Indonesian Economic Review
Volume. 4, Nomor. 1, February 2024
e-ISSN : 2774-8073 ; Hal. 29-42
DOI: https://doi.org/10.53787/iconev.v4i1.53
Available online at: https://www.iconev.org/index.php/ier

Legal Implications of Civil and Criminal Law on Investment Fraud Under the Guise of Online Business

Moh. Ja'far Sodiq Maksum
Universitas KH. A. Wahab Hasbullah Jombang, Indonesia
Email : jafarsodiq@unwaha.ac.id

Abstract *The development of digital technology has opened new opportunities in online platform-based investments, but it has also increased the risk of fraud disguised as legal businesses. The prevalence of online investment fraud in Indonesia shows that national laws have not fully been able to respond to the complexity of increasingly sophisticated and cross-border digital crimes. This study aims to examine the legal implications, both civil and criminal, of online investment fraud practices and to propose an integrative and adaptive legal approach. The method used is Systematic Literature Review (SLR), by reviewing scientific articles, regulations, and relevant court decisions from 2014 to 2024, based on the PRISMA stages. Research findings indicate that perpetrators employ various modalities such as Ponzi schemes, illegal MLM, and cryptocurrency manipulation, targeting communities with low legal literacy. From the civil perspective, challenges arise regarding the validity of digital contracts and the execution of compensation, while from the criminal perspective, proving elements of fraud and tracking down offenders poses significant challenges. Additionally, the dualism of legal approaches weakens and makes victim protection ineffective. This study concludes that civil and criminal law must synergize through regulatory reform, strengthening institutions, and enhancing public legal literacy to ensure justice and security in digital investment. Legal reforms based on inter-institutional collaboration and responsive to digital dynamics are key to breaking the cycle of fraud that undermines public trust in the national legal and economic system.*

Keywords*: Investment Fraud, Digital Law, Civil Law, Criminal Law, Victim Protection*

1. INTRODUCTION

In recent years, the phenomenon of investment fraud disguised as online business has become a rapidly growing global threat, alongside the increasing use of the internet and digital transformation in the financial sector (Tambunan & Nasution, 2023). This modus operandi often utilizes online platforms to promise high returns in a short period, thus attracting the attention of people from various educational and economic backgrounds (Ahmad, 2024; Anjani et al., 2023; Sulthanah & Ginting, 2025). The losses from fraudulent investment schemes on digital platforms reach billions of dollars per year and continue to increase. The European Securities and Markets Authority (ESMA) has also recorded a surge in public complaints regarding online investment fraud, especially those conducted through social media and unregistered financial applications. In Indonesia, this situation is emerging alongside the increasing digital literacy that is not matched by an understanding of legal frameworks and investment risks. The official website of the Financial Services Authority of Indonesia (www.ojk.go.id) states that by early 2024, there are at least over 1,000 illegal investment entities that have been dealt with. This issue reflects the still weak legal protection system for the public in terms of regulation and law enforcement in the digital space.

Online investment fraud not only causes material losses but also creates profound psychological and social impacts, especially on victims who lose all their savings (Nur,

Received: Januari 20, 2024; Revised: Februari 10, 2024; Accepted: Februari 26, 2024; Published: Februari 28, 2024;

2023). The modus operandi of the perpetrators often involves pyramid schemes, illegal multi-level marketing, as well as offers of fake cryptocurrencies that lack legal basis or operational permits (Tri et al., 2025). According to the United Nations Conference on Trade and Development (UNCTAD), the weakness of international regulatory systems and law enforcement presents a significant gap exploited by actors to cross borders with little hindrance. The absence of global standards in identifying and acting against illegal entities also complicates law enforcement's efforts to trace and freeze assets. The global community, particularly from developing countries, becomes an easy target due to low financial literacy and limited access to legal information. In this context, the conventional legal system has not fully been able to respond to the complexities of cybercrime based on fictitious investments (Harapansyah et al., 2025). Therefore, the need for synergy between national and international legal approaches has become an urgent matter to protect the rights of society as digital consumers.

