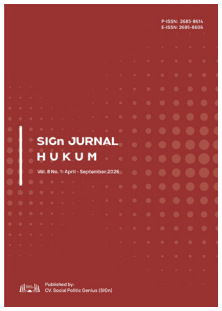

SIGn Jurnal Hukum

E-ISSN: 2685 – 8606 || P-ISSN: 2685 – 8614
https://jurnal.penerbitsign.com/index.php/sjh/article/view/v8n1-11

Vol. 8 No. 1: April - September 2026 Published Online: May 20, 2026

Article Title

A Criminological Review of Futures Investment Fraud: Digital Platform Exploitation and Social Engineering

Author(s)

Maghfirah Ramadhayanti Pagala
Universitas Muhammadiyah Kendari, Indonesia || maghfirahrmdhyntip@gmail.com

Faisal Abdaud*
Universitas Muhammadiyah Kendari, Indonesia || faisal.abdaud@umkendari.ac.id
**Corresponding Author*

Huzaiman Huzaiman
Universitas Muhammadiyah Kendari, Indonesia || huzaiman@umkendari.ac.id

How to cite:

Pagala, M. R., Abdaud, F., & Huzaiman, H. (2026). A Criminological Review of Futures Investment Fraud: Digital Platform Exploitation and Social Engineering. *SIGn Jurnal Hukum, 8*(1), 172-186. https://doi.org/10.37276/sjh.v8i1.698

ABSTRACT

Futures investment fraud has evolved from a conventional economic offense into a systemic financial crisis exploiting the public's psychological vulnerabilities and absence of digital literacy. This research aims to synthesize the criminological anatomy of these crimes, unveil social engineering tactics within cyber ecosystems, and formulate adaptive legal policy prescriptions to restore victims' rights. Utilizing a socio-legal research design based on a literature review, the secondary data corpus is analyzed qualitatively by integrating a statute approach and a conceptual approach toward positive law instruments and reputable international journal literature. The research results prove that crime syndicates exploit white-collar anomic pressure through the creation of multi-level recruitment structures, which are subsequently amplified via cultural pseudo-legitimacy and algorithmic manipulation. These exploitation tactics are sustained by information asymmetry and jurisdictional uncertainty within financial supervisory institutions, which subsequently generates a silence cycle among victims due to the impediment of transnational law enforcement by law enforcement agencies. Halting the continuous cycle of these fictitious investment crimes necessitates a sentencing paradigm shift toward the optimization of asset recovery instruments through the application of money laundering criminal offense regulations. These repressive efforts must be synergistically integrated with mutual legal assistance instruments and the enforcement of anti-fraud firewalls at the financial service sector corporate level.

Keywords: *Asset Recovery; Criminology; Fraud; Futures Investment; Information Asymmetry.*

INTRODUCTION

The transformation of the financial ecosystem toward digitalization has established an environment for organized and transnational white-collar crimes (Edrisy et al., 2023). These cybercrimes pose severe threats to economic stability and public security, particularly in the form of online fraud. In Indonesia, investment schemes act as highly detrimental manipulative instruments to public finances. Official data indicate that accumulated public losses resulting from illegal financial service activities have reached IDR 120 trillion (Febiola & Estherina, 2025). Such a massive scale of loss indicates that investment fraud is not merely a conventional economic crime but a systemic financial crisis that threatens national economic resilience and demands systemic intervention.

This crisis subsequently evaluates classical victimological assumptions, which argue that fraud victims predominantly originate from low-income demographics. Empirical evidence demonstrates a significant shift in victim profiling, where highly educated individuals from the upper-middle class are currently exploited by fictitious investment schemes (Tambunan & Hendarsih, 2022). This phenomenon proves that victim vulnerability is no longer determined by fundamental financial literacy. The modus operandi, systematically constructed through algorithmic manipulation and information asymmetry, establishes a perception of rationality that bypasses the cognitive defenses of educated demographics.

Socioeconomic pressures influencing modern capitalist societies serve as a driving factor for this phenomenon. Merton (1968) asserts that social structures exert strong pressure on individuals to achieve material success, although legitimate avenues for achievement are limited. The discrepancy between the obsession with wealth and the absence of legal access triggers individuals to undertake innovative adaptation through illicit methods. In the context of illegal investments, this pressure operates bi-directionally and simultaneously. White-collar perpetrators are driven to create manipulative schemes to accumulate unlimited capital, while victims are compelled to allocate funds due to the desire for instantaneous high yields.

