GIJLSS
Greenation International Journal of Law and Social Sciences
+62 81210467572 https://research.e-greenation.org/GIJLSS greenation.info@gmail.com
GREENATION RESEARCH

DOI: https://doi.org/10.38035/gijlss.v4i4

Criminal Liability for Technology-Based Digital Investment Fraud in Indonesia: Challenges of Evidence, Mens Rea, and Corporate Accountability

Pudjianto Gondosasmito
Universitas Prima Indonesia, Medan, Indonesia, gondosasmito@yahoo.com

Corresponding Author: gondosasmito@yahoo.com

Abstract: The rapid advancement of digital technology has transformed investment activities through technology-based platforms, providing easier public access while creating opportunities for digital investment crimes. These crimes commonly involve fraudulent investment schemes, fictitious digital platforms, and technological manipulation aimed at deceiving victims. This study examines digital investment crime from the perspective of criminal law, focusing on the development of digital investment practices, technology-based fraud schemes, and criminal liability for both individual and corporate offenders. The research applies a normative legal method using statutory, conceptual, and case approaches, supported by primary, secondary, and tertiary legal materials, analyzed descriptively and qualitatively. The findings reveal that digital investment crimes are complex, transnational, and difficult to detect because perpetrators exploit technological sophistication to conceal identities and activities, thereby complicating evidentiary processes. As a novelty, this article proposes an integrated criminal liability framework that combines the Indonesian Criminal Code, the Electronic Information and Transactions Law, the Anti-Money Laundering Law, OJK regulations, and the principle of mens rea to assess criminal responsibility in digital investment fraud. The study concludes that combating digital investment crime requires adaptive legal frameworks, stronger law enforcement, and enhanced public literacy.

Keywords: Digital Investment Crime, Criminal Law, Technology-Based Fraud, Criminal Liability, Cybercrime.

INTRODUCTION

The rapid advancement of digital technology over the past few decades has significantly transformed various aspects of social life, particularly within the fields of economics and investment. Digital transformation has stimulated the emergence of technology-based investment instruments such as financial technology (*fintech*), crypto assets, and online trading platforms.(Ms. Janvi Sanjay Gotad, 2026) These technological developments have provided greater convenience for the public in conducting investment activities through faster access, more efficient transaction processes, and increased flexibility to invest anytime and anywhere. Investments that were previously accessible only to certain groups have now become more open to the wider public. This condition demonstrates that digital technology has made a substantial contribution to the development of the modern investment sector.(Anfas et al., 2022)

Despite these advantages, the advancement of digital technology has also generated negative consequences in the form of an increased potential for investment-related crimes. Technology, which should ideally support economic growth and enhance public welfare, is frequently misused by certain parties to obtain unlawful profits.(Nurmala et al., 2025) The emergence of various forms of digital investment crime illustrates that technological development not only creates new opportunities but also opens avenues for increasingly complex, dynamic, and difficult-to-detect criminal activities. This phenomenon indicates that the evolution of digital technology has progressed simultaneously with the evolution of criminal methods that exploit technology as the primary instrument for carrying out illicit activities.(Halawi & Bacon, 2024)

The growing public interest in digital investment is not always accompanied by adequate understanding of investment mechanisms, risks, and legality. Many individuals are attracted to investment opportunities because of promises of substantial profits within a short period of time, without fully comprehending the potential risks involved. Low levels of financial literacy and digital literacy have become major factors exploited by perpetrators in conducting various forms of investment fraud. Such conditions have given rise to increasingly diverse fraudulent schemes, including fraudulent investment operations, illegal trading robots, and the emergence of fake platforms and applications that imitate legitimate investment services. These schemes are deliberately designed to appear professional and convincing, resulting in many individuals becoming victims and suffering substantial financial losses.(Papasavva et al., 2025)

The phenomenon of digital investment crime can no longer be regarded as a simple legal issue. In recent years, technology-based investment fraud cases have continued to increase and generated extensive social consequences. The losses suffered by victims are not merely material in nature but also contribute to declining public trust in investment systems in general. In the long term, such conditions may hinder the development of a healthy investment climate and reduce public participation in legitimate and productive investment activities.(Irfan Ridha et al., 2024) Consequently, the growth of digital investment requires stricter supervision to ensure that technological advancement does not become a means of facilitating criminal conduct.