The rapid increase in internet penetration and the emergence of various digital financial innovations such as peer-to-peer lending, cryptocurrencies, and NFTs have opened up new opportunities for people to access economic prospects, but have also created new vulnerabilities that are often exploited by irresponsible individuals. Many bogus investment platforms claim to have legitimate operations and promise fixed profits, even though they are not registered with the relevant authorities. In Indonesia, the Investment Alert Task Force (SWI) recorded that throughout 2023, the public suffered losses amounting to more than Rp 5 trillion due to illegal investments. This situation indicates that both civil and criminal legal systems need to be optimized to provide a deterrent effect for offenders and maximum protection for victims. Unfortunately, not all cases of fraud can be classified as pure criminal cases due to limitations of evidence, ambiguity of malicious intent (mens rea), and a lack of public understanding of their legal rights. Therefore, a comprehensive and adaptive legal approach is needed to address the changing modes of fraud in the highly dynamic digital era.

In Indonesian law, many cases of investment fraud disguised as online businesses are only addressed through civil mechanisms in the form of breach of contract lawsuits, without adequate criminal consequences. A study by Siregar & Putri (2022) in the IUS Law Journal shows that the confusion between unlawful civil acts and criminal fraud remains a dilemma in the investigation and prosecution process. On the other hand, reporting by Kompas (2024) reveals that many victims struggle to obtain compensation because the perpetrators have fled with assets or engaged in money laundering. Investigative interviews with legal practitioners, as aired on the CNN Indonesia Law and Crime channel, emphasize that law enforcement

often encounters obstacles in proving criminal elements due to a lack of witnesses and weak digital documentation. This problem is exacerbated by the low reporting rates from victims who feel ashamed or afraid of being criminalized for having 'followed' illegal investments. As a result, many perpetrators escape criminal charges and only face administrative sanctions, without considering the significant losses suffered by the community.

Another problem lies in the lack of synchronization of regulations related to digital investor protection among institutions such as OJK, PPATK, and the Police. The 2023 edition of the Rechtsvinding journal notes that regulations concerning online business are still scattered across various sectoral regulations without clear harmonization, making comprehensive law enforcement difficult. On the civil side, the court resolution process tends to take a long time and incur high costs, while on the criminal side, many reports are stalled at the police because the perpetrators operate from abroad or use false identities. In an interview with a former investigator from the National Police's Special Crime Unit, it was mentioned that cases of investment fraud based on applications often end with restorative justice or a termination of investigation (SP3) for efficiency reasons. This situation indicates a normative gap and weaknesses in the legal handling system, in terms of substance, structure, and legal culture. Therefore, an integrated approach between civil and criminal law becomes crucial to create a deterrent effect and maximum protection for the public.

The impact of digital investment fraud is not only felt in the form of individual economic losses but can also undermine public trust in the financial system and state authorities (Nugraha et al., 2025). Many of the victims are housewives, informal workers, and even students who get caught up due to the lure of easy profits through WhatsApp, Telegram, or TikTok groups. The Ministry of Communication and Informatics has recorded that thousands of websites and social media accounts offering illegal investments have been blocked, but they always reappear with new names and methods. This shows that conventional legal measures are not adequately effective in responding to digital crimes that adapt very quickly. A reform of the legal system is needed that focuses not only on sanctions but also on prevention, public education, and the empowerment of the digital community. Digital legal literacy has become an urgent need, especially among the productive age group that is most vulnerable to being targeted by fraudulent investments. Thus, studies examining the implications of civil and criminal law in parallel could serve as a strategic and practical alternative solution.

Although there have been many studies on cybercrime and digital investment fraud, most of the research still focuses on purely criminal aspects or consumer protection alone,

without examining the connection between civil and criminal law in an integral manner. The visible gap is the lack of in-depth analysis on how these two legal domains can be used simultaneously to provide justice and legal certainty for victims. The novelty of this research lies in the dualistic approach between civil and criminal legal instruments within a single analytical framework, as well as exploring how the synergy between the two can enhance the effectiveness of addressing online investment fraud cases. This research will also highlight the sociological and psychological dimensions of the victims, making its approach not only normative but also humanistic.