Manipulative schemes perpetrated by these offenders are concealed behind the facade of formal corporate imagery. Sahetapy (1994) identifies this practice as the primary characteristic of corporate crime, which is laden with identity dualism. Perpetrators design white-collar crimes without physical violence; instead, they exploit public trust through the establishment of pseudo-legitimacy. The offenders systematically abuse religious symbols, provide luxurious office facilities, and demonstrate wealth to conceal their malicious intent (*mens rea*). This manipulative nature, which exploits the foundations of communal culture, results in the public voluntarily surrendering assets without realizing they are targets of organized exploitation within cyberspace.

This organized exploitation proliferates because perpetrators precisely utilize transitional periods and regulatory loopholes within national financial supervision regulations. The development of digital asset instruments and crypto commodities accelerates faster than the establishment of a comprehensive regulatory framework. This creates supervisory coordination ambiguity, particularly regarding jurisdictional obscurity during the transition of institutional authority between the Commodity Futures Trading Regulatory Agency (CoFTRA) and the Financial Services Authority (FSA) as mandated by Law Number 4 of 2023 (Pratama & Angriani, 2025). Offenders perceive these strategic opportunities as momentum to operate fictitious investment platforms and collect public funds before supervisory instruments become fully operational.

Illegal public fund collection resulting in mass losses generates substantive injustice in the law enforcement process. The criminal justice system frequently focuses merely on imposing imprisonment on the perpetrators, failing to facilitate economic recovery instruments for the victims. This practice is evident in the handling of the Auto Trade Gold trading bot case, which involved the losses of thousands of clients (Perdana & Wadrianto, 2024). Although the principal offenders have received criminal sentences, the recovery of victims' rights is hindered by the complexity of asset execution. The absence of integrated restitution causes victims to bear financial

losses absolutely, which subsequently generates a silence cycle where victims are reluctant to report crimes due to trauma and social stigmatization.

These legal and social polemics necessitate a renewal of perspective in criminological studies. Previous studies have tended to dissect illegal investment crimes partially, either by emphasizing cybercrime phenomena generally (Tambunan & Hendarsih, 2022; Tanaka et al., 2025) or focusing purely on dogmatic comparisons of criminal law without sociological foundations (Paluaran et al., 2024). A significant literature gap exists in synthesizing criminological etiology with digital platform exploitation tactics comprehensively. This research addresses this analytical gap by constructing the anatomy of social engineering while simultaneously projecting the provisions in Law Number 1 of 2023 and Law Number 1 of 2024 as adaptive criminal policy instruments for the future.

Specifically, this research aims to construct a comprehensive criminological understanding regarding the anatomy of futures investment fraud. The discussion systematically focuses on the analysis of social pressure etiology, digital platform exploitation tactics, and the effectiveness of closing sectoral regulatory loopholes. Furthermore, this study intends to formulate prescriptive legal countermeasures to optimize victim protection through asset recovery instruments and structural corporate prevention. The results of this research are expected to provide a theoretical foundation for law enforcement and policymakers in designing an economic criminal justice system that permanently eradicates corporate crime motives.

METHOD

This research is constructed utilizing a socio-legal research design based on a literature review. This methodological selection is predicated on the urgency that futures investment fraud cannot be dissected solely through the analysis of static legal norms; rather, it must be comprehended as a phenomenon operating dynamically within social, economic, and digital engineering realities. Within the socio-legal framework, the law is positioned as an instrument that interacts reciprocally with the sources of criminal pathology in society (Qamar & Rezah, 2020). The primary approaches employed encompass a conceptual approach to synthesize structural and cultural criminological doctrines, and a statute approach to evaluate the effectiveness of positive law instruments in responding to cyberspace exploitation.

The data sources in this research are classified into two primary categories to fulfill the objective socio-legal analysis standards. The first category is legal materials, which centers on primary legal materials in the form of authoritative regulations. These primary instruments encompass Law Number 10 of 2011, Law Number 1 of 2023, Law Number 4 of 2023, Law Number 1 of 2024, and FSA Regulation Number 22

of 2023. The second category comprises social data or non-legal materials, extracted from twenty-three reputable national and international scientific journal literatures, as well as credible mass media documentation recording the factual footprints of digital fraud cases to fortify criminological and victimological arguments.