From the perspective of criminal law, the development of digital investment crime gives rise to various complex legal issues. Existing criminal law concepts have largely been developed within the framework of conventional crimes and, therefore, are not yet fully capable of addressing the characteristics of digital crimes, which are transnational, organized, and highly dependent on sophisticated technology.(AllahRakha, 2025) Furthermore, legal regulations concerning illegal digital investment activities remain insufficiently comprehensive, creating difficulties in law enforcement practices regarding the appropriate legal basis for prosecuting offenders. Evidentiary processes in digital crime cases also present significant challenges because perpetrators frequently employ false identities, complex digital systems, and networks that are difficult to trace. As a result, law enforcement processes do not always operate effectively or optimally.(Y. Zhou et al., 2024)

Within the context of criminal law, criminal liability constitutes one of the fundamental doctrines in determining whether an offender may be held accountable for unlawful conduct. Criminal liability is not solely concerned with the existence of an unlawful act but also requires consideration of the element of fault attributable to the perpetrator. The doctrine of criminal liability recognizes two principal elements, namely *actus reus* and *mens rea*. *Actus reus* refers to the physical act committed by the offender, whereas *mens rea* concerns the mental state or intention accompanying the commission of the act. Both elements serve as essential foundations in determining the existence of criminal liability.(Ormerod et al., 2024) This principle is closely related to the doctrine of *nulla poena sine culpa*, meaning that there can be no punishment without fault. In cases of digital investment crime, proving the element of fault becomes increasingly important because perpetrators often exploit technology to conceal both their identities and their unlawful activities.

The development of digital investment crime further demonstrates that criminal acts are not always committed solely by individuals but may also involve corporations or legal entities that benefit from such unlawful practices. Accordingly, criminal liability in digital investment crimes should not only be imposed upon individual offenders but may also extend to corporations involved in the commission of such offenses. This condition reflects the necessity for criminal law to adapt to technological developments and modern patterns of crime to remain effective in providing legal protection for society.(Simpson, 2002)

Although previous studies have widely examined illegal digital investment from the perspectives of consumer protection, financial technology regulation, and cybercrime prevention, several important gaps remain. Existing scholarship largely emphasizes regulatory compliance, licensing issues, and investor protection mechanisms, while insufficient attention has been paid to the criminal law dimensions of technology-based investment fraud. In particular, prior studies have not adequately explained how digital fraud schemes involving algorithmic trading manipulation, fictitious investment platforms, and crypto-based deception can satisfy the evidentiary requirements of actus reus and mens rea. Moreover, limited studies have critically examined the extension of criminal liability to corporations or legal entities that facilitate or benefit from such fraudulent schemes. This gap indicates the need for a more integrated criminal law analysis that connects digital modus operandi with evidentiary challenges, fault attribution, and corporate criminal accountability.

Accordingly, this study addresses three principal research questions. First, how do technology-based digital investment fraud schemes operate and evolve within the Indonesian digital investment ecosystem? Second, how should the elements of actus reus and mens rea be constructed and proven in digital investment fraud involving electronic systems and technology-assisted deception? Third, to what extent can Indonesian criminal law impose criminal liability upon both individual offenders and corporations involved in digital investment fraud?

Based on the foregoing discussion, this study aims not only to analyze the development of digital investment and the evolution of technology-based fraud schemes, but also to develop an integrated criminal liability analysis linking digital modus operandi with the evidentiary construction of actus reus, proof of mens rea, and corporate criminal accountability under Indonesian criminal law. Through this approach, the study seeks to provide a more comprehensive framework for assessing criminal responsibility in digital investment fraud cases.(Kayser et al., 2025)

METHOD

This study employs a normative legal research method, which focuses on the examination of legal norms embodied in statutory regulations, legal doctrines, and legal theories. The research is conducted to analyze digital investment crime from the perspective of criminal law, particularly concerning technology-based fraud schemes and the criminal liability of perpetrators. The approaches adopted in this study include the statutory approach, conceptual approach, and case approach. The statutory approach is applied through the examination of relevant legal instruments, including the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana* / KUHP), the Electronic Information and Transactions Law (*Undang-Undang Informasi dan Transaksi Elektronik* / ITE Law), as well as regulations issued by the Indonesian Financial Services Authority (*Otoritas Jasa Keuangan* / OJK). The conceptual approach is utilized to analyze legal concepts related to criminal liability, fraud, and cybercrime, The case approach is applied through the analysis of selected Indonesian digital investment fraud cases, including illegal trading robot schemes, fictitious investment platforms, and crypto-related fraud. These cases are examined to assess how criminal liability is established in practice, particularly regarding evidentiary challenges, the proof of actus reus and mens rea, and the attribution of liability to corporate entities.

The cases analyzed in this study were selected based on four criteria: (1) cases involving significant financial losses to victims, (2) cases in which digital technology served as the primary instrument of fraudulent conduct, (3) cases presenting substantial challenges in proving evidentiary elements and criminal intent, and (4) cases indicating the involvement of corporate entities or organized structures in facilitating the fraud.

The legal materials employed in this research consist of primary, secondary, and tertiary legal sources. Primary legal materials include statutory regulations, court decisions, and official regulatory documents relevant to digital investment fraud. Secondary legal materials consist of academic journals, legal textbooks, scholarly commentaries, and previous research findings related to criminal law, cybercrime, and financial fraud. Tertiary legal materials include legal dictionaries, encyclopedias, and other supporting reference materials.