This research aims to comprehensively analyze the legal implications of civil and criminal law on investment fraud practices disguised as online businesses, as well as to propose a relevant integrated legal approach model that meets the needs of the digital age. The urgency of this research is very high, considering the escalation in the number of victims and the increasingly sophisticated modus operandi of perpetrators that can no longer be addressed with classical legal approaches. It is hoped that the results of this research can serve as a reference for policymakers, law enforcement, academics, and the general public in understanding and anticipating the threats of illegal investments. This research is also expected to encourage regulatory reform in the field of digital law and contribute to improving the legal literacy of society. The great hope is to create a legal system that is adaptive, responsive, and humanistic in protecting citizens from the ever-evolving digital crimes. This research is also intended as an academic contribution to efforts to realize a safer, fairer, and more dignified Indonesia in the rapidly growing digital business world.

2. METHOD

This research uses a Systematic Literature Review (SLR) approach, which is a systematic and structured method to identify, evaluate, and synthesize all relevant literature on a specific topic transparently and replicably (Jispendiora et al., 2023). This type of research is qualitative descriptive, focusing on in-depth analysis of regulations, legal theories, as well as academic findings and legal practices related to investment fraud disguised as online business in the context of civil and criminal law. SLR is chosen because it can provide a comprehensive mapping of how the law is applied and interpreted in various contexts, without having to conduct direct field research. This approach is also suitable for evaluating the novelty, effectiveness of regulations, and the relevance of legal policies in the dynamic digital era.

The data sources in this research consist of primary and secondary literature obtained through national and international academic databases. The selected literature includes legal journals, scholarly books, regulations, court rulings, and official reports relevant to the topic of digital investment fraud. Data selection was carried out using inclusion and exclusion criteria, namely literature published within the last 10 years (2014–2024), relevant to keywords such as 'online investment fraud', 'civil and criminal law', and 'digital legal protection'. Literature lacking an academic foundation or that did not undergo the peer-review process was eliminated to maintain the quality and validity of the data.

Data collection techniques were carried out through a systematic search procedure using structured keywords, initial screening based on abstracts and titles, followed by in-depth content review of the publications that passed the selection stage. After that, the data were analyzed using thematic content analysis methods, by grouping findings based on main themes such as civil and criminal legal bases, fraud modalities, law enforcement, and victim protection. Synthesis was conducted narratively, by comparing various perspectives and different study results, which were then formulated into main findings that address the problem formulation. The SLR process is carried out transparently by documenting every stage of data collection, selection, and analysis so that the research results can be reliable, replicable, and serve as academic references as well as legal policy guidance in the future.

3. RESULT AND DISCUSSION

Patterns and Modes of Online Investment Scams

The rapid development of digital technology has created new opportunities in the economic sector, including platform-based online investment (Adha, 2020). However, on the other hand, this progress is also exploited by irresponsible parties to carry out fraud schemes that are increasingly sophisticated. This research reveals that in the last ten years, there has been a surge in investment fraud cases that use the guise of online companies, either through fake websites, imitation investment apps, or paid social media accounts. The perpetrators generally disguise themselves as investment managers or legal fund managers, providing false legal evidence such as business licenses, tax identification numbers, and fictitious documents from the Financial Services Authority. The tactics used are very persuasive and convincing, complete with promotional videos, fake customer testimonials, and attractive referral bonus offers. The public, who wishes to gain quick profits but has minimal understanding of financial and digital literacy, becomes the main target of these illegal practices. Most victims are unaware that they are being deceived, until the promised profits

do not materialize or the investment system is abruptly closed unilaterally. In this context, the digital world becomes fertile ground for crimes disguised as legitimate businesses.