Data collection techniques are implemented entirely through holistic and structured documentary research. The researcher conducted an inventory of legal documents while simultaneously extracting social facts and criminological records from the literature and digital footprints utilizing a topic mapping matrix. This data collection process is designed to establish an objective validity foundation prior to synthesizing the realities of cybercrime with the availability of structural regulatory frameworks. The utilization of a literature review in this research design ensures that all argument constructions are supported by relevant and academically accountable secondary data, thereby negating the necessity for field observations without diminishing analytical acuity (Sampara & Husen, 2016).

The entire validated data corpus is subsequently processed utilizing comprehensive qualitative analysis techniques based on a socio-legal paradigm. The analytical process does not merely evaluate the certainty of a legal text, but confronts these regulations with the empirical reality of the crimes utilizing deductive and inductive reasoning (Irwansyah, 2020). The operational steps of the analysis are systematically structured: commencing with the description of algorithmic manipulation and information asymmetry phenomena, followed by etiological dissection utilizing anomie, differential association, and socio-cultural-structural theories. In the final stage, the research evaluates the jurisdictional uncertainty of institutional transitions to formulate adaptive criminal policy prescriptions, culminating in the optimization of asset recovery instruments to proportionately restore the victims' economic rights.

RESULTS AND DISCUSSION

A. The Criminological Anatomy of Investment Fraud: From Anomic Pressure to Illicit Opportunities

Futures investment fraud does not operate in isolation; rather, it manifests as a cross-class organized crime (Edrisy et al., 2023). The fundamental cause of these financial crimes can be precisely analyzed through the anomie theory. Merton (1968) describes that the structure of capitalist society instills an obsession with material success in all individuals. However, society fails to distribute legitimate means of achievement equitably. This discrepancy generates economic pressure that compels individuals to undertake innovative adaptation by creating illicit methods that violate the law. Specifically for white-collar offenders, this pressure does not originate from structural financial deprivation, but rather from the drive for unlimited capital accumulation in pursuit of financial success expectations.

This innovative adaptation directly generates a primary modus operandi in the form of offering unrealistic yield promises. Offenders exploit the desire for instantaneous wealth among the public, who concurrently experience anomic pressure. This modus of unnatural profit offerings is empirically proven to be the principal method that involves and financially harms victims (Tambunan & Hendarsih, 2022). Dogmatically, this manipulative practice is classified as a definitive criminal offense. Specifically regarding crimes involving the manipulation of futures commodity instruments, Indonesian positive law absolutely prohibits any action of inducing or providing expectations of unreasonable profits. This provision is explicitly regulated in Article 57 of Law Number 10 of 2011, proving that the engineering of public expectations constitutes an economic law violation.

To materialize these fictitious profit promises, offenders require a systematic institutional instrument. Cloward and Ohlin (1960) provide an analytical foundation through the differential opportunity structure theory. This theory elaborates that individuals lacking access to legitimate business structures will establish their own illicit opportunity structures by replicating legal corporate hierarchies. The tangible implementation of this illicit structure is the creation of multi-level recruitment schemes. Perpetrators design pyramid systems and Ponzi schemes as forms of systematic financial crimes to ensure continuous liquidity flow from new members to disburse fictitious profits to earlier members (Pradnyani et al., 2022; Anggriawan et al., 2023).

These multi-level recruitment schemes proliferate because they are sustained by the loss of moral responsibility among the offenders. This phenomenon is not an isolated individual pathology, but rather the result of rationalization internalization explained through the differential association theory, where justifications for manipulative techniques are learned directly within the syndicate network (Sutherland et al., 1992). Perpetrators construct psychological justifications asserting that they are operating legitimate multi-level marketing business entities, a system engineering instrument possessing an extensive track record across various cases (Amar, 2022). Through the rationalization of crime veiled by manipulative corporate characteristics (Sahetapy, 1994), offenders distort reality by engaging in victim-blaming. The offenders normalize the losses by claiming that such circumstances are components of reasonable business risks or the consequence of the victims' own negligence. These conditions fortify the command structure of the fraud syndicate to continuously expand the network without moral impediments.

The combination of anomic pressure, the creation of illicit opportunity structures in the form of Ponzi schemes, and the rationalization of crime establishes a solid foundation for the anatomy of the fraud syndicate. Nevertheless, these

fictitious entities would be incapable of recruiting tens of thousands of victims without amplification instruments that reach the public domain massively. The perpetrators necessitate mechanisms for information distribution and public trust exploitation. Therefore, the etiological analysis of this crime proceeds by dissecting how syndicates transmit manipulative techniques through social engineering within digital platform ecosystems.

