Eduvest – Journal of Universal Studies
Volume 6 Number 6, June, 2026
p- ISSN 2775-3735- e-ISSN 2775-3727

Law Enforcement Actions Against Investment Fraud Committed Via WhatsApp (WA) at the Cirebon City Police Department

Ilham*, Sanusi, Siska Karina
Universitas Swadaya Gunung Jati, Indonesia
Email: azailham57@gmail.com*, sanusi@ugj.ac.id, okekarina763@gmail.com

Keywords
law enforcement, investment fraud, cyber crime, cirebon city

Abstract
This study discusses law enforcement actions against investment fraud committed via WhatsApp (WA) at the Cirebon City Police Department. This study employed a normative juridical approach with a qualitative descriptive method, namely by analyzing applicable laws and regulations, supported by data from interviews and field studies. The results of the study indicate that the perpetrators committed fraud by offering investments through a fundraising system, promising quick profits, using false identities, and employing persuasive communication to convince victims. Law enforcement against this crime was carried out in accordance with procedures through the investigation and inquiry stages based on Article 492 of the Criminal Code and the Information and Electronic Transactions Law. However, in practice, several obstacles remained, such as difficulties in tracking the perpetrators, the use of third-party accounts, and limited access to digital data. This study recommends increasing the capacity of law enforcement officers, updating regulations, and combining preventive and repressive approaches in the community as important steps to improve the effectiveness of law enforcement in the digital era.

INTRODUCTION

Law enforcement is one of the crucial components in realizing an orderly and just society. Law enforcement aims not only to punish those who commit crimes but also to protect society and prevent crime from occurring. In reality, the success of law enforcement is influenced by several variables, including legal substance, the capacity of law enforcement officials, available facilities, and public legal awareness. Unfortunately, law enforcement performance does not always keep pace with the development of crime, resulting in an increase in criminal acts. Fraud is one of the most common crimes in society (Adorjan & Colaguori, 2023). Legally, fraud is defined as an unlawful act committed through deception or false statements to persuade another person to hand over something . Fraud has evolved over time and is now frequently committed by exploiting advances in information technology, thereby causing harm to victims (Button & Cross, 2017).

In the digital era, the development of information technology has brought significant changes to various aspects of human life, particularly communication and economic transactions (Feather, 2017; Lee et al., 2018; Xia et al., 2024). However, these advancements have also created opportunities for the emergence of cybercrime. Cybercrime is an unlawful act that exploits computer networks and the internet. Due to its wide reach and the ease with which perpetrators can access technology, this type of crime has become increasingly complex. This shows that technological advancement has two sides: it facilitates human activities while also increasing the likelihood of criminal acts.

Fraud through electronic media, including instant messaging applications such as WhatsApp, is one of the growing forms of cybercrime (Ezeji, 2024; McGuire, 2019). This type of fraud exploits victims' trust and the lack of a reliable digital identity verification system. This condition increases the challenges faced by law enforcement officials in handling online fraud cases, particularly because such cases are affected by various obstacles, such as the quality of law enforcement personnel, limited facilities, and low public legal awareness (Curtis & Oxburgh, 2023; Qu & Cheng, 2024). Investment fraud is also one type of fraud that is currently widespread. Investment scams usually have no clear legal basis and offer large profits within a short period (Ali et al., 2024; Bawornchai et al., 2025). Perpetrators commonly use various electronic platforms to attract victims' attention. Technological advances are often misused by irresponsible parties to commit investment fraud and victimize members of the public (Anderson et al., 2024; Ebenezer et al., 2016).

Investment scams carried out through WhatsApp are usually committed by spreading false information about transactions that promise substantial profits (Youvan, 2024). Perpetrators often use fake testimonials, manipulative tactics, and promises of high returns with minimal risk within a short period. This clearly contradicts the basic principles of investment, which always require caution and involve risk. The public's limited understanding of legal and financial matters makes people easily tempted and less likely to verify investment offers. This indicates that public legal literacy is crucial in addressing the increasing number of digital-based fraud cases.

Technology-based investment fraud has also occurred within the jurisdiction of the Cirebon City Police Department. As the number of individuals using social media and instant messaging applications continues to increase, technology-based crimes have become increasingly difficult to avoid. These crimes cause significant financial losses to victims and reduce public trust in law enforcement systems and electronic transactions. As a result, the role of law enforcement officials, particularly the police, is essential in providing legal protection to the community. Law enforcement against investment fraud committed through WhatsApp inevitably faces many challenges. The police must comply with the provisions stipulated in Law No. 1 of 2024 concerning Electronic Information and Transactions, the second amendment to Law No. 11 of 2008, in addition to proving the elements of fraud as regulated under Article 492 of the Criminal Code (KUHP). The main obstacles in the investigation include proving electronic evidence, identifying perpetrators who often use false identities, and addressing the lack of adequate tools and technical capabilities.

METHOD

This study employed a qualitative method with a normative juridical approach to examine law enforcement against perpetrators of fraud committed through WhatsApp group chats. The study focused on the application of written legal norms, legal principles, and relevant legal doctrines in handling fraud cases involving digital communication media. This approach was selected because the research problem was related to the application of criminal law, particularly Article 492 of the Criminal Code and the provisions of the Electronic Information and Transactions Law (UU ITE).

RESULTS AND DISCUSSION

Modus operandi of the Perpetrators of Investment Fraud

Based on the results of an interview with Abdur Rochim at the Cirebon City Police, it is known that the modus operandi of the perpetrator of investment fraud through WhatsApp takes advantage of the ease of digital communication and the trust of the victim. The perpetrator usually starts by contacting the victim directly via private message or putting them into a specific investment group. In the early stages, the perpetrator creates trust by using a false identity, profiteering from the name of an investment company, or pretending to be a person known to the victim. The perpetrator then offers investments with a custodial system that promises large profits in a short period of time, usually only one to seven days. Perpetrators often show testimonials, screenshots, and evidence of transfers to convince victims. The perpetrator will ask the victim to send a certain amount of money to the nominee's account—an account usually owned by someone else—if they are interested. Then, after the victim made the transfer, the perpetrator provided a fake profit report to encourage them to increase funds. The perpetrator then begins to evade for various reasons, such as problems with the system, additional administrative costs, or withheld funds. In the end, the perpetrator will stop talking and leave, causing the victim to lose money.

Based on these findings, the results show that this crime is evolving with technology and utilizing the psychology of the victim. In this case, there is clearly a process of social manipulation planned. In addition to providing false information, perpetrators create trust through intense communication, the use of false identities, and showing evidence of fabricated profits. The use of digital technology also makes law enforcement more difficult because perpetrators can hide their identities and change locations easily.

Law Enforcement Efforts Against Investment Fraud Crimes via *WhatsApp* (WA) at the Cirebon City Police Station

The Cirebon City Police have taken appropriate legal action for investment fraud cases through WhatsApp. This process begins by requesting reports from the community at SPKT. Officers will immediately conduct initial clarification and collect evidence such as digital conversations, proof of transfer, and the identity of the perpetrator after the report is received. Then the case was handed over to the Criminal Investigation Unit to be examined to find the crime scene and identify the perpetrator. The case will proceed to the investigation stage if there is sufficient preliminary evidence. At this point, investigators examined witnesses and victims, seized evidence, and worked with banks to trace the source of the funds.

The Cirebon City Police used the provisions of Article 492 of the Criminal Code regarding fraud that has been updated and the provisions of the ITE Law to handle this case. If there is a hidden source of funds from criminal acts, they may also apply money laundering rules in some cases.

Analyzed according to the theory of law enforcement by Soerjono Soekanto, law enforcement against investment fraud cases through WhatsApp at the Cirebon City Police is influenced by five main factors. The substance of the law, law enforcement officials, facilities and infrastructure, society, and legal culture are these factors. In terms of legal substance, laws such as Article 492 of the Criminal Code and the ITE Law are sufficient to arrest perpetrators, but they do not fully meet the demands of the increasingly complex development of cybercrime. Although regulations have been complied with, law enforcement officials need

better skills, especially in digital forensics, to combat this type of technology-based crime. In addition, the law enforcement process is also hampered by limited facilities and infrastructure, especially in terms of access to digital data and technology that supports investigations. From a society's perspective, a poor understanding of digital technology and a tendency to be tempted by quick profits increase the likelihood of criminal acts (Helbing, 2018; Wall, 2024). In addition, slow reporting hinders investigations. However, from the perspective of legal culture, the lack of public awareness on how to transact safely and report crime shows that the function of the law as a tool of social control has not been functioning properly. According to this theory, law enforcement in this case has not been fully effective because there is no balance between the variables that affect it.

In addition, in the context of comparative criminal law, Sanusi stated that cybercrimes such as investment fraud through WhatsApp are a global phenomenon that requires the national legal system to adapt to these changes (Lazarus, 2026; Maksum, 2024). This shows that law enforcement does not only need to be done domestically, but also requires international collaboration and harmonization of regulations (Hufnagel, 2017, 2021).

Therefore, normative and qualitative juridical analysis in this study shows that there is already a strong legal basis for implementing laws prohibiting investment fraud through WhatsApp at the Cirebon City Police, but the implementation of the law still needs to be strengthened. To improve law enforcement performance in the computer and internet age, important steps include increasing the capacity of the apparatus, revising regulations, and applying preventive and repressive methods to the public.

CONCLUSION

The modus operandi of investment fraud perpetrators through WhatsApp operates systematically by exploiting victims' trust and digital technology. These techniques include using fake identities, soliciting investments through a custodial system, and promising quick profits supported by persuasive communication and false evidence.

Law enforcement actions against investment fraud committed through WhatsApp have been carried out by the Cirebon City Police with reference to Article 492 of the Criminal Code and the ITE Law. However, several problems remain in its implementation, including difficulties in identifying the actual perpetrators, the use of other people's accounts, limited access to digital data, and low public awareness of reporting crimes. This situation shows that increasing law enforcement officers' capacity, updating regulations, and integrating preventive and repressive approaches in the community are important steps toward optimizing law enforcement performance in the digital era.

REFERENCES

Adorjan, M., & Colaguori, C. (2023). Scams, fraud, and cybercrime in a globalized society. *Crime, Deviance, and Social Control in the 21st Century: A Justice and Rights Perspective*, *407*, 407–437.

Ali, E. M., Dirgantara, F., & Darmawan, D. (2024). Legal Protection of Consumers in Online Transactions: A Case Study of Online Fraud in Indonesia. *International Journal of Service Science, Management, Engineering, and Technology*, *6*(3), 27–38.

Anderson, M., March, E., Land, L., & Boshuijzen-van Burken, C. (2024). Exploring the roles played by trust and technology in the online investment fraud victimisation process.

Journal of Criminology, *57*(4), 488–514.
Bawornchai, D., Aonnom, I., Kitchombhu, S., Cheuaprakhobkit, S., Kanthasi, M., Netthip, W., Mektraitrat, T., & Nhomchopphitak, P. (2025). Developing Guidelines for the Prevention and Suppression of Online Fraud Crimes: Guidelines for Law Enforcement by Police Officials in the Investigation. *Nimitmai Review Journal*, *8*(2), 1–17.
Button, M., & Cross, C. (2017). Technology and Fraud: The 'Fraudogenic'consequences of the Internet revolution. In *The Routledge handbook of technology, crime and justice* (pp. 78–95). Routledge.
Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world'policing and law enforcement. *The Police Journal*, *96*(4), 573–592.
Ebenezer, A. J., Paula, A. M., & Allo, T. (2016). Risk and investment decision making in the technological age: A dialysis of cyber fraud complication in Nigeria. *International Journal of Cyber Criminology*, *10*(1), 62.
Ezeji, C. L. (2024). Emerging technologies and cyber-crime: strategies for mitigating cyber-crime and misinformation on social media and cyber systems. *International Journal of Business Ecosystem & Strategy (2687-2293)*, *6*(4), 271–284.
Feather, J. (2017). *The information society: A study of continuity and change*.
Helbing, D. (2018). Societal, economic, ethical and legal challenges of the digital revolution: from big data to deep learning, artificial intelligence, and manipulative technologies. In *Towards digital enlightenment: Essays on the dark and light sides of the digital revolution* (pp. 47–72). Springer.
Hufnagel, S. (2017). Regulation of cross-border law enforcement:'locks' and 'dams' to regional and international flows of policing. *Global Crime*, *18*(3), 218–236.
Hufnagel, S. (2021). *Policing global regions: The legal context of transnational law enforcement cooperation*. Routledge.
Lazarus, S. (2026). 'Funds Left Delaware in the Morning': Online Fraud Networks and Money Laundering Operations. *International Criminal Justice Review*, 10575677261416902.
Lee, M., Yun, J. J., Pyka, A., Won, D., Kodama, F., Schiuma, G., Park, H., Jeon, J., Park, K., & Jung, K. (2018). How to respond to the fourth industrial revolution, or the second information technology revolution? Dynamic new combinations between technology, market, and society through open innovation. *Journal of Open Innovation: Technology, Market, and Complexity*, *4*(3), 21.
Maksum, M. J. S. (2024). Legal Implications of Civil and Criminal Law on Investment Fraud Under the Guise of Online Business. *Indonesian Economic Review*, *4*(1), 29–42.
McGuire, M. (2019). Social media platforms and the cybercrime economy. *Bromium. Preuzeto*, *21*, 2023.
Qu, J., & Cheng, H. (2024). Policing telecommunication and cyber fraud: Perceptions and experiences of law enforcement officers in China. *Crime, Law and Social Change*, *82*(2), 283–305.
Wall, D. S. (2024). *Cybercrime: The Transformation Of Crime In The Information Age (2nd Ed.)*. https://doi.org/10.13140/Rg.2.2.28017.45928
Xia, L., Baghaie, S., & Sajadi, S. M. (2024). The digital economy: Challenges and opportunities in the new era of technology and electronic communications. *Ain Shams Engineering Journal*, *15*(2), 102411.
Youvan, D. C. (2024). *The Art of Deception: How Scammers Use WhatsApp to Exploit Trust Through Intelligent Engagement*.