One of the most dominant modes found in the literature review is the Ponzi scheme, where profits for old investors are paid from the funds of new investors, until the system collapses due to a lack of real income(Cortés et al., 2016). In addition, illegal multi-level marketing (MLM) schemes have also become a popular disguise, presenting promises of sponsorship bonuses and the sale of fictitious or overpriced products compared to their utility. Fraud based on digital assets, such as fake cryptocurrencies, trading robots, and NFTs without technological foundations, has become increasingly rampant since the COVID-19 pandemic, when economic activities shifted to the digital realm. Many perpetrators sell "future investments" that are not licensed by Bappebti or OJK, but exploit the popularity of blockchain technology to lure victims. The perpetrators not only come from within the country but also from cross-border networks that exploit weaknesses in regulations and the limitations of Indonesia's digital oversight. In this scheme, the perpetrators target the productive age group that is active on social media, using a digital marketing strategy that appears professional and credible. When the system collapses, the perpetrators often disappear without a trace, while the victims lose all the funds they have invested. This situation proves that investment fraud has undergone a complex transformation, both technologically and psychologically.

The pattern of the perpetrator's disguise continues to evolve following the developments in communication applications and the security vulnerabilities of digital financial systems (Musyayadah & Margaret, 2024). After receiving attention from the media and authorities, the modus operandi of fraud no longer relies on public websites, but instead shifts to more difficult-to-monitor peer-to-peer communication, such as through WhatsApp groups, Telegram, and Zoom. In many cases, the perpetrators claim that investment opportunities are only opened to 'insiders' or 'priority customers', thus fostering an impression of exclusivity and provoking the curiosity of the victims. This closed communication model makes it difficult to trace the perpetrators, especially if transactions are conducted in cryptocurrency or through third-party accounts that are not easily identifiable. Findings in this study also show that perpetrators typically set daily targets for victims, such as inviting three new members to earn commissions, which further adds to the impression that the scheme is genuinely operational. This system not only harms victims economically but also damages social structures by involving close individuals as recruitment tools. This condition

shows that online fraud not only harms individuals but also has a widespread impact on public trust in the national digital economic system.

One of the factors that further strengthens the effectiveness of this fraud scheme is the low level of digital and legal literacy among the community, especially in urban fringe and rural areas that have only recently come to know app-based investments. Most victims do not understand how to verify the legitimacy of a business entity and are unaware of official reporting channels they can access when they realize they have been scammed. Reports from the Investment Alert Task Force show that out of thousands of reported fraud cases, only a small portion is legally processed because victims do not keep transfer proof or communication with the perpetrators. It is also not uncommon for victims to choose to remain silent for fear of being blamed by family or peers for their poor investment decisionsIn some cases, the victims are even forced by the perpetrators to continue recruiting others so they don't lose their money, thus making them a part of the fraud cycle itself. This phenomenon shows that the aspect of legal protection cannot stand alone without being accompanied by an increase in public awareness and financial education. The government, legal institutions, and players in the digital industry have an important role in creating a safe, transparent, and community-oriented digital ecosystem.

In this situation, the urgency of legal intervention becomes even higher. The state must be present not only as a law enforcement agency after losses occur, but also as a regulator and supervisor of the digital economic system from an early stage. Many findings from the literature emphasize the importance of preventive legal policies, such as strengthening national digital literacy, real-time monitoring of investment applications, and imposing administrative sanctions on platforms that facilitate the promotion of fraud. Criminal and civil law must be able to adapt to the dynamics of the cyber world, including accommodating digital evidence, cryptocurrency transactions, and virtual identities in the investigation and judicial process. In addition, synergy between the Financial Services Authority (OJK), the Ministry of Communication and Information (Kominfo), the Police, and the Financial Transaction Reports and Analysis Center (PPATK) must be enhanced to enable quick action on public reports and to freeze the assets of perpetrators before they flee. Online investment fraud is not merely an individual offense, but has become a threat to the stability of the digital economy and public trust in the legal system. Therefore, a firm, adaptive, and collaborative legal approach is the only way to end this increasingly complex and damaging cycle of fraud.