B. Digital Platform Exploitation and Social Engineering in Criminal Practices

The digital platform ecosystem has transformed into a psychological manipulation ecosystem sustained by knowledge distribution inequality or information asymmetry. This epistemological disparity destructively intersects with the anomic pressure experienced by the victims. The desire to acquire instantaneous wealth causes victims to disregard rational judgment, while information asymmetry within cyberspace conceals the fact that fraudulent acts are occurring. Cybercrime perpetrators exploit the public's absence of technological literacy regarding the complexity of algorithms and modern investment instruments to monopolize digital narratives unilaterally (Tanaka et al., 2025). Such conditions of information asymmetry and digital marginalization place victims in a defenseless position, rendering them reliant on the perpetrators' fictitious claims.

This digital narrative monopoly is the product of a systematic learning process within the group. This aligns with the differential association theory posited by Sutherland et al. (1992), which postulates that criminal techniques are learned through communicative interactions within a group. Within investment fraud syndicates, social engineering techniques to deceive victims are transmitted hierarchically from network leaders to lower-tier members as a criminal operational standard to replicate manipulation massively (Sari & Faridah, 2022).

The effectiveness of this deviant cultural transmission reaches its apex through the creation of systematic illusions based on algorithmic manipulation. In the Auto Trade Gold trading bot case, the perpetrators' primary method was software manipulation on the application dashboard itself. The syndicate manipulated investment charts to display fictitious profit simulations daily. The syndicate's capability to produce and reproduce visual deception schemes in a coordinated manner successfully involved more than 25,000 cross-border members (Faizal & Hartik, 2023).

To ensure these algorithmic deceptions are accepted without public suspicion, offenders precisely design camouflage tactics that exploit the victims' sociological aspects. This phenomenon can be analyzed utilizing socio-cultural-

structural theories from Sahetapy (1994). Perpetrators recognize that societies with paternalistic cultural roots tend to render obedience to authority figures or status symbols without independently verifying legality. The exploitation of local cultural values possessing communal bonds is utilized as a facade of legitimacy to conceal the *mens rea* of fictitious entities (Saputra et al., 2022).

The tangible manifestation of socio-cultural context abuse within cyberspace is the creation of pseudo-legitimacy. Futures fraud perpetrators exploit religious symbols or Sharia labels to provide an illusion of sanctity to fictitious investment products, thereby degrading the rationality of prospective victims (Miftahuddin, 2020). These tactics are subsequently amplified through social media platforms by practicing flexing and producing fabricated testimonies from fictitious clients. Such visual and social manipulations are structurally designed to construct an artificial reality convincing the public that the investment is secure and possesses legality (Paminto et al., 2024).

Social engineering based on information asymmetry and pseudo-legitimacy constitutes a form of cybercrime that must fall within the jurisdiction of positive law. Dogmatically, the creation of fabricated testimonies on social media has been prosecuted under Article 28 section (1) and Article 45A section (1) of Law Number 1 of 2024, which penalizes the distribution of false information that harms consumers. However, the field application of this offense triggers dogmatic debate. In economic criminal law, the status of pyramid scheme fraud victims cannot be absolutely classified as legitimate consumers, as they participate in unauthorized investment entities. This condition proves that prosecuting fictitious investment crime offenders requires further criminological analysis regarding the urgency of financial sector supervisory regulatory intervention and the application of Law Number 1 of 2023 to close such operational jurisdictional uncertainty.

C. Closing Regulatory Loopholes and Constructing Adaptive Law Enforcement

The dogmatic obscurity within the previously elaborated cyber law instruments creates an avenue for fraud syndicates to exploit regulatory vulnerabilities in the financial sector. This phenomenon is rooted in a legal transitional period that generates a transitional authority duality for digital asset investor protection (Riyaadhotunnisa et al., 2022). Offenders systematically utilize the authority coordination ambiguity in the field, particularly during the transition of institutional authority between the CoFTRA and the FSA (Pratama & Angriani, 2025). This operational jurisdictional uncertainty provides a timeframe for fictitious entities to collect public funds before supervisory instruments become fully operational.

To close these transitional regulatory loopholes, the state intervenes through Law Number 4 of 2023. Article 312 of the Law acts as a jurisdictional loophole closer by mandating the comprehensive transition of digital financial asset regulatory and supervisory duties to the FSA. Dogmatically, this legal certainty truncates the institutional maneuverability utilized by syndicates, although its effectiveness relies on the decisiveness of authority execution. Through this legislation, supervisory authorities are consolidated under a single institution possessing direct enforcement authority against any entity operating without legitimate authorization.