The collection of legal materials was conducted through library research using document review and systematic literature analysis. Legal materials were identified, classified, and organized according to their relevance to the research issues. All collected materials were analyzed using descriptive qualitative analysis to interpret legal norms, compare case patterns, and formulate a comprehensive criminal liability framework concerning technology-based digital investment fraud.

RESULTS AND DISCUSSION

The Development of Digital Investment and Its Relevance to the Potential for Crime in the Sector

The advancement of digital technology has brought significant transformation to the investment sector. Investment activities that were previously conducted through conventional mechanisms have now shifted toward digital-based systems utilizing applications, websites, and other electronic platforms.('Study on the Role of Technology in Empowering Individual Investors to Make Investment Decisions', 2025) The emergence of digital investment has provided various advantages, including faster access, greater flexibility, and higher efficiency, enabling individuals to conduct investment transactions anytime and anywhere without the need to physically visit financial institutions. Contemporary forms of digital investment include stock trading through online securities applications, *peer-to-peer lending* (*P2P lending*), crypto assets such as Bitcoin and Ethereum, digital mutual funds, and crowdfunding platforms. These investment instruments offer more practical investment processes with relatively affordable initial capital requirements.(Wales, 2015)

Digital investment in Indonesia has grown substantially over the past several years. This development has been influenced by expanding internet accessibility, the widespread use of smartphones, and the rapid growth of financial technology (*fintech*) services. In addition, the COVID-19 pandemic accelerated the transition of public transaction patterns toward digital systems, including in the investment sector. Such conditions have contributed to the increasing number of retail investors shifting from conventional investment mechanisms to technology-based investment platforms.(Lukiyanto et al., 2024) Data from the Indonesian Central Securities Depository (*Kustodian Sentral Efek Indonesia* / KSEI) indicate a highly significant increase in the number of capital market investors in recent years, as illustrated in the following table:

Table 1. Data on the Growth of Indonesian Capital Market Investors

Year	Number of Capital Market Investors
2019	2.48 million investors
2020	3.88 million investors
2021	7.49 million investors
2022	10.31 million investors
2023	12.16 million investors
2024	More than 13 million investors

Source: KSEI and the Indonesian Financial Services Authority (*Otoritas Jasa Keuangan* / OJK).

The increase in the number of investors demonstrates that digital transformation has enabled the public to gain easier access to investment instruments through online platforms. Younger generations constitute the most dominant group in the growth of new investors due to their greater familiarity with digital technology. Although digital investment has experienced rapid growth, the level of financial literacy among the Indonesian population remains uneven. The National Survey on Financial Literacy and Inclusion conducted by OJK reveals a disparity between the levels of financial inclusion and financial literacy within society.

Source: OJK National Survey on Financial Literacy and Inclusion 2024.

Figure 1. Data on Financial Literacy and Financial Inclusion

These data indicate that while many individuals have utilized digital financial services, not all of them adequately understand investment mechanisms and associated risks. This condition constitutes one of the primary factors contributing to the vulnerability of the public to digital investment fraud. Nevertheless, the rapid expansion of digital investment has also generated various legal issues and new forms of criminal activity. Certain parties frequently exploit the accessibility provided by digital platforms to conduct investment fraud through illegal platforms, fake applications, and investment offers promising unrealistic returns.(Moh. Ja'far Sodiq Maksum, 2024) Limited financial and digital literacy among the public is a major factor that causes many investors to become trapped in illegal investment schemes. Many individuals are enticed by promises of substantial profits without first verifying the legality of the platforms they use.

The Task Force for the Eradication of Illegal Financial Activities (*Satgas PASTI*) recorded that public financial losses resulting from illegal investment activities and digital-based fraud have continued to increase over recent years.

Table 2. Data on Losses Resulting from Illegal Investment Activities

Year	Estimated Public Financial Losses
2020	IDR 5.9 trillion
2021	IDR 10.4 trillion
2022	IDR 14.7 trillion
2023	IDR 27 trillion

Source: OJK and Satgas PASTI.

The data demonstrate that the development of digital investment not only contributes positively to financial inclusion but also increases the risk of technology-based economic crime. The findings of this study reveal that the most common forms of crime in digital investment activities include investment fraud, Ponzi schemes, misuse of personal data, and manipulation of electronic systems. Ponzi schemes operate by using funds from new investors to pay returns to earlier investors, thereby creating the illusion of profits generated from legitimate investment activities.(Halomoan Napitupulu et al., 2025) In addition, perpetrators frequently utilize social media, instant messaging services, and digital advertisements to disseminate promotions for illegal investments designed to resemble legitimate platforms.

In addition to technological factors, the potential for digital investment crime is also influenced by public behavior. Many investors tend to prioritize rapid profits without adequately considering investment risks and legality. This condition is exacerbated by limited understanding of digital investment mechanisms and insufficient public awareness regarding technology-based fraud schemes.