Implications of Civil Law: Contract Disputes and Damages

From a civil law perspective, online investment fraud is often categorized as breach of contract or unlawful act (Arti & Nur, 2024; Kaunang, 2024). Victims typically sue the perpetrators based on the breached investment agreement or losses due to information manipulation. However, in practice, many obstacles arise because contracts are often made in informal digital forms that do not meet the principles of formal legality. In several rulings, judges have dismissed victims' lawsuits because the contracts lack evidentiary power or do not meet the requirements for a valid agreement according to Article 1320 of the Civil Code. This poses a serious challenge for the community engaging in online transactions, as not everyone understands the importance of formal and notarial legality in business contracts.

The process of civil lawsuits is often ineffective because the perpetrators have disappeared, moved to another country, or do not have assets that can be seized. Even when the victims win the lawsuit, the enforcement of the court's decision is often hindered because the perpetrators are uncooperative and do not have wealth that can be executed. The Lex Justitia Journal notes that 73% of civil lawsuits against fraudulent investment perpetrators fail to achieve loss recovery. This shows that although civil law theoretically grants victims the right to claim compensation, in practice the results are often negligible. Therefore, civil law needs to be redefined to be more adaptive to digital transactions and to provide realistic recovery mechanisms.

Another implication is the confusion among the public regarding the legal channels to take. Many victims do not understand whether they should report to the police or file a lawsuit in civil court (Eliwarti et al., 2009; Suzanalisa, 2011). In many cases, criminal reports are not processed because they are considered ordinary civil disputes, while civil lawsuits do not proceed because the perpetrators are difficult to trace. This phenomenon reveals weaknesses in the design of the legal system that are not synchronized and tend to rigidly separate the civil and criminal realms. In cases of digital fraud, however, both often run concurrently and complement each other. The absence of integrative mechanisms between these two legal avenues causes many victims to lose their legal rights.

The issue arises in terms of proof. Digital evidence such as screenshots, conversations on WhatsApp, or application balance screenshots are often not recognized or questioned regarding their validity in court(Dwivedi & Kakkar, 2023). The Civil Code has not provided an explicit legal framework regarding the strength of electronic evidence, making it heavily reliant on the interpretation of judges. Although the ITE Law acknowledges electronic evidence, its application in the context of civil disputes is still limited. This is what causes

many victims to feel they do not receive justice through civil channels because the legal system has yet to accommodate the complexities of digital transactions. Therefore, it is necessary to update civil law to fully recognize forms of contracts and electronic evidence.

In the context of victim recovery, a civil approach actually has the potential to be a more peaceful and non-repressive solution. However, this can only be realized if the civil justice system is simplified, the processes are expedited, and supported by strong execution mechanisms. One option that can be considered is the establishment of digital commercial courts or online mediation that can quickly and affordably reach a wide audience. The state also needs to provide legal assistance for victims of fraudulent investments so they can effectively access justice. Without systemic intervention, civil law will only become a symbolic instrument that fails to provide a substantive sense of justice for victims of digital crimes.

Legal Implications of Criminal Law: Elements of Fraud and Challenges of Proof

Investment scams disguised as online businesses are often prosecuted under Article 378 of the Penal Code concerning fraud or Article 28 paragraph (1) and Article 45A paragraph (1) of the ITE Law. However, in practice, there is legal ambiguity because not all elements can be adequately proven. The element of 'deception' or 'inducing others to hand over goods' in the Penal Code becomes a subject of debate, especially when the perpetrators disguise their fraudulent motives through investment contracts or digital applications. Investigators and prosecutors often have difficulty proving the malicious intent of the perpetrators since not all cases involve explicit elements of violence, intimidation, or forgery. Many perpetrators present themselves as legitimate entrepreneurs with seemingly legal supporting documentation. In such conditions, law enforcement is caught in doubt as to whether the case warrants criminal charges or should only be pursued civilly(Levi & Reuter, 2006). As a result, criminal reports from victims are often not followed up.

Another serious problem lies in the very rigid proof mechanism in criminal law. Electronic evidence such as screenshots, digital footprints, or online conversation recordings has not been fully recognized as valid or equivalent to conventional evidence, although the ITE Law has regulated its recognition. In practice, proof still requires support from witnesses, experts, and official documents to be accepted in court. Digital fraud perpetrators often use foreign servers, VPNs, or encryption to evade detection, making the investigation process very lengthy or even stalled. This makes handling digital fraud cases tend to be ineffective, often leading to the termination of investigations. This is evidence that the Indonesian

criminal justice system is not yet capable of optimally addressing crimes based on information technology.