The closure of these jurisdictional loopholes must be balanced with the renewal of substantive criminal law instruments, considering that the complexity of proving capital market crimes makes them difficult to prosecute utilizing obsolete regulations (Opit & Frans, 2025). Considering that criminal law is subject to the legality principle, which prohibits the retroactive application of the law, this fundamental renewal is realized as a future criminal policy projection (*ius constituendum*) through Law Number 1 of 2023. Article 492 of the Law precisely accommodates the social engineering element by penalizing any person utilizing false status or deceit to induce the surrender of assets. Furthermore, Article 488 of the Law aggravates the sanctions for offenders who abuse their profession to commit embezzlement. Comparative analysis confirms that this national legal product is superior and more adaptive as a preventive mitigation instrument in prosecuting modern corporate manipulation (Paluaran et al., 2024).

Although the legal substance has been comprehensively renewed, the decisiveness of these regulations will encounter operational constraints if unsupported by an adequate cyber law enforcement structure. Field facts indicate that fraud syndicates possess the technical capacity to relocate servers or website domains abroad within a brief timeframe. These technological maneuvers create impediments for investigators because cross-border legal jurisdictional boundaries become obscured (Canjaya et al., 2023). The lag in digital forensic infrastructure within law enforcement institutions results in delayed website blocking processes after victims' assets are transferred into transnational money laundering networks.

These asymmetrical operational conditions demand the escalation of law enforcement institutional capacity. Judicial and police institutions require investment in digital forensic development and the enhancement of cyber patrol effectiveness capable of detecting illegal investment algorithmic anomalies (Syahfallah et al., 2026). However, the sophistication of these digital forensics must be integrated with the optimization of international legal cooperation instruments, such as Mutual Legal Assistance Treaties, to reach the haven jurisdictions of the

offenders. Furthermore, the apprehension of criminal offenders and domain blocking within the international cyber domain cannot be perceived as the ultimate limit of enforcement. The success of imposing custodial sentences on perpetrators lacks a comprehensive meaning of justice if the victims' financial losses are not compensated. Therefore, this sentencing analysis must absolutely proceed to the evaluation of legal instrument optimization to trace the offenders' assets and execute the recovery of victims' losses.

D. The Optimization of Victim Protection through Asset Recovery Instruments

The evaluation of the law enforcement construction must culminate in the restoration of justice for the victims. The accumulation of financial losses resulting from the exploitation of transitional regulatory loopholes and social engineering within cyberspace has reached the escalation of a national economic crisis. Official data indicate that the value of public losses resulting from illegal financial service activities has reached IDR 120 trillion (Febiola & Estherina, 2025). Such a massive scale of monetary loss confirms that investment fraud constitutes a systemic financial crisis threatening national economic resilience. Therefore, a criminal law approach oriented solely toward imposing custodial sentences on the perpetrators proves inadequate to resolve the victims' economic losses.

Beyond mere material losses, this crisis generates psycho-social damages that have historically remained beyond the reach of conventional judicial instruments. Investment fraud victims frequently encounter profound trauma and social stigmatization due to the perception of being easily exploited individuals. This psychological pressure generates a silence cycle phenomenon, where shame and fear of public judgment impede victims from reporting the crimes to law enforcement authorities. Sociologically, the silence cycle debilitates crime eradication efforts and provides an avenue for syndicates to operate without impediments. Thus, loss recovery instruments do not merely function to return financial assets, but are necessary to restore the victims' social dignity so they are emboldened to break this chain of silence.

To realize the recovery of the victims' economy and dignity, legal instruments are directed to trace and confiscate the proceeds of crime concealed by syndicate networks. Historically, asset recovery execution constitutes an empirical reality proven in the handling of the Auto Trade Gold trading bot case. In that case, law enforcement successfully executed the confiscation of assets valued at billions of rupiah, utilizing the specific instruments of Law Number 8 of 2010 to be returned to the victims (Perdana & Wadrianto, 2024). This jurisprudence asserts that to eliminate the offenders' anomic motives, namely the drive for unlimited capital accumulation, the state must confiscate all their sources of wealth. As a

prescriptive measure to fortify this foundation, the codification of asset recovery is fundamentally projected through the application of Article 607 of Law Number 1 of 2023.

