The Legal Challenges of Corporate Criminal Liability in Robot Trading and Binary Option Investment Fraud

Edi Winata, Henry Aspan, Fitri Rafianti

Abstract

The development of digital investment platforms, particularly robot trading and binary option applications, has created new opportunities for investment while simultaneously generating complex forms of investment fraud. This research aims to analyze the legal challenges of establishing corporate criminal liability for fraudulent investment activities conducted through robot trading and binary option platforms and to examine the adequacy of the existing legal framework in protecting investors. This research employs a normative juridical method using a statutory, conceptual, and case approach. Legal materials are analyzed qualitatively through systematic and juridical interpretation of legislation, legal doctrines, and relevant scholarly literature concerning corporate criminal liability, digital investment, and financial fraud. The results demonstrate that establishing corporate criminal liability in digital investment fraud faces challenges related to identifying the corporate actor, attributing criminal conduct to corporations and their management, proving fraudulent intent, tracing digital financial transactions, and determining the relationship between corporate responsibility and the individual responsibility of directors or other controlling persons. The research concludes that corporate criminal liability must be strengthened through clearer attribution standards, effective digital evidence mechanisms, and coordinated financial and criminal law enforcement. The implication is that regulatory harmonization and stronger corporate accountability are necessary to provide legal certainty, protect investors, and prevent the development of increasingly sophisticated digital investment fraud.

Keywords: Corporate Criminal Liability; Digital Investment Fraud; Robot Trading; Binary Options; Corporate Crime; Investor Protection.

[1]Edi Winata
Master of Laws, Panca Budi Development University, Indonesia
e-mail: winataedi0406@gmail.com

[2,3]Henry Aspan, Fitri Rafianti
e-mail: henryaspan@dosen.pancabudi.ac.id, fitrirafianti@dosen.pancabudi.ac.id
2nd International Cofference on the Epicentrum of Economic Global Framework (ICEEGLOF)
Theme: Navigating The Future: Business and Social Paradigms in a Transformative Era.
https://proceeding.pancabudi.ac.id/index.php/ICEEGLOF

Introduction

The rapid development of digital technology has fundamentally transformed the investment sector. Investment activities that were previously conducted through conventional financial institutions can now be accessed through digital platforms offering various financial and investment products. This development provides convenience, speed, and broader access to investment opportunities. However, digitalization also creates new challenges for law enforcement because investment activities can be conducted across jurisdictions, transactions can be performed electronically, and information concerning the identity and activities of investment operators may be difficult to verify. The development of digital financial activities has therefore created a legal environment in which technological innovation and investor protection must develop simultaneously.

One of the increasingly problematic forms of digital investment involves robot trading and binary option platforms. Robot trading is generally promoted as an automated trading system that utilizes algorithms or software to execute transactions, while binary options are presented as digital financial products in which users speculate on the movement of an underlying asset within a predetermined period. In practice, certain platforms have been associated with misleading investment offers, unrealistic profit promises, aggressive recruitment systems, and the collection of funds from members of the public without adequate legal authorization. Such circumstances demonstrate that digital investment fraud cannot be viewed merely as a conventional fraud conducted through a different medium, but requires a legal framework capable of addressing the technological and organizational characteristics of digital platforms.

The complexity becomes greater when fraudulent investment activities are conducted through a corporate structure. Digital investment platforms may involve companies, directors, managers, promoters, affiliates, technology providers, payment intermediaries, and other parties. Consequently, identifying the person who should bear criminal responsibility is not always straightforward. A fraudulent investment scheme may be designed, managed, or facilitated collectively, while the corporation itself may function as the instrument through which funds are collected from investors. This raises a fundamental legal question concerning whether criminal responsibility should be attributed exclusively to individual actors or may also be imposed upon the corporation as a legal entity.

The development of corporate criminal liability has changed the traditional understanding of criminal law, which historically focused primarily on individuals as perpetrators. The recognition of corporations as subjects of criminal law reflects the reality that corporations can possess organizational structures, resources, decision-making mechanisms, and economic interests that enable them to commit or facilitate criminal conduct. Therefore, the principle of corporate accountability is increasingly relevant in addressing economic crimes and financial crimes committed through complex organizational structures.

The issue of corporate criminal liability is particularly significant in digital investment fraud because the separation between the corporation, its management, and the technological platform may create difficulties in attributing criminal conduct. A corporation may argue that fraudulent conduct was committed by individual employees, agents, affiliates, or third-party promoters. Conversely, individual managers may attempt to avoid responsibility by asserting that the relevant decisions were made within the corporate structure. This situation creates a potential accountability gap in which victims suffer losses while the actual beneficiary or controlling party remains difficult to identify.

The development of the Indonesian criminal law system demonstrates that the concept of criminal responsibility has evolved in response to changing forms of crime and changes in society. Siregar, Adrian, and Rambe explain that the development of the criminal law system

in Indonesia has been influenced by historical and legal developments that have shaped the structure of criminal responsibility and law enforcement [1]. This development is relevant to corporate criminal liability because the emergence of technologically mediated crimes requires criminal law to respond to forms of conduct that may not fit neatly within traditional individual-based models of responsibility.