The jurisdictional issues in the context of transnational criminal law. Many perpetrators operate from abroad but reach victims in Indonesia through the internet. In this situation, Indonesian law enforcement needs international cooperation to take action against the perpetrators, such as Mutual Legal Assistance (MLA) or extradition. However, this process takes a long time and does not always yield results, as not all countries have extradition treaties with Indonesia. Additionally, digital crimes are fast-paced, and perpetrators can easily move between virtual locations. In this case, enforcement mechanisms become ineffective due to the constraints of territorial boundaries and complicated procedures. The lack of a special cybercrime unit integrated with financial institutions and the judiciary also poses a major barrier to the effective enforcement of criminal law.

The enforcement of criminal law against online investment fraudsters is still minimal in terms of deterrent effect (Hanifawati, 2021; Maharani, 2024). Based on the studies reviewed in the SLR, many offenders are only given light sentences, and there are quite a few who escape due to insufficient evidence. When offenders are sentenced, victims still do not receive significant compensation because criminal law does not automatically regulate restitution. This results in public dissatisfaction with the legal process and triggers a perception that the law does not provide justice for victims of digital crimes. In fact, in certain contexts, the enforcement of criminal law should not only focus on punishment but also on the restoration of victims. Therefore, it is necessary to revise the Criminal Code and the ITE Law to include a comprehensive scheme for the protection and compensation of victims.

In some cases, law enforcement officials also resolve issues through non-litigation avenues such as restorative justice. Although this approach is considered progressive and efficient, in the context of digital investment fraud, it is often irrelevant due to the large number of victims and the significant losses involved. Restorative justice becomes problematic when the perpetrators do not demonstrate goodwill or are unable to compensate for the losses. Therefore, the application of restorative justice must be selective and should not replace formal legal processes in cases of massive fraud. The decision to halt cases for the sake of efficiency must be evaluated ethically and constitutionally. Otherwise, it will set a bad precedent that fraudsters can escape through unfair compromises.

To face this challenge, Indonesia needs a redesign of the digital criminal justice system (Cahyono et al., 2025). The formation of a cross-ministerial cybercrime unit is

needed, collaborating with OJK, PPATK, the Ministry of Communication and Informatics, and international institutions. Reporting systems also need to be strengthened through digital platforms that allow for quick verification, storage of digital evidence, and automated tracking. In addition, enhancing the capacity of personnel in digital forensics is a priority so that the proof of cybercrime no longer relies on conventional evidence. These changes will strengthen the criminal justice system to be able to face the complexities of technology-based investment crimes that are increasingly developing.

Dualism of Civil-Criminal Law and Victim Protection

One important finding in this research is the existence of dualism in legal approaches that often leaves victims of online investment fraud trapped in confusion(Lo Iacono, 2014). They do not know whether to pursue criminal or civil routes, and ultimately they do not receive justice from either. Law enforcement officials frequently shift responsibility for handling cases between agencies without concrete solutions. This reflects a lack of coordination systems among legal institutions in handling digital fraud cases in an integrated manner. When the criminal route cannot prove elements of intent, and the civil route is unable to execute compensation, victims are left to face their losses alone. This creates significant legal uncertainty that is extremely detrimental to society.

When civil and criminal pathways do not run in harmony, the effectiveness of victim protection weakens. Many victims not only suffer material losses but also experience psychological trauma, damaged social relationships, and mental pressure. Unfortunately, the Indonesian legal system has not explicitly regulated the rights of victims of digital fraud, especially those conducted on a large scale. There is no collective compensation system, simple class action lawsuits, or legal insurance schemes capable of ensuring victim recovery. In the journal Rechtsvinding, it is stated that legal protection for victims of digital crime remains sporadic and unsustainable. This indicates an urgent need to establish a systematic, integrative, and socially just victim protection mechanism.

Another issue arises in the context of legal education and literacy in society. Most victims of digital fraud do not have adequate legal understanding and are reluctant to report cases for fear of being blamed. Some victims are actually counter-reported by the perpetrators for allegedly defaming them on social media. This phenomenon proves that besides regulatory aspects, the cultural aspects of law are also very important to consider(Van Hoecke & Warrington, 1998). The public needs to be educated to understand the difference between legal agreements and illegal investments, as well as their legal rights as victims.

Without strong legal literacy, the public will continue to be an easy target for increasingly sophisticated online investment crimes.

From an institutional standpoint, there is currently no mechanism bridging coordination between civil courts, criminal courts, and supervisory institutions such as the OJK and PPATK. There is often a lack of coordination in handling cases, where perpetrators receive criminal sentences but the assets derived from their crimes are not tracked and returned to the victims. Similarly, in civil proceedings, judges are unable to impose criminal sanctions on perpetrators even though the motives for the crimes are very clear. This highlights the importance of designing a dual justice system that allows for the integration of evidence, decisions, and recovery of losses. The establishment of a national task force to tackle digital investment crimes could serve as a strategic medium-term solution.

To address the dualism of law and enhance victim protection, a more flexible and holistic legal approach needs to be developed. For example, through the establishment of lex specialis rules regarding digital investment that simultaneously encompass criminal, civil, and consumer protection aspects. These rules should be complemented by restitution mechanisms, collective compensation, and access to free legal assistance for victims. The state can also leverage technology such as blockchain to track illegal fund flows and ensure that restorative justice can be realized. These efforts will create legal harmony and improve the public's sense of justice towards the national justice system.

Victims of digital investment fraud must be positioned as the main subjects within the legal system, not as passive parties who merely wait for decisions from institutions. Protection for victims cannot be achieved solely through formal judicial routes, but also through state policies oriented towards recovery and prevention. An application-based reporting system, online education, and the establishment of victim advocacy communities could be initial steps. If civil and criminal approaches are not integrated into a broader policy framework, digital investment crimes will continue to proliferate and undermine public trust in the law. Therefore, the synergy between civil and criminal approaches, along with a victim-centered approach, must be a priority in future digital law reforms.

4. CONCLUSION

Investment fraud disguised as online business is a form of complex, structured digital crime that continuously transforms in line with technological developments and gaps in legal regulations. The civil and criminal legal systems in Indonesia, although they provide a normative basis, have not been able to offer comprehensive and effective protection to

victims, especially in terms of proving claims, recovering losses, and taking action against cross-border perpetrators. Disparities in coordination among agencies, low digital literacy among the public, and the absence of a holistic legal policy result in victims not only suffering economic losses but also losing trust in the legal system. Therefore, an integrative, responsive, and justice-based legal approach is needed to build a safe, transparent digital investment ecosystem that favors the wider community.

BIBLIOGRAPHY

Adha, L. A. (2020). Digitalisasi industri dan pengaruhnya terhadap ketenagakerjaan dan hubungan kerja di Indonesia. *Jurnal Kompilasi Hukum, 5*(2), 267–298.

Ahmad, N. H. (2024). Implementasi Undang-Undang No. 8 tentang Pasar Modal terhadap praktek investasi digital pada platform Advance Global Technology. *Journal of Islamic Business Law, 8*(2), 132–145.

Anjani, D. A. M., Hartono, M. S., & Suastika, I. N. (2023). Kajian kriminologis influencer sebagai pelaku penyebar konten judi online di Kabupaten Buleleng. *Jurnal Komunitas Yustisia, 6*(3), 26–36.

Arti, A., & Nur, S. (2024). Pertanggungjawaban hukum perdata terhadap investasi bodong. *Crossroad Research Journal, 1*(3), 38–56.

Cahyono, S. T., Erni, W., & Hidayat, T. (2025). Rekonstruksi hukum pidana terhadap kejahatan siber (cyber crime) dalam sistem peradilan pidana Indonesia. *DJH: Dame Journal of Law, 1*(1), 1–23.

Cortés, D., Santamaría, J., & Vargas, J. F. (2016). Economic shocks and crime: Evidence from the crash of Ponzi schemes. *Journal of Economic Behavior & Organization, 131*, 263–275.

Dwivedi, S. K., & Kakkar, K. (2023). Analysis of impact of social media and information technology on evidence law. *International Journal of Law Management & Humanities, 6*, 1239.

Eliwarti, E., Suranta, F. A., & others. (2009). Perlindungan saksi korban dan restitusi dalam tindak pidana trafiking (Studi di Pengadilan Negeri Lubuk Pakam). *Jurnal Mercatoria, 2*(1), 35–50.

Hanifawati, S. D. (2021). Urgensi penegakan hukum pidana pada penerima pinjaman kegiatan peer to peer lending fintech ilegal dan perlindungan data pribadi. *Jurnal Penegakan Hukum dan Keadilan, 2*(2), 162–172.

Harapansyah, M., Rahman, S., & Badaru, B. (2025). The effectiveness of law enforcement for criminal fraud via WhatsApp in the legal area of the Pasangkayu Police. *International Journal on Advanced Science, Education, and Religion, 8*(1), 77–93.

Jispendiora, J., No, V., Karakter, P., Sekolah, D. I., Norlita, D., Nageta, P. W., & Faradhila, S. A. (2023). Systematic literature review (SLR): Pendidikan karakter di sekolah

dasar. *Jurnal Pendidikan Karakter, 2*(1). *(Catatan: Perlu pastikan nama jurnal dan volume yang akurat karena tidak disebut jelas.)*

Kaunang, J. N. (2024). Tanggung jawab perusahaan pialang terhadap hilangnya aset nasabah dalam investasi online di Indonesia. *Lex Privatum, 13*(3).

Levi, M., & Reuter, P. (2006). Money laundering. *Crime and Justice, 34*(1), 289–375.

Lo Iacono, E. (2014). Victims, sex workers and perpetrators: Gray areas in the trafficking of Nigerian women. *Trends in Organized Crime, 17*, 110–128.

Maharani, F. P. (2024). Perlindungan hukum terhadap korban penipuan online investasi ilegal menurut Undang-Undang Nomor 19 Tahun 2016 perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik dalam perspektif hukum pidana. *Lex Privatum, 13*(4).

Musyayadah, R. A., & Margaret, M. (2024). Strategi pencegahan kejahatan sniffing di M-banking melalui WhatsApp oleh lembaga perbankan. *Ranah Research: Journal of Multidisciplinary Research and Development, 6*(4), 859–867.

Nugraha, R. S., Rohaedi, E., Kusnadi, N., & Abid, A. (2025). The transformation of Indonesia's criminal law system: Comprehensive comparison between the old and new penal codes. *Reformasi Hukum, 29*(1), 1–21.

Nur, F. (2023). Penegakan hukum terhadap kejahatan digital perbankan. *Innovative: Journal of Social Science Research, 3*(6), 3234–3249.

Sulthanah, M. Y., & Ginting, R. (2025). Analisis problematika penegakan hukum terhadap tindak pidana perjudian online di Indonesia. *Jembatan Hukum: Kajian Ilmu Hukum, Sosial dan Administrasi Negara, 2*(2), 1–15.

Suzanalisa, S. (2011). Perlindungan hukum terhadap korban tindak pidana kekerasan seksual dalam sistem peradilan pidana. *Lex Specialist, 14*, 14–25.

Tambunan, R. T., & Nasution, M. I. P. (2023). Tantangan dan strategi perbankan dalam menghadapi perkembangan transformasi digitalisasi di era 4.0. *Sci-Tech Journal, 2*(2), 148–156.

Tri, N. G. A. A. M., Antari, P. E. D., & others. (2025). Penegakan hukum terhadap pelaku kejahatan bisnis dengan sistem Ponzi di Indonesia. *PAMPAS: Journal of Criminal Law, 6*(1), 418–434.

Van Hoecke, M., & Warrington, M. (1998). Legal cultures, legal paradigms and legal doctrine: Towards a new model for comparative law. *International & Comparative Law Quarterly, 47*(3), 495–536.