Although asset recovery precedents exist, claims regarding restitution success must not be perceived naively. The field execution of restitution encounters technical complexities. Law enforcement must trace crypto asset footprints concealed abroad, mitigate the value fluctuations of confiscated assets, and structure a proportional distribution scheme for tens of thousands of victims. These technical impediments prove that a court verdict mandating restitution can transform into a merely normatively binding verdict if unsupported by an adequate asset recovery infrastructure. Therefore, the realization of substantive justice demands the optimization of the FSA's role, which possesses high authority and technical capacity in executing the return of public funds.

Alongside curative instruments in the form of asset recovery, comprehensive mitigation efforts necessitate systemic preventive mechanisms at the corporate level. Illegal investment syndicates operate outside official supervisory jurisdictions, yet their proceeds of crime ultimately traverse the formal financial system. In this context, the state institutionalizes a firewall through Article 55 of FSA Regulation Number 22 of 2023, to compel every legitimate financial service provider, such as national banking institutions, to construct rigorous anti-fraud systems during the preventive stage. Compliance with this regulation ensures that the formal banking system cannot be illegally intervened in and does not become a money laundering conduit for fictitious corporations. The synergy between systemic prevention from the FSA and the optimization of restitution instruments establishes a comprehensive law enforcement system in mitigating the anatomy of investment crimes in the digital era.

CONCLUSIONS AND SUGGESTIONS

Futures investment fraud constitutes a structural threat exploiting the public's psychological vulnerabilities and digital literacy disparities. Based on criminological etiological analysis, these criminal practices are triggered by the anomic pressure upon white-collar demographics to accumulate capital limitlessly, materialized through the creation of illicit opportunity structures in the form of multi-level recruitment schemes. This modus operandi is systematically transmitted within syndicate networks and amplified through social engineering within cyber ecosystems. Perpetrators manipulate software algorithms to construct illusions of fictitious profits, exploit religious and cultural symbols to establish pseudo-legitimacy, and utilize information asymmetry to degrade the victims' rational judgment. The combination of sociological

and technological exploitation proves that modern investment fraud is a covert corporate crime reaching across all social classes.

The crime syndicates' success in involving tens of thousands of victims is facilitated by the exploitation of operational jurisdictional uncertainty during sectoral regulatory transitions and the dogmatic obscurity of cyber law instruments. Although the state has conducted structural intervention through Law Number 4 of 2023 to consolidate supervisory authorities, and projected Law Number 1 of 2023 to prosecute the abuse of false status, field law enforcement continues to encounter transnational jurisdictional impediments. The suboptimal digital forensic infrastructure of law enforcement agencies results in delays in anticipating the perpetrators' maneuvers in relocating cyber servers and concealing the proceeds of crime. These asymmetrical operational conditions exacerbate the victims' psycho-social damages, generating a silence cycle due to public stigmatization and injuring the achievement of a substantive sense of justice.

Addressing the complexity of this criminal anatomy, the policy implication that must be realized is a criminal justice paradigm shift from an orientation of imposing custodial sentences toward the optimization of asset recovery instruments. Judicial institutions and law enforcement agencies are recommended to apply money laundering criminal offenses instruments to trace and execute the return of victims' financial losses, ensuring the perpetrators' capital motivations can be permanently eliminated. Concurrently, absolute structural preventive measures are required through the enforcement of compliance with FSA Regulation Number 22 of 2023. This regulation must function as a firewall compelling all legitimate financial service providers to construct rigorous anti-fraud systems. Considering the transnational nature of these syndicate operations, the digital forensic acuity of domestic agencies must be integrated with mutual legal assistance instruments to reach the perpetrators' haven jurisdictions. Comprehensive synergy among international legal cooperation, restitution optimization, and structural corporate defense constitutes the primary key to halting the continuous cycle of fictitious investment crimes in the digital era.

REFERENCES

Amar, A. A. P. (2022). TVI Express Member Rights based on Consumer Protection Perspective. *SIGn Jurnal Hukum*, *3*(2), 84-100. https://doi.org/10.37276/sjh.v3i2.129

Anggriawan, R., Susila, M. E., Sung, M. H., & Irrynta, D. (2023). The Rising Tide of Financial Crime: A Ponzi Scheme Case Analysis. *Lex Scientia Law Review*, *7*(1), 307-346. https://doi.org/10.15294/lesrev.v7i1.60004

Canjaya, M. A. D., Lubis, Y., & Affan, I. (2023). Penegakan Hukum Terhadap Pelaku Tindak Pidana Penipuan dengan Modus Investasi (Studi di Kepolisian Resor Asahan). *Jurnal Meta Hukum*, *2*(3), 128-140. Retrieved from https://ejournal.steitholabulilmi.ac.id/index.php/metahukum/article/view/453

Cloward, R. A., & Ohlin, L. E. (1960). *Delinquency and Opportunity: A Theory of Delinquent Gangs*. Free Press. https://books.google.co.id/books?id=nf09AAAAYAAJ

Edrisy, I. F., Kamilatun, K., & Putri, A. (2023). *Kriminologi*. Pusaka Media. https://repository.umko.ac.id/id/eprint/291

Faizal, A., & Hartik, A. (2023, March 8). *Member Robot Trading ATG Wahyu Kenzo Capai 25.000 Orang, Kerugian Rp 9 Triliun*. Kompas. Retrieved February 21, 2026, from https://surabaya.kompas.com/read/2023/03/08/165554578/member-robot-trading-atg-wahyu-kenzo-capai-25000-orang-kerugian-rp-9

Febiola, A., & Estherina, I. (2025, August 19). *OJK: Kerugian akibat Jasa Keuangan Ilegal Rp 120 Triliun*. Tempo. Retrieved February 21, 2026, from https://www.tempo.co/ekonomi/ojk-kerugian-akibat-jasa-keuangan-ilegal-rp-120-triliun-2060734

Irwansyah. (2020). *Penelitian Hukum: Pilihan Metode & Praktik Penulisan Artikel*. Mirra Buana Media.

Law of the Republic of Indonesia Number 32 of 1997 on Commodity Futures Trading (State Gazette of the Republic of Indonesia of 1997 Number 93, Supplement to the State Gazette of the Republic of Indonesia Number 3720). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/574

Law of the Republic of Indonesia Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2008 Number 58, Supplement to the State Gazette of the Republic of Indonesia Number 4843). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/138

Law of the Republic of Indonesia Number 8 of 2010 on Prevention and Eradication of the Crime of Money Laundering (State Gazette of the Republic of Indonesia of 2010 Number 122, Supplement to the State Gazette of the Republic of Indonesia Number 5164). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/232

Law of the Republic of Indonesia Number 10 of 2011 on Amendment to Law Number 32 of 1997 on Commodity Futures Trading (State Gazette of the Republic of Indonesia of 2011 Number 79, Supplement to the State Gazette of the Republic of Indonesia Number 5232). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/247

Law of the Republic of Indonesia Number 19 of 2016 on Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2016 Number 251, Supplement to the State Gazette of the Republic of Indonesia Number 5952). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1683

Law of the Republic of Indonesia Number 1 of 2023 on the Penal Code (State Gazette of the Republic of Indonesia of 2023 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6842). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1818

Law of the Republic of Indonesia Number 4 of 2023 on Financial Sector Development and Strengthening (State Gazette of the Republic of Indonesia of 2023 Number 4, Supplement to the State Gazette of the Republic of Indonesia Number 6845). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1821

Law of the Republic of Indonesia Number 1 of 2024 on the Second Amendment to Law Number 11 of 2008 on Electronic Information and Transactions (State Gazette of the Republic of Indonesia of 2024 Number 1, Supplement to the State Gazette of the Republic of Indonesia Number 6905). https://www.dpr.go.id/dokumen/jdih/undang-undang/detail/1842

Merton, R. K. (1968). *Social Theory and Social Structure* (Revised Edition). Simon and Schuster. https://books.google.co.id/books?id=dyqZOcux9o0C

Miftahuddin, M. (2020). Revitalisasi Kearifan Lokal dan Nilai Keislaman dalam Pengembangan Potensi Pariwisata Syariah. *Jurnal Al-Iqtishad*, *16*(1), 54-67. https://doi.org/10.24014/jiq.v16i1.9722

Opit, S. E., & Frans, M. P. (2025). Proving Securities Trading Fraud in Capital Market Crimes. *SIGn Jurnal Hukum*, *7*(1), 54-69. https://doi.org/10.37276/sjh.v7i1.413

Paluaran, D., Purwanda, S., Kasim, A., & Jumardin, J. (2024). Analisis Komparatif Tindak Pidana Penipuan dalam KUHP Kolonial dan KUHP Nasional. *Jurnal Litigasi Amsir*, *11*(3), 345-351. Retrieved from https://journalstih.amsir.ac.id/index.php/julia/article/view/434