The comparison of criminal law systems also provides an important conceptual basis for examining corporate responsibility. Siregar explains that comparative criminal law allows legal scholars to examine differences in criminal responsibility, criminal sanctions, and mechanisms for dealing with criminal conduct across legal systems [2]. From this perspective, corporate criminal liability requires clear principles concerning the attribution of an individual's conduct to a corporate entity. Without clear attribution standards, the enforcement of criminal law against corporations may become inconsistent and unpredictable.

The problem of digital investment fraud is also closely related to the development of digital financial services. Aspan, Nasution, and Malikhah explain that the development of digital banking and cashless culture in Indonesia has significantly changed the way financial transactions are conducted and has generated new regulatory challenges [3]. Although digital investment platforms differ from digital banking, the development of financial technology demonstrates a broader transformation in financial transactions in which legal regulation must adapt to technological innovation and increasingly digital forms of economic activity.

The development of digital transactions also creates challenges in relation to the identification and verification of parties involved in online activities. Aspan et al. emphasize the importance of technological and legal adaptation in the development of cyber-related transactions [4]. In the context of robot trading and binary options, the digital character of the platform may complicate the collection of evidence, identification of controlling parties, tracing of funds, and determination of the location where criminal conduct occurred. These circumstances require law enforcement to integrate conventional criminal law principles with digital evidence and financial investigation mechanisms.

The state of the art of this research is situated at the intersection of corporate criminal law, digital investment regulation, cybercrime, and investor protection. Existing legal studies concerning investment fraud generally focus on individual perpetrators, fraudulent investment practices, consumer losses, or the legality of investment platforms. Meanwhile, studies concerning corporate criminal liability tend to focus on conventional corporate crimes and questions of attribution between corporations and their management. There remains a need for more integrated analysis concerning how corporate criminal liability should operate when investment fraud is conducted through technologically complex platforms such as robot trading and binary options.

The central research gap therefore concerns the legal mechanism for attributing fraudulent conduct committed through digital investment platforms to a corporate entity. The problem is not simply whether a corporation can be held criminally responsible, but under what legal circumstances the conduct of directors, managers, employees, agents, or controlling persons can be attributed to the corporation. This issue becomes particularly important where corporate structures are intentionally used to conceal the identity of the actual perpetrators or beneficiaries of the fraudulent scheme.

Another important issue concerns proof of corporate involvement. Digital investment fraud may involve electronic communications, platform records, digital wallets, bank accounts, transaction histories, algorithms, promotional materials, and social media activity. These forms of evidence must be connected to the decision-making structure of the corporation to establish whether the fraudulent conduct resulted from corporate policy, corporate benefit, inadequate supervision, or the acts of individuals acting within the scope of their corporate functions.

The principle of accountability becomes particularly important in this context. Aspan's discussion of good corporate governance emphasizes the importance of accountability and

responsibility in corporate management [5]. These principles can be extended to the criminal law context by requiring corporations and their management to maintain adequate systems of supervision, compliance, and risk control. Where a corporation benefits from fraudulent investment activities or fails to prevent misconduct despite having the capacity to do so, the question of corporate criminal responsibility becomes increasingly significant.

The problem is further complicated by the distinction between corporate criminal liability and individual criminal liability. The imposition of criminal responsibility upon a corporation should not automatically eliminate the responsibility of directors, managers, or other individuals who intentionally participate in the offense. Conversely, the existence of individual perpetrators should not automatically exclude corporate responsibility where the corporation itself is involved in, benefits from, or facilitates the criminal conduct. A comprehensive legal framework must therefore regulate the relationship between these forms of responsibility.

Digital investment fraud also demonstrates the importance of the principle of legal certainty. Investors must be able to determine whether a platform is legally authorized, who operates it, what financial products are being offered, and what legal protection is available when losses occur. From the perspective of criminal law, law enforcement must also have sufficient legal certainty to determine the applicable offense, identify the responsible party, collect evidence, and impose sanctions based on a clear legal basis.

The enforcement of corporate criminal liability should also take into account the principle of proportionality. Not every violation committed within a corporation should automatically result in criminal responsibility for the corporate entity. There must be an assessment of the corporation's involvement, the role of its management, the benefits obtained, the level of supervision, the nature of the violation, and the consequences suffered by investors. Proportionality is necessary to distinguish between deliberate corporate fraud and isolated misconduct committed by an individual without corporate knowledge or benefit.

The scientific novelty of this research lies in developing an analytical model for establishing corporate criminal liability in digital investment fraud by integrating three dimensions: corporate attribution, digital evidence, and investor protection. Corporate attribution determines the relationship between the conduct of individuals and the corporate entity. Digital evidence provides the evidentiary basis for tracing decision-making, communication, transactions, and financial benefits. Investor protection provides the normative objective for ensuring that criminal law enforcement does not merely punish perpetrators but also addresses the consequences suffered by victims.

The proposed approach can be formulated through the following analytical sequence:
Digital Investment Activity → Identification of Corporate Structure → Identification of Individual Actors → Attribution of Conduct to Corporation → Digital and Financial Evidence → Determination of Criminal Responsibility → Corporