E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

LAW ENFORCEMENT OF ONLINE FRAUD CRIMINAL ACTS IN OBTAINING VICTIMS' MONEY IN THE JURISDICTION OF THE BALI REGIONAL POLICE

Ni Kadek Intan Sukma Primadini[1]
Universitas Mahendradatta

Erikson Sihotang[2]
Universitas Mahendradatta

Komang Edy Dharma Saputra[3]
Universitas Mahendradatta

Correspondence : Ni Kadek Intan Sukma Primadini (intansprimadini@gmail.com)

Submited : 10-05-2026 Accepted : 09-06-2026 Published : 10-07-2026

Abstract

Regarding the recovery of funds for victims of online fraud within the jurisdiction of the Bali Regional Police, the matter is handled by the Cyber Crime Investigation Directorate (Ditres Siber). Funds cannot be automatically recovered by the police; instead, recovery occurs through legal proceedings, the freezing of bank accounts, or compensation settlements reached via restorative justice mediation. The steps required to process a report and recover losses are: 1. Initiate an initial account freeze. 2. Report the incident to the Bali Regional Police—specifically the Cyber Crime Investigation Directorate—so that the case can be pursued criminally. 2. Challenges faced by the police in handling online fraud cases include both internal and external obstacles.

Keywords: Law Enforcement, Crime, and Online Fraud

INTRODUCTION

Online fraud is a form of crime that is increasingly prevalent in Indonesia. This crime is carried out by exploiting information and communication technology (ICT) as a means to deceive victims using increasingly sophisticated and difficult-to-detect methods. In some cases, online fraud not only harms victims financially but can also have significant psychological consequences. Therefore, addressing online fraud crimes is crucial. Online fraud is an act carried out via the internet or digital media with the intent of defrauding others by stealing their money or personal information. In the context of economic crimes, online fraud can be categorized as a form of crime that harms the economic aspects of society. Therefore, addressing online fraud crimes from an economic perspective is crucial to protect the public and strengthen national economic security.

Problem Formulation

By looking at the background above, the following problem formulation can be drawn: first, how is the law enforcement against online fraud crimes in recovering victims' money in the jurisdiction of the Bali Regional Police, and second, what are the obstacles in enforcing the law against online fraud crimes in the jurisdiction of the Bali Regional Police.

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

Purpose of Writing

This study aims to find out and analyze in depth the law enforcement against online fraud crimes in recovering victims' money along with the obstacles faced.

METHOD

The research method used in this research is a normative research method supported by empirical research that uses various types of primary legal materials in the form of laws and regulations and secondary legal materials in the form of library materials related to law enforcement against online fraud crimes in recovering victim's money as a source of research material. Johnny Ibrahim is of the opinion that normative legal research is a form of scientific research aimed at finding the truth based on the logic of legal science reviewed from the normative part, or which is in the form of an effort to discover law that is adapted to a particular case.

RESULTS AND DISCUSSION

Law Enforcement Against Online Fraud Crimes in Recovering Victims' Money in the Bali Police Jurisdiction

According to Simons, a crime is an unlawful act committed intentionally or unintentionally by a person who can be held responsible for his actions, which are declared by law as punishable. With these limitations, according to Simons, for a crime to occur, the following elements must be met: 1) Human actions, both in the sense of positive actions (doing) and negative actions (not doing); 2) Threatened with punishment; 3) Against the law; 4) Done with error; and 5) By a person who is capable of being responsible. With this explanation, it is concluded that all the requirements for a crime are attached to the criminal act. Simons does not separate criminal acts from criminal responsibility. If this opinion is followed, then if someone commits murder, for example in Article 338 of the Criminal Code, but then the person who committed the murder turns out to be a person who is not capable of being responsible, for example because of insanity, then in this case it cannot be said that a crime has occurred. It can be easily explained why this event cannot be called a crime, because the elements of a criminal act are not fulfilled, namely the element of a person who is not capable of being responsible. Because there is no crime, there is no punishment.

Crime, as a social phenomenon occurring on earth, will likely never end in line with the developments and social dynamics within society. This problem of crime seems to continue to grow and never recede, both in terms of quality and quantity. This development causes concern for society and the government. Crime is a form of deviant behavior that is always present and inherent in every form of society. In the sense that crime will always exist, like disease and death, which always recur, just as the seasons change from year to year.

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

Fraud itself essentially always begins with an act of persuasion using lies to easily gain the trust of the person being persuaded. Fraud comes from the word "tipu," which means dishonest or deceitful actions or words, falsehoods, and so on, intended to mislead, deceive, or seek profit. Fraud is an act that harms another person and is therefore subject to criminal penalties.

Due to the numerous crimes committed and the resulting unrest within society, laws are necessary to reduce crime. Essentially, every law enacted by lawmakers represents a legal response to societal issues at the time it was enacted. Legal development should align with societal developments. As society changes or evolves, laws must evolve to manage all developments in an orderly manner amidst the growth of modern society. One of the factors behind the enactment of the Electronic Transactions (ITE) Law is the increasing prevalence of crime in society, necessitating legal developments to fulfill its function of providing a sense of security. This law is expected to discourage people from committing mistakes, thereby reducing crime.

An electronic transaction is a legal act involving an agreement between a seller and a buyer, conducted using media such as computers, gadgets, the internet, or other electronic media, as defined by the ITE Law. A legal bond or legal relationship conducted electronically, where buying and selling activities involve a combination of electronic media networks such as computers and gadgets with a network-based communication system, namely the internet, is the definition of an electronic transaction. Electronic commerce contracts, e-commerce transactions, and web contracts are other terms frequently used in e-commerce. Therefore, an electronic transaction is a trade transaction between a seller and a buyer that utilizes electronics as the medium and the internet as the connecting network. The process of ordering goods, payment for ongoing transactions, and delivery of goods are communicated electronically via internet-connected media.

Fraud in electronic transactions, also often referred to as online fraud, is a fraudulent crime that refers to activities using computers, gadgets, and anything else that uses an internet network. Electronic transactions themselves have their own characteristics, including: 1. Borderless transactions, where an online business with consumers and growing in various countries has very large capital without any restrictions; 2. Anonymous transactions, namely transactions that do not require face-to-face contact, identity names, or other identification between the seller and buyer; 3. Digital and non-digital goods/products, namely the products sold are digital products such as software that can be downloaded via the internet and non-digital products such as electronic goods and daily necessities such as clothing, vehicles, etc.,

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

and 4. Intangible products/goods, namely products that do not have a form such as files, software, or ideas that are sold on the internet.

The police are the guardians of the community and are supposed to prevent any crimes that arise within the community. The primary duty of the police, as stipulated in Article 13 letter C of the Police Law Number 2 of 2002, is to protect, serve, and serve against various social ills.

In addressing online fraud, the police have implemented various measures. Based on an interview with Brigadier I Wayan Bayu Semadi, S.H., M.H., Ba, Unit 4, Sub-Directorate 1, Directorate of Special Criminal Investigation, Bali Regional Police, he stated that the police have implemented both preventative and repressive law enforcement efforts. The explanation is as follows: 1. Law Enforcement Through Preventive Efforts. The first step taken by the Bali Regional Police in enforcing the law against perpetrators of online fraud is preventive action. The Bali Regional Police carry out systematic, planned, and targeted prevention efforts to address the possibility of online fraud. Preventive efforts are carried out through: a. Appealing to the public through social media; The initial step taken by the Bali Regional Police as an effort to prevent online fraud is to issue warnings, appeals and prohibitions against online fraud accompanied by threats of sanctions conveyed on various social media. b. Carrying out outreach to the Community; The Bali Regional Police carry out outreach and counseling on preventing online arisan fraud to the community within the jurisdiction of the Bali region. The Bali Regional Police are intensively carrying out fraud prevention efforts through counseling, thus providing information to the community who lack legal awareness, and the general public who are unaware of the methods used by online fraud perpetrators. These efforts are expected to run effectively, providing an understanding to the community to be more vigilant because everyone has the potential to be a target of crime. Therefore, the police need to explain to the public to be more careful in acting because crime is increasing. 2. Law Enforcement Through Enforcement Efforts (Repressive). Repressive efforts are a conceptual crime prevention effort taken after a crime has occurred. Repressive measures are intended to punish the perpetrators of crimes according to their actions and to correct them so that they realize that their actions are unlawful and detrimental to society, so that they will not repeat them and others will not do it either considering the sanctions they will bear are very heavy. Responsibility for online arisan fraud is regulated in Article 28 paragraph (1) Jo. Article 45A paragraph (1) of Law Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Electronic Information and Transactions and Article 378 of the Criminal Code (Article 492 of the New Criminal Code) which regulates the crime of fraud. These repressive measures can take place

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

with 2 possibilities, namely the case continues to court or dispute resolution through restorative justice (peace) with certain conditions.

In an interview with AKP Budi Santoso, S.H., Head of Unit 2, Sub-Directorate 4, Directorate of Special Criminal Investigation of the Bali Regional Police, he explained that criminal law enforcement against online fraudsters through repressive measures is carried out in several stages, starting with the investigation stage, the inquiry stage, the examination stage, and finally, the settlement and submission of the case to the Public Prosecutor. The following is the law enforcement process for online fraud perpetrators at the Bali Regional Police Criminal Investigation Unit: 1. Investigation Stage; 2. Investigation Stage; 3. Examination Stage; 4. Settlement Stage and Submission of the Case to the Public Prosecutor (JPU).

Regarding the resolution of online fraud cases occurring at the Bali Regional Police after the investigation process, due to a settlement between the reporter and the accused, the handling is carried out using restorative justice. This is in accordance with Police Regulation No. 8 of 2021 concerning the Handling of Criminal Acts Based on Restorative Justice, which must meet formal and material requirements. According to Article 5 of Police Regulation No. The material requirements for compliance with Law No. 8 of 2021 are: a) not causing unrest and/or rejection from the community; b) not impacting social conflict; c) not having the potential to divide the nation; d) not being radical or separatist; e) not being a repeat offender based on a court decision; and f) not committing a crime of terrorism, a crime against state security, a crime of corruption, or a crime against human life. According to Article 6, the formal requirements are: a. peace between both parties; and b. fulfillment of the victim's rights and the perpetrator's responsibility. According to AKP Budi Santoso, S.H., Head of Unit 2, Sub-Directorate 4, Directorate of Special Criminal Investigation of the Bali Regional Police, the restorative justice approach to handling online fraud cases is in accordance with the wishes of each party, and the parties have entered into a peace agreement.

In online fraud cases, victims often demand material compensation from the perpetrator to obtain the return of their rights due to the losses suffered by the victim and the perpetrator's accountability. However, this has not been fully realized because there is no legal regulation regarding compensation for victims of online fraud. Compensation for victims of online transaction fraud is crucial for achieving victims' rights, a form of justice. The Electronic Information and Transactions (ITE) Law only contains one main criminal article and criminal penalties for perpetrators, but it does not yet explain how victims are protected, or what protection they can receive after the case is resolved, with both material and immaterial losses suffered.

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

Compensation for injured victims is a legal protection, providing certainty not only through legal protection but also through the subsequent fulfillment of their rights. Compensation itself is only available in civil cases. If a victim feels the need for compensation, they can file a lawsuit through civil channels. However, this appears to be highly detrimental to the victim, as it demonstrates that the victim has already suffered material losses and filed a criminal complaint for fraud. Furthermore, if the victim is burdened with a claim for compensation, it can result in multiple losses, resulting in significant harm from the victim's perspective.

Based on the results of an interview with AKP Budi Santoso, S.H., Head of Unit 2 Sub-Directorate 4 of the Bali Regional Police's Special Criminal Investigation Directorate, the recovery of losses due to online fraud in the Bali Regional Police (Polda) is handled by the Cyber Investigation Directorate (Ditres Siber). Money cannot be returned automatically by the police, but through legal processes, blocking bank accounts, or settlement of compensation through restorative justice mediation. Furthermore, according to Brigadier I Wayan Bayu Semadi, S.H., M.H. Ba, Unit 4 Sub-Directorate 1 of the Bali Regional Police's Special Criminal Investigation Directorate, the steps that need to be taken to process the reporting and recovery of losses are: 1. Perform Initial Blocking. Immediately contact the bank to report the fraudulent transaction and request blocking of the destination account. You can also check or report the perpetrator's account number through the CekRekening.id portal owned by the Ministry of Communication and Digital. 2. Report to the Bali Regional Police Report the incident to the Bali Regional Police's Cyber Directorate so that the case can be followed up criminally. Bali Cyber Report Service: Complainants can make an initial online complaint through the official Bali Cyber Report portal. In Person: Complainants can also visit the Bali Police's SPKT or the Bali Police Cyber Directorate office in Denpasar with strong evidence (such as screenshots of conversations, proof of transfers, and the perpetrator's account number). Legal Process and Refund. After the report is processed and the perpetrator is caught, the compensation mechanism can be pursued in two ways: a. Restorative Justice (Mediation): If the perpetrator is caught, investigators can facilitate mediation so that the perpetrator is willing to return or compensate your losses outside of court (based on a peace agreement). b. Court Decision (Restitution/Confiscation): If the case proceeds to court, investigators will confiscate the perpetrator's assets or remaining funds. The panel of judges will decide whether the remaining funds are returned to the victim as evidence or compensation.

Obstacles in Law Enforcement Against Online Fraud Crimes in the Bali Regional Police Jurisdiction

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

The perpetrators' use of social media as a target for their actions is not without reason. The law still lacks adequate coverage and leaves no evidence behind. When linked to criminology, the extent of the fraudulent activity is examined and all aspects and causes of the crime are understood. Several factors contribute to someone committing fraudulent transactions using social media, in particular: 1. Cultural factors; 2. Motivating factors; and 3. Economic factors.

The ITE Law regulates every crime that falls under the category of cybercrime. In its application, the ITE Law not only regulates legal acts occurring in Indonesia and/or committed by Indonesian citizens, but also applies to legal acts committed outside of Indonesia's jurisdiction, whether by Indonesian citizens or foreign citizens, or Indonesian or foreign legal entities that have legal consequences in Indonesia, considering that the use of Information Technology for Electronic Information and Electronic Transactions can be cross-territorial or universal. This is stipulated in Article 2 of the ITE Law, which states: "This law applies to any person who commits a legal act as stipulated in this law, whether within or outside Indonesian jurisdiction, which has legal consequences within Indonesian jurisdiction and/or outside Indonesian jurisdiction and is detrimental to Indonesia's interests."

The Bali Regional Police's efforts to enforce the law against perpetrators of online fraud have encountered several obstacles. The weak mentality of law enforcement officers has resulted in law enforcement not running as expected. Many factors contribute to this weak mentality, including a weak understanding of religion, economics, a non-transparent recruitment process, and so on. Therefore, it can be emphasized that law enforcement plays a crucial role in the functioning of the law. If regulations are good but the quality of law enforcement is low, problems will arise. Likewise, if regulations are poor but the quality of law enforcement is good, problems are still possible. Law enforcement by the police is also considered very inadequate, as evidenced by the numerous motor vehicle tickets issued that end in bribes (UUD-Ujungnya Duit). In addition to these problems, weak laws also weaken national resilience. This can be seen in various cases concerning national borders and the annexation of territory and culture by neighboring countries. These obstacles, when broken down, can be seen as follows:

1. Internal constraints

a. Human Resources

Police investigators play a crucial role in law enforcement against online fraud perpetrators, and their expertise is crucial to uncovering these cases. Specialized investigators with expertise in information and electronic transactions are needed to address cybercrime. The

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

limited number of experts within the police force is a significant factor. This limited number of experts hinders the timely completion and investigation of online fraud cases, leaving perpetrators with greater freedom to commit fraud. Investigators' lack of technical knowledge and experience in handling online fraud cases, along with the complexities of the evidence system, also complicates the process.

b. Evidence Aspects

Evidence in online fraud cases differs from evidence in other crimes, where the target or medium of cybercrime is data or computer systems or the internet, which are easily deleted, altered, or hidden by the perpetrator. Furthermore, victim witnesses play a crucial role in online fraud cases, as witnesses are rare in online arisan fraud cases because they are located outside the region or even abroad, making it difficult for investigators to examine witnesses and file investigations.

c. Facility Aspects

Online fraud is said to be difficult to apprehend. This is because perpetrators can easily erase digital traces and easily sever ties with their victims. Therefore, in the process of searching for perpetrators, the police need adequate technology to apprehend them. Solving cybercrime cases, including online arisan fraud, requires facilities capable of supporting police performance. These facilities include computer forensics laboratories used to uncover digital data and record and store evidence in the form of images, programs, HTML, audio, and other files.

2. External Constraints

a. Lack of Public Legal Awareness

Public legal awareness regarding the function and response to cybercrime, including online fraud, is still considered lacking. This is due to a lack of public understanding and knowledge of the types of online fraud. This lack of knowledge has hampered online fraud law enforcement efforts related to legal regulation and public oversight of any activity suspected of being related to online fraud. .

b. Lack of Public Response to Socialization or Counseling Carried Out by the Police

The obstacle faced by the police in conducting outreach or education about online fraud is the lack of public response to the police. This demonstrates the public's limited knowledge of online fraud laws and regulations, as they still believe there are no binding regulations governing technology and that violations will result in sanctions.

c. Lack of Public Reports

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

The lack of public reporting of online fraud means that when crimes occur in the community, people seem to ignore them. This contributes to the lack of police reports of online fraud.

CONCLUSION

Law enforcement regarding criminal acts of online fraud in recovering victims' money in the Bali Regional Police's jurisdiction. Recovering losses due to online fraud in the Bali Regional Police (Polda) is handled by the Cyber Investigation Directorate (Ditres Cyber). The money cannot be returned automatically by the police, but rather through legal processes, blocking bank accounts, or resolving compensation through restorative justice mediation. Steps that need to be taken to process loss reporting and refunds: 1. Perform Initial Blocking. 2. Report it to the Bali Police. Report the incident to the Bali Police Cyber Directorate so that the case can be followed up criminally. In enforcing the law, internal and external obstacles were found.

REFERENCES

Arif Gosita, 2003, Masalah Korban Kejahatan, Akademika Pressindo, Jakarta.

Budi Suhariyanto, 2012, Tindak Pidana Teknologi Informasi (cybercrime), RajaGrafindo Persada, Jakarta.

I Gusti Made Jaya Kesuma, Ida Ayu Putu Widiati, I Nyoman Gede Sugiartha, 2020, Penegakan Hukum Terhadap Penipuan Melalui Media Elektronik, Jurnal Preferensi Hukum, Fakultas Hukum Universitas Warmadewa, Denpasar-Bali, Indonesia, Vol 1, No. 2.

Johnny Ibrahim, 2007, Teori dan Metodelogi Penelitian Hukum Normatif, Citra Aditya Bakti, Bandung.

Mastur, 2016, "Implementasi Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagai Tindak Pidana Non Konvensional", Vol. 16 No. 2, Juni.

P.A.F. Lamintang, 2007, Dasar-dasar Hukum Pidana Indonesia, Citra Aditya Bhakti, Bandung, hal 185.

Tongat, 2012, Dasar-dasar Hukum Pidana Indonesia Dalam Perspektif Pembaharuan, UMM Pres, Malang.

Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

Kitab Undang-Undang Hukum Pidana

Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Lembaran Negara

E-ISSN: 3032-0135
Vol. 4, No.1, July - December (2026), pp. 124-134

Republik Indonesia Tahun 2016 Nomor 251, Tambahan Lembaran Negara Republik Indonesia Nomor 5952.