Paminto, S. R., Amalia, M., Mulyana, A., & Auliya, A. H. (2024). Peran Hukum dalam Melindungi Korban Penipuan Media Sosial Perspektif Sosiologi. *Journal Customary Law*, *2*(1), 1-18. https://doi.org/10.47134/jcl.v2i1.3335

Perdana, N., & Wadrianto, G. K. (2024, November 19). *Bakal Terima Ganti Rugi, Korban Robot Trading ATG Datangi Kejari Kota Malang*. Kompas. Retrieved February 21, 2026, from https://surabaya.kompas.com/read/2024/11/19/191833878/bakal-terima-ganti-rugi-korban-robot-trading-atg-datangi-kejari-kota-malang

Pradnyani, N. P. R. S., Budiartha, I. N. P., & Widyantara, I. M. M. (2022). Tindak Pidana Penipuan Investasi Fiktif di Pasar Modal Menggunakan Skema Piramida. *Jurnal Preferensi Hukum*, *3*(2), 443-449. https://doi.org/10.55637/jph.3.2.4960.443-449

Pratama, R., & Angriani, J. (2025). Legal Protection for Investors in Cases of Illegal Cryptocurrency-Based Investments in Indonesia. *Journal of Law Science*, *7*(2), 278-286. Retrieved from https://iocscience.org/ejournal/index.php/jls/article/view/6080

Qamar, N., & Rezah, F. S. (2020). *Metode Penelitian Hukum: Doktrinal dan Non-Doktrinal*. CV. Social Politic Genius (SIGn). https://books.google.co.id/books?id=TAQHEAAAQBAJ

Regulation of the Financial Services Authority of the Republic of Indonesia Number 22 of 2023 on Consumer and Public Protection in the Financial Services Sector (State Gazette of the Republic of Indonesia of 2023 Number 40/OJK, Supplement to the State Gazette of the Republic of Indonesia Number 62/OJK). https://peraturan.go.id/id/peraturan-ojk-no-22-tahun-2023

Riyaadhotunnisa, S., Amirulloh, M., & Yuanitasari, D. (2022). Activities of Uncertified Crypto Asset Physical Traders: A Study of Legal Protection for Investor. *SIGn Jurnal Hukum*, *4*(2), 160-172. https://doi.org/10.37276/sjh.v4i2.211

Sahetapy, J. E. (1994). *Kejahatan Korporasi*. Eresco.

Sampara, S., & Husen, L. O. (2016). *Metode Penelitian Hukum*. Kretakupa Print.

Saputra, K. A. K., Mu'ah, M., Jurana, J., Korompis, C. W. M., & Manurung, D. T. H. (2022). Fraud Prevention Determinants: A Balinese Cultural Overview. *Australasian Accounting, Business and Finance Journal*, *16*(3), 167-181. https://doi.org/10.14453/aabfj.v16i3.11

Sari, W., & Faridah, H. (2022). Analisa Kriminologis Kejahatan Pencurian Berdasarkan Teori Differential Association. *Jurnal Panorama Hukum*, *6*(2), 111-118. Retrieved from https://ejournal.unikama.ac.id/index.php/jph/article/view/6084

Sutherland, E. H., Cressey, D. R., & Luckenbill, D. F. (1992). *Principles of Criminology* (Eleventh Edition). General Hall. https://books.google.co.id/books?id=JVB3AAAAQBAJ

Syahfallah, Z. A., Razak, A., & Salle, S. (2026). The Effectiveness of Law Enforcement on Cybercrime: A Case Study of Online Fraud in South Sulawesi. *SIGn Jurnal Hukum*, *7*(2), 1116-1130. https://doi.org/10.37276/sjh.v7i2.557

Tambunan, D., & Hendarsih, I. (2022). Waspada Investasi Ilegal di Indonesia. *Perspektif: Jurnal Ekonomi dan Manajemen Akademi Bina Sarana Informatika*, *20*(1), 108-113. https://doi.org/10.31294/jp.v20i1.12518

Tanaka, V., Chandra, J., & Banke, R. (2025). Kriminalitas di Era Digital: Kajian Kriminologi Terhadap Kejahatan Online. *Jurnal Pendidikan, Sosial, dan Humaniora*, *4*(4), 6095-6100. https://doi.org/10.56799/peshum.v4i4.9352