpetrator's identity, transaction locations, recipient bank accounts, and any digital traces left behind during the commission of the crime. In online fraud cases, the investigation process relies heavily on the ability to perform digital tracing of the electronic activities engaged in by the perpetrator.

The subsequent stage is the formal investigation. During this phase, investigators question the victim and other witnesses familiar with the electronic transaction, consult digital

forensic experts if necessary, and seize electronic evidence in accordance with the Law on Electronic Information and Transactions. Commonly seized items include mobile phones, computers, SIM cards, bank passbooks, ATM cards, flash drives, and other electronic devices suspected of being used to commit the crime. Electronic evidence possesses characteristics distinct from conventional evidence; investigators must ensure the integrity of the electronic data is maintained from the moment of seizure through to its examination in the digital forensics laboratory. Consequently, specific procedures are required to ensure the electronic evidence retains its probative value in court. This highlights that the successful handling of online fraud cases depends not only on the investigators' ability to locate the perpetrator but also on their ability to preserve the authenticity (integrity) of the digital evidence.

In practice, the Criminal Investigation Unit of the Denpasar City Police (Satreskrim Polresta Denpasar) coordinates with various entities, including banks to obtain information on fund transfer destination accounts, the Financial Transaction Reports and Analysis Center (PPATK) to trace financial transactions, the Financial Services Authority (OJK), the Ministry of Communication and Digital Affairs, and electronic system providers. Such cross-sector collaboration is essential, given that much of the evidence resides within electronic systems managed by third parties. Beyond repressive measures involving formal investigations, the unit also implements preventive strategies, such as raising public awareness regarding online fraud schemes, educating the public on digital transaction security, disseminating information via police social media channels, and advising the public against readily sharing personal data with unknown parties. This preventive approach embodies the police functions mandated by Law Number 2 of 2002, which emphasizes not only law enforcement action but also the prevention of criminal acts.

Viewed through the lens of Soerjono Soekanto's law enforcement theory, the enforcement of laws against online fraud by the Criminal Investigation Unit of the Denpasar City Police reflects the application of legal norms through actions taken by law enforcement officers with a focus on public protection. However, the effectiveness of this enforcement remains influenced by various factors—ranging from legal aspects, law enforcement personnel, and facilities and infrastructure to the public and the evolution of information technology itself.

Factors Influencing the Effectiveness of Law Enforcement Against Online Fraud Crimes at the Criminal Investigation Unit of the Denpasar City Police

The effectiveness of law enforcement serves as a measure of how successfully law enforcement officials achieve legal objectives—namely legal certainty, justice, and utility. According to Soerjono Soekanto, law enforcement effectiveness is influenced by five key

factors: the law itself, law enforcement personnel, facilities and infrastructure, the community, and culture. These five factors are interconnected and determine the success of handling criminal offenses, including online fraud. Research findings indicate that law enforcement operations at the Criminal Investigation Unit (Satreskrim) of the Denpasar City Police generally proceed according to established procedures; however, their effectiveness faces various normative and technical obstacles. These obstacles stem not only from limitations within law enforcement agencies but are also influenced by the evolution of information technology, which outpaces the development of legal systems and the capabilities of law enforcement institutions.

The Legal Factor (Legal Substance)

Legal substance is the primary factor influencing the effectiveness of law enforcement. Clear legislation provides the foundation for law enforcement officials to conduct inquiries and investigations, and to eventually refer cases to public prosecutors. Indonesia currently possesses an adequate legal framework for addressing online fraud, comprising the Criminal Code (KUHP), Law Number 1 of 2023 concerning the Criminal Code, the Criminal Procedure Code (KUHAP), and Law Number 1 of 2024 regarding the Second Amendment to the Law on Electronic Information and Transactions. These regulations authorize law enforcement officials to utilize electronic evidence as valid evidence during the evidentiary process.

Nevertheless, the evolution of digital crime **modus operandi** far outpaces the creation of regulations. Fraud perpetrators exploit technological advancements—such as anonymous accounts, cryptocurrency, intermediary accounts, encrypted communication apps, and overseas servers—aspects that are often not yet detailed within national law enforcement mechanisms. Consequently, investigators must exercise caution in interpreting the law to ensure that its application upholds the principle of legality. Furthermore, the cross-jurisdictional—and even transnational—nature of cybercrimes means that law enforcement requires international coordination, which cannot always be executed rapidly. Therefore, updating regulations to adapt to advancements in information technology is an urgent necessity for enhancing the effectiveness of law enforcement against cybercrime.

Law Enforcement Personnel Factor

The second factor influencing the effectiveness of law enforcement is the quality of law enforcement personnel. The professionalism, integrity, experience, and technical capabilities of investigators are crucial to the successful resolution of online fraud cases. Research findings indicate that investigators from the Criminal Investigation Unit of the Denpasar City Police have carried out their investigative duties in accordance with criminal procedural law.

Investigators have conducted witness examinations, seized electronic evidence, analyzed financial transactions, and coordinated with various relevant agencies to uncover the perpetrators' identities.

However, the evolution of digital technology necessitates the continuous enhancement of investigator competence. Handling cybercrimes requires skills in digital investigation, open-source intelligence (OSINT), blockchain tracing, electronic device analysis, and constantly evolving digital forensic techniques. Without such competency upgrades, the process of resolving cases becomes increasingly difficult. Therefore, enhancing human resource capacity—through education, digital forensics training, cyber investigator certification, and collaboration with agencies possessing information technology expertise—is a strategic step toward improving the effectiveness of law enforcement.

Facilities and Infrastructure Factor

The successful handling of online-based crimes is heavily influenced by the availability of facilities and infrastructure that support the investigative process. Unlike conventional crimes, online fraud cases require various technological tools, such as digital forensic laboratories, electronic data analysis software, electronic transaction tracking systems, mobile forensic tools, and social media analysis tools.

Research results indicate that a persistent obstacle is the limitation of digital forensic facilities; consequently, for some cases, investigators must coordinate with the Cyber Investigation Directorate of the Bali Regional Police or the National Police Forensic Laboratory to obtain results from the examination of electronic evidence. This situation results in an investigative process that takes longer than that of conventional crimes. Therefore, increasing budgets, modernizing investigative equipment, strengthening digital forensic laboratories, and developing police information systems are essential requirements for enhancing the effectiveness of law enforcement against cybercrime.

Societal Factors

Societal factors play a decisive role in the effectiveness of law enforcement. The public's level of digital literacy significantly influences both the number of victims and the success of investigation processes. Research indicates that a large proportion of online fraud victims are still prone to trusting information received via social media or messaging apps without prior verification. Victims also frequently delay reporting incidents to the police, often resulting in the loss of the perpetrator's digital footprint or the emptying of the destination bank account.

Furthermore, many people still fail to grasp the importance of preserving electronic evidence—such as conversation logs, transfer receipts, website addresses, and communication metadata—which is crucial for establishing proof. Consequently, efforts to enhance digital literacy through outreach, public education, legal awareness programs, and campaigns on electronic transaction security must be sustained. Prevention through raising public awareness is a far more effective measure than taking enforcement action after a crime has already occurred.

Cultural Factors

The societal shift toward the digital era has impacted patterns of social interaction and economic activity. The convenience of electronic transactions is often accompanied by a culture of instant gratification, a lack of caution, and a high level of trust in information circulating on social media. Fraudsters exploit this digital culture to gain profit through psychological manipulation (social engineering). Perpetrators no longer rely on physical violence; instead, they exploit victims' psychological vulnerabilities through lures involving prizes, investments, job offers, or online transactions.

On the other hand, a cultural tendency to avoid reporting crimes—often because the financial loss is perceived as minor—also hinders the effectiveness of law enforcement. Many victims choose to simply absorb the loss, leaving perpetrators free to commit crimes against others. According to Soerjono Soekanto, legal culture is a key element determining the success of law enforcement. Therefore, fostering a legal culture among the public must be pursued through legal education, the promotion of ethical social media behavior, and the cultivation of legal awareness from an early age, enabling the public to play an active role in the cybercrime prevention system.

Research findings indicate that law enforcement regarding online fraud by the Denpasar City Police Criminal Investigation Unit (Satreskrim Polresta Denpasar) has been conducted in accordance with positive law. However, this effectiveness is not yet optimal, as it remains hindered by various interconnected obstacles. An analysis based on Soerjono Soekanto's theory of legal effectiveness reveals that the most dominant factors are facilities and infrastructure, the capabilities of law enforcement officers, and the role of the public; these three factors are closely interrelated. The modernization of investigative technology must be accompanied by enhanced investigator competence and improved public digital literacy. Consequently, strategies to combat online fraud cannot rely solely on a penal approach through law enforcement; they must be combined with preventive measures—such as public education and the strengthening of electronic system security—alongside more intensive collaboration among

the Police, the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), the Ministry of Communication and Digital Affairs, banking institutions, and electronic system providers.

CONCLUSION

Based on the research findings and discussion regarding the effectiveness of law enforcement against online fraud crimes at the Criminal Investigation Unit (Satreskrim) of the Denpasar City Police (Polresta Denpasar), several conclusions can be drawn as follows:

1. First, law enforcement regarding online fraud crimes at Satreskrim Polresta Denpasar has been carried out in accordance with statutory regulations, specifically the Criminal Code (KUHP), the Criminal Procedure Code (KUHP), Law Number 2 of 2002 concerning the Indonesian National Police, and Law Number 1 of 2024 concerning the Second Amendment to the Law on Electronic Information and Transactions. The law enforcement process encompasses stages such as report intake, preliminary inquiry, formal investigation, collection of electronic evidence, examination of witnesses and experts, and the handover of the case to the Public Prosecutor. In its execution, Satreskrim Polresta Denpasar coordinates with the Financial Transaction Reports and Analysis Center (PPATK), the Financial Services Authority (OJK), banking institutions, the Ministry of Communication and Digital Affairs, and electronic system providers to support case resolution. Nevertheless, the effectiveness of case handling still faces technical obstacles due to the nature of cybercrimes, which are characterized by anonymity and can span multiple regions or even countries.
2. Second, the effectiveness of law enforcement against online fraud crimes is influenced by five key factors as outlined by Soerjono Soekanto: the law itself, law enforcement officials, facilities and infrastructure, the community, and culture. Among these five factors, the most dominant obstacles are the limited ability to trace perpetrators' identities, limited digital forensic facilities, the complexity of establishing electronic evidence, and the public's still-low level of digital literacy. Therefore, enhancing the effectiveness of law enforcement requires strengthening the capacity of investigators, modernizing digital forensics facilities, refining regulations to adapt to information technology advancements, improving inter-agency coordination, and raising public awareness regarding secure electronic transactions.

Suggestion

Based on these conclusions, the author offers the following recommendations:

1. The Indonesian National Police—specifically the Criminal Investigation Unit of the Denpasar City Police (Polresta Denpasar)—should enhance investigator competence through continuous education and training in the fields of cybercrime, digital forensics, electronic transaction analysis, and open-source intelligence (OSINT). Furthermore, investigative facilities and infrastructure need to be modernized to keep pace with the technological advancements utilized by cybercriminals.
2. The public needs to improve digital literacy, exercise caution when conducting electronic transactions, safeguard the confidentiality of personal data, and promptly report incidents to law enforcement authorities if they fall victim to online fraud. Public legal awareness is a key factor in supporting successful law enforcement efforts against cybercrime.

REFERENCES

- Achmad Ali. 2009. *Unveiling Legal Theory and Judicial Theory (Jurisprudence)*. Kencana, Jakarta.
- Barda Nawawi Arief. 2014. *Issues in Law Enforcement and Criminal Law Policy*. Kencana, Jakarta.
- Edmon Makarim. 2015. *Introduction to Telematics Law*. RajaGrafindo Persada, Jakarta.
- Law Number 1 of 2023 concerning the Criminal Code (State Gazette of the Republic of Indonesia of 2023 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6842).
- Law Number 1 of 2024 concerning the Second Amendment to Law Number 11 of 2008 concerning Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024, Supplement to the State Gazette of the Republic of Indonesia).
- Law Number 2 of 2002 concerning the Indonesian National Police (State Gazette of the Republic of Indonesia of 2002 Number 2, Supplement to the State Gazette of the Republic of Indonesia Number 4168).
- Maskun. 2013. *Cyber Crime*. Kencana, Jakarta.
- Satjipto Rahardjo. 2009. *Law Enforcement: A Sociological Perspective*. Genta Publishing, Yogyakarta.
- Soerjono Soekanto. 2016. *Factors Influencing Law Enforcement*. Rajawali Pers, Jakarta.
- The 1945 Constitution of the Republic of Indonesia.
- The Criminal Code.
- The Criminal Procedure Code.
- Widodo. 2013. *Legal Aspects of Cyber Crime*. Aswaja Pressindo, Yogyakarta.
-