From the perspective of criminal law, digital investment crimes may generally be classified as offenses involving fraud, embezzlement, and, in certain cases, money laundering. However, the transnational nature of digital crime and its reliance on sophisticated technology significantly complicate law enforcement efforts. Law enforcement authorities are not only required to understand criminal law provisions but must also possess technological expertise to trace perpetrators' activities and uncover digital evidence.(Raharjo et al., 2022)

Furthermore, data from the Ministry of Communication and Digital Affairs indicate that thousands of illegal investment-related content and websites are blocked annually. This condition demonstrates that digital space has become a highly vulnerable medium for investment-related fraud activities.

Table 3. Annual Number of Illegal Investment Websites/Platforms Blocked in Indonesia, 2021–2023

Year	Number of Illegal Investment Websites/Platforms Blocked
2021	1,222 websites
2022	1,730 websites
2023	2,352 websites

Source: Ministry of Communication and Digital Affairs of the Republic of Indonesia.

The foregoing analysis reveals that the development of digital investment has two contradictory dimensions. On the one hand, digital investment provides easier access and promotes greater financial inclusion within society. On the other hand, such development simultaneously creates opportunities for increasingly complex and difficult-to-detect forms of crime. Therefore, more adaptive regulatory reforms, stronger supervision by relevant authorities, and enhanced public digital and financial literacy are necessary to minimize the potential for digital investment crime effectively.

Patterns and the Development of Fraudulent Modus Operandi in Technology-Based Digital Investment

The rapid advancement of digital technology has transformed investment activities into processes that are faster, more accessible, and more flexible. Investments that were previously conducted through conventional mechanisms can now be accessed solely through digital applications and online platforms. Such convenience has contributed to the increasing number of digital investment users in Indonesia. Nevertheless, alongside these developments, various new forms of crime have emerged that exploit technology as the primary instrument for carrying out investment fraud.(Aissyach et al., 2025)

The findings of this study indicate that fraudulent patterns in digital investment have evolved dynamically and become increasingly sophisticated. Perpetrators no longer rely on conventional fraudulent methods; instead, they utilize information technology, digital systems, social media platforms, and psychological manipulation of victims through *social engineering* techniques to obtain unlawful profits. The modus operandi employed is often designed in a highly professional manner, making it difficult to distinguish fraudulent platforms from legitimate investment services.(Cross et al., 2018)

One of the most common fraudulent schemes identified is the Ponzi and pyramid scheme models. In practice, returns paid to earlier investors are not derived from genuine investment activities but rather from funds contributed by new investors. Such schemes generally promise substantial profits within a short period of time, thereby attracting public interest.(Thilakarathna & De Peiris, 2025) During the initial stages, victims are often provided with returns to build trust; however, the system ultimately collapses once the inflow of new funds ceases.

Table 4. Forms of Fraudulent Modus Operandi in Digital Investment

Modus Operandi	Characteristics	Consequences
Ponzi Scheme	Utilizes funds from new investors to pay earlier investors	Massive financial losses
Illegal Trading Robots	Displays manipulated automatic profits	Fraud and transaction data manipulation
Fake Investment Platforms	Websites/applications designed to resemble legitimate platforms	Loss of investor funds
Social Engineering	Psychological manipulation through social media and digital communication	Victims are persuaded to transfer funds
Crypto Asset Fraud	Offering fake tokens or coins	Money laundering and investment losses

Source: Compiled from various reports issued by OJK, Satgas PASTI, and literature relating to digital investment crime, 2025.

In addition to Ponzi schemes, the evolution of fraudulent practices is also evident in the increasing use of illegal trading robots. These schemes has developed alongside growing public interest in digital asset trading, including stocks, foreign exchange (*forex*), and cryptocurrencies. Perpetrators offer automated systems allegedly capable of generating stable profits without risk. In practice, however, many such platforms merely display fictitious profit data and do not conduct actual trading activities within financial markets.(Zellagui et al., 2025)

Another common method involves the use of fake investment platforms or applications. Perpetrators create websites or applications that closely resemble legitimate investment platforms, complete with financial institution logos and professional visual designs to convince victims of their authenticity. During the initial phase, victims are often provided with small profits to increase their confidence and encourage additional investment. However, once substantial funds have been collected, the platform disappears and the victims' assets cannot be recovered.

Table 5. Number of Illegal Investment Entities in Indonesia (2020–2023)

Year	Number of Illegal Investment Entities
2020	99 entities
2021	336 entities
2022	508 entities
2023	537 entities

Source: Task Force for the Eradication of Illegal Financial Activities (*Satgas PASTI*) and the Indonesian Financial Services Authority (OJK), 2024.

The increase in the number of illegal entities demonstrates that perpetrators continuously develop new methods to attract victims through digital media. Social media has become one of the primary instruments used to disseminate illegal investment promotions due to its broad reach and the difficulty of rapidly controlling such content.

Furthermore, patterns of digital investment fraud are strongly influenced by *social engineering* techniques. These techniques involve establishing emotional relationships and trust with victims through social media platforms, instant messaging applications, and digital communities. Perpetrators frequently disguise themselves as investment mentors, financial analysts, or credible public figures, thereby persuading victims to follow their instructions and invest funds.

Figure 2. Pattern of Technology-Based Digital Investment Fraud

Source: Compiled by the author based on patterns observed in digital investment fraud cases in Indonesia, 2025.

The findings further demonstrate that digital investment crimes possess characteristics distinct from conventional criminal activities. First, they are adaptive in nature, meaning that perpetrators continuously modify their modus operandi in accordance with technological developments and societal trends. Second, they are transnational, as perpetrators and victims are often located in different jurisdictions. Third, technology itself functions as the primary instrument for concealing perpetrators' identities, complicating tracing processes, and eliminating transactional evidence.

Table 6. Characteristics of Digital Investment Crime

Characteristics	Explanation
Adaptive	Fraudulent methods evolve alongside technological developments
Transnational	Perpetrators and victims may be located in different countries
Technology-Based	Utilizes applications, websites, social media, and digital systems
Difficult to Trace	Employs false identities and overseas servers
Exploits Victim Psychology	Utilizes emotional manipulation and promises of high returns

Source: Compiled from research findings and literature on cyber criminal law, 2025

From the perspective of criminal law, each fraudulent modus operandi in digital investment may be analyzed through the constituent elements of criminal fraud. Ponzi schemes and fake investment platforms generally fulfill the element of deception through false representations regarding investment legitimacy, projected returns, and operational transparency. The element of a series of lies is reflected in continuous misleading communications, fabricated transaction reports, manipulated profit dashboards, and false testimonials used to maintain investor trust. The element of unlawful conduct is established when perpetrators intentionally operate unlicensed platforms or collect public funds without legal authorization. Victim losses arise when investors transfer funds based on such false information and are unable to recover their assets. Furthermore, the intention to unlawfully benefit oneself or others is evident from the systematic diversion or appropriation of victims' funds for personal or organizational gain. A causal relationship is also present where misleading digital information directly induces victims to transfer funds, thereby completing the chain of criminal liability.

From the perspective of criminal law, these various fraudulent schemes may generally be classified as offenses involving fraud, embezzlement, money laundering, and, under certain circumstances, cybercrime. Nevertheless, law enforcement in cases involving digital investment continues to encounter numerous obstacles, particularly regarding digital evidentiary processes, tracing financial transactions, and identifying perpetrators who employ false identities and foreign servers. In addition to repressive measures through law enforcement, the findings of this study indicate that preventive efforts are equally essential. Enhancing public digital literacy and financial literacy constitutes a primary strategy for reducing the risk of individuals becoming victims of illegal investment schemes. Moreover, supervision of digital investment platforms must be strengthened through cooperation among government institutions, OJK, law enforcement agencies, and digital service providers.(Nugroho & Chandrawulan, 2023) Based on the foregoing analysis, the development of digital investment not only generates economic benefits and promotes financial inclusion but also gives rise to increasingly complex and organized forms of crime. Accordingly, a balance must be established between technological innovation, regulatory strengthening, effective supervision, and increased public awareness to ensure that the development of digital investment remains secure and capable of providing adequate legal protection for society.

The Extent to Which Criminal Law Can Prosecute and Impose Liability upon Perpetrators of Digital Investment Crimes

The rapid development of digital investment has given rise to new forms of crime that possess characteristics distinct from conventional criminal activities. Digital investment crimes are no longer committed through simple or traditional methods; rather, they involve utilization of information technology, electronic systems, and organized transnational networks.(Abdurrahman, 2025) This condition presents serious challenges for criminal law, particularly in determining the extent to which criminal law is capable of effectively prosecuting and imposing liability on perpetrators of digital investment crimes. In this context, criminal law is not only required to provide a normative basis for punishing offenders but must also adapt to technological advancements and continuously evolving patterns of modern crime.(Ahyani et al., 2025)

From the perspective of criminal liability theory, a person may only be subjected to criminal punishment when the elements of actus reus and mens rea are proven through legally admissible evidence. In digital investment crimes, actus reus may be identified through concrete unlawful acts, including the creation and operation of fake investment platforms, dissemination of misleading promotional content, manipulation of profit data or transaction records, unauthorized collection of public funds, and the transfer or diversion of victims' funds into controlled accounts. These acts constitute observable manifestations of fraudulent conduct within digital environments.

Meanwhile, mens rea refers to the perpetrator's guilty mind or criminal intent and may be inferred from various evidentiary indicators. In digital investment fraud, mens rea can be demonstrated through the intentional design of fraudulent schemes, promises of unrealistic or guaranteed returns, deliberate concealment of identity, use of layered bank accounts or crypto wallets to obscure financial flows, deletion of digital traces, and systematic efforts to prevent detection by authorities. Such indicators demonstrate that the unlawful conduct is not accidental but carried out knowingly, deliberately, and with the purpose of obtaining unlawful financial benefit.(King et al., 2020)

This principle of criminal liability is consistent with the doctrine of *nulla poena sine culpa*, which means that there can be no punishment without fault. The doctrine emphasizes that criminal sanctions may only be imposed where fault on the part of the perpetrator can be proven. In digital investment crimes, the element of fault constitutes a particularly important aspect because perpetrators conduct most activities systematically and in a planned manner. Perpetrators not only exploit technology as a means of committing offenses but also consciously establish schemes intended to deceive victims and unlawfully obtain financial benefits.(W. Zhou & Kapoor, 2011) Indonesian criminal law already provides a legal framework capable of prosecuting perpetrators of digital investment crimes. Under the Indonesian Criminal Code (*Kitab Undang-Undang Hukum Pidana* / KUHP), such conduct may be classified as fraud pursuant to Article 378 of the KUHP, which stipulates that 'any person who, with the intention of unlawfully benefiting themselves or another person, uses a false name, deceptive means, or a series of lies to induce another person to surrender property or incur debt may be punished for fraud.' The elements contained within this provision essentially encompass the patterns of digital investment crimes that rely upon information manipulation and deception as primary instruments for obtaining funds from victims.

In addition to Article 378 of the KUHP, certain cases may also be associated with the offense of embezzlement as regulated under Article 372 of the KUHP, particularly where investor funds entrusted to perpetrators are utilized for personal purposes beyond the promised investment objectives. In practice, fraud and embezzlement frequently coexist within digital investment crimes because perpetrators not only obtain funds through deception but also unlawfully control and utilize those funds. Beyond the KUHP, Law Number 11 of 2008 concerning Electronic Information and Transactions, as amended by Law Number 19 of 2016 (ITE Law), also provides an important legal basis for addressing digital investment crimes. Article 28 paragraph (1) of the ITE Law stipulates that any person who intentionally and unlawfully disseminates false and misleading information causing consumer losses in electronic transactions may be subjected to criminal sanctions. This provision is highly relevant to illegal digital investment practices that utilize electronic media to disseminate false information, manipulate profit data, or promote fictitious investment opportunities. Furthermore, because electronic systems constitute the primary means through which such crimes are committed, the ITE Law serves as a crucial legal instrument for addressing the digital dimensions of these offenses.

In its development, digital investment crime is also frequently associated with money laundering offenses. Proceeds obtained through fraudulent investment schemes are commonly transferred through multiple bank accounts, digital assets, or electronic payment systems in order to conceal the illicit origin of the funds. Consequently, Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering may also be applied to prosecute perpetrators of illegal digital investment activities, particularly where attempts to conceal or disguise criminal proceeds are identified. Although the existing legal framework is normatively adequate, the effectiveness of law enforcement against digital investment crime continues to face numerous obstacles. One of the principal challenges lies in the technological and transnational nature of these crimes. In many cases, perpetrators employ false identities, overseas servers, Virtual Private Networks (VPNs), and crypto assets to complicate tracing efforts. Such conditions render evidentiary processes significantly more complex than those associated with conventional criminal offenses.

Within criminal procedural law, evidentiary proof constitutes a fundamental element in determining criminal liability. However, in digital investment crimes, most evidence exists in the form of electronic evidence requiring specialized technical expertise for analysis and verification. Law enforcement authorities are therefore required not only to understand criminal law but also to possess competence in information technology and digital forensics. Limitations in human resources and technological infrastructure remain among the factors contributing to the suboptimal enforcement of laws against illegal digital investment activities.

In addition to individual criminal liability, the development of modern criminal law has also recognized the concept of corporate criminal liability. This concept is particularly relevant because many digital investment crimes are conducted through business entities or corporations that formally appear legitimate. Under the theory of corporate criminal liability, a corporation may be held criminally responsible where an offense is committed by directors, managers, or parties acting for and on behalf of the corporation in pursuit of corporate interests. Accordingly, criminal sanctions may be imposed not only upon individual offenders but also upon legal entities that benefit from the criminal conduct. Nevertheless, the implementation of corporate criminal liability continues to encounter significant challenges, particularly in establishing the relationship between individual conduct and corporate policies or organizational structures. In practice, corporations frequently utilize complex organizational arrangements that make it difficult to determine the parties most responsible for the offense. Furthermore, the absence of specific regulations comprehensively governing digital investment crime has created legal gaps within the law enforcement process.

From the perspective of modern criminal law theory, criminal law should function not merely as a repressive mechanism for punishing offenders after crimes occur but also as a preventive instrument aimed at preventing criminal acts from arising in the first place. Consequently, efforts to address digital investment crime cannot rely solely upon punitive measures. More adaptive regulatory reforms responsive to the development of financial technology are required, alongside strengthened supervision of digital investment platforms, enhanced technological capabilities among law enforcement authorities, and stronger international cooperation in combating transnational digital crimes.(Hecker, 2015)

Accordingly, it may be concluded that Indonesian criminal law fundamentally possesses sufficient normative foundations to prosecute and impose liability upon perpetrators of digital investment crimes through the provisions of the KUHP, the ITE Law, and regulations concerning money laundering offenses. Nevertheless, the effectiveness of their implementation continues to face numerous obstacles related to technological advancement, the complexity of criminal modus operandi, limitations in digital evidence, and weak intersectoral coordination. Therefore, more responsive and adaptive criminal law reform is necessary to ensure that the legal system remains capable of addressing the increasingly complex and dynamic nature of digital investment crime.

CONCLUSION

The rapid development of digital investment in Indonesia has significantly expanded public access to financial markets while simultaneously increasing exposure to technology-based investment crime. This study finds that digital investment fraud has evolved into complex and adaptive forms, including Ponzi schemes, illegal trading robots, fake investment platforms, social engineering, and crypto-related fraud. These crimes are characterized by sophisticated digital manipulation, transnational operations, and difficulties in tracing perpetrators. From the perspective of criminal law, such conduct may fulfill the elements of criminal liability through the establishment of actus reus, reflected in unlawful digital activities, and mens rea, reflected in intentional deception for unlawful financial gain. Indonesian criminal law generally provides sufficient normative grounds to prosecute such offenses through the Criminal Code, the ITE Law, and anti-money laundering regulations, although significant enforcement challenges remain.

This study recommends several normative reforms to strengthen criminal law responses to digital investment crime. First, harmonization is required between the Criminal Code, the ITE Law, anti-money laundering regulations, and OJK regulatory frameworks to reduce legal fragmentation. Second, digital forensic capacity among law enforcement agencies must be strengthened to improve electronic evidence analysis and transaction tracing. Third, clearer evidentiary standards are needed to assess mens rea in digital investment crimes, particularly regarding digital deception, concealment strategies, and fraudulent intent. Fourth, more effective corporate criminal liability mechanisms should be developed to ensure accountability for corporations benefiting from digital investment fraud.

REFERENCES

Abdurrahman, A. (2025). Examining the impact of digital transformation on digital product innovation performance in banking industry through the integration of resource-based view and dynamic capabilities. *Journal of Strategy & Innovation*, *36*(1), 200540. https://doi.org/10.1016/j.jsinno.2025.200540

Ahyani, H., Parhan, P., Muhtolib, M., Berizi, A., Nurhasana, N., & Adnan, N. I. M. (2025). Fraud in the Digital Space: A Comparative Study of Jinayah Fiqh and Indonesian Criminal Law. *Jurnal Hukum Islam*, *23*(1), 37–72. https://doi.org/10.28918/jhi.v23i1.02

Aissyach, A. N. C., Sigid, S. S., & Budi, B. A. A. (2025). Understanding the Characteristics of Pig Butchering Scams: Impact on Victims and Challenges for Law Enforcement in

Indonesia. *KRTHA BHAYANGKARA*, *19*(2), 467–478. https://doi.org/10.31599/krtha.v19i2.3788

AllahRakha, N. (2025). Cross-Border E-Crimes: Jurisdiction and Due Process Challenges. *ADLIYA: Jurnal Hukum Dan Kemanusiaan*, *18*(2), 153–170. https://doi.org/10.15575/adliya.v18i2.38633

Anfas, A., Syamsuddin, F. R., & Zainuddin, Z. (2022). The impact of financial literacy and information technology on millennials' stock market investment motivation. *International Journal of Research in Business and Social Science (2147- 4478)*, *11*(7), 201–209. https://doi.org/10.20525/ijrbs.v11i7.2005

Cross, C., Dragiewicz, M., & Richards, K. (2018). Understanding Romance Fraud: Insights From Domestic Violence Research. *The British Journal of Criminology*, *58*(6), 1303–1322. https://doi.org/10.1093/bjc/azy005

Halawi, L., & Bacon, R. (2024). Exploring the Nexus of Cybercrime, Money Laundering, Ethics and Deterrence in the Age of Smart Machines. In K. Hakan Dogan (Ed.), *Corruption, Bribery, and Money Laundering—Global Issues*. IntechOpen. https://doi.org/10.5772/intechopen.1004131

Halomoan Napitupulu, J., L. Panggabean, M., Panjaitan, H., & Sri Widiarty, W. (2025). An Integrated Legal Framework for Digital Investment Fraud Prevention in Indonesia. *Journal of Sustainable Development and Regulatory Issues (JSDERI)*, *3*(3), 540–567. https://doi.org/10.53955/jsderi.v3i3.154

Hecker, B. (2015). The Development of Individual Rights Protection in European Criminal Law After the Lisbon Treaty. In S. Ruggeri (Ed.), *Human Rights in European Criminal Law* (pp. 1–6). Springer International Publishing. https://doi.org/10.1007/978-3-319-12042-3_1

Irfan Ridha, Intan Rahmadina Putri Harahap, Abdullah Syani Alamsyah, Ahmad Sulaiman, Dea Putri Gustianingsih, Adyta Telianda, Alfani H. Mustofa, Ifthinatul Mupidah, Inayah Al-Inffah, Andre Wirandi, & Dicky Kurniawan. (2024). Efektivitas Hukum Perlindungan Konsumen Dalam Bisnis Investasi Online. *Eksekusi : Jurnal Ilmu Hukum Dan Administrasi Negara*, *3*(1), 42–56. https://doi.org/10.55606/eksekusi.v3i1.1653

Kayser, C. S., Dearden, T., Parti, K., & Choi, S. (2025). Navigating the Digital Frontier: New Perspectives on Cybercrime and Governance. *International Journal of Cybersecurity Intelligence & Cybercrime*, *8*(2). https://doi.org/10.52306/2578-3289.1222

King, T. C., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. *Science and Engineering Ethics*, *26*(1), 89–120. https://doi.org/10.1007/s11948-018-00081-0

Lukiyanto, K., Trisilia, M., Vinanti, S., & Wijayaningtyas, M. (2024). Perception of the Role of Fintech on Formal Workers During the COVID-19 Pandemic (Study on Construction Workers). *KnE Social Sciences*. https://doi.org/10.18502/kss.v9i10.15695

Moh. Ja'far Sodiq Maksum. (2024). Legal Implications of Civil and Criminal Law on Investment Fraud Under the Guise of Online Business. *Indonesian Economic Review*, *4*(1), 29–42. https://doi.org/10.53787/iconev.v4i1.53

Ms. Janvi Sanjay Gotad. (2026). *Digital Transformation in E-commerce, and FinTech*. Nature Light Publication. https://doi.org/10.5281/ZENODO.19316335

Nugroho, A., & Chandrawulan, A. A. (2023). Research synthesis of cybercrime laws and COVID-19 in Indonesia: Lessons for developed and developing countries. *Security Journal*, *36*(4), 651–670. https://doi.org/10.1057/s41284-022-00357-y

Nurmala, L. D., Ariyanti, & Estella Fransisca Workala. (2025). Corporate Criminal Liability in Cases of Investment Fraud Offenses. *Walisongo Law Review (Walrev)*, *7*(1), 1–11. https://doi.org/10.21580/walrev.2025.7.1.25545

Ormerod, D., Laird, K., & Gibson, M. (2024). 2. The elements of a crime: Actus reus. In D. Ormerod, K. Laird, & M. Gibson, *Smith, Hogan, and Ormerod's Criminal Law* (pp. 28–89). Oxford University Press. https://doi.org/10.1093/he/9780198890942.003.0002

Papasavva, A., Lundrigan, S., Lowther, E., Johnson, S., Mariconti, E., Markovska, A., & Tuptuk, N. (2025). Applications of AI-Based Models for Online Fraud Detection and Analysis. *Crime Science*, *14*(1), 7. https://doi.org/10.1186/s40163-025-00248-8

Raharjo, A., Bintoro, R. W., Tri Utami, N. A., & Suzuki, M. (2022). The Legal Policy of Criminal Justice Bureaucracy Cybercrime. *BESTUUR*, *10*(2), 105. https://doi.org/10.20961/bestuur.v10i2.64498

Simpson, S. S. (2002). *Corporate Crime, Law, and Social Control* (1st edn). Cambridge University Press. https://doi.org/10.1017/CBO9780511606281

Study on the Role of Technology in Empowering Individual Investors to make Investment Decisions. (2025). *European Economic Letters*. https://doi.org/10.52783/eel.v15i2.3173

Thilakarathna, A. S., & De Peiris, N. (2025). Financial deception in the digital age: Investigating online pyramid schemes and their socioeconomic impacts in Sri Lanka. *Journal of Financial Crime*, *32*(6), 1191–1210. https://doi.org/10.1108/JFC-03-2025-0073

Wales, K. (2015). Internet finance: Digital currencies and alternative finance liberating the capital markets. *Journal of Governance and Regulation*, *4*(4), 190–201. https://doi.org/10.22495/jgr_v4_i4_c1_p6

Zellagui, W., Imine, A., & Tadjeddine, Y. (2025). Cryptocurrency Frauds for Dummies: How ChatGPT introduces us to fraud? *Digital Government: Research and Practice*, *6*(1), 1–16. https://doi.org/10.1145/3673764

Zhou, W., & Kapoor, G. (2011). Detecting evolutionary financial statement fraud. *Decision Support Systems*, *50*(3), 570–575. https://doi.org/10.1016/j.dss.2010.08.007

Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, *19*(3), 419–439. https://doi.org/10.1007/s11417-024-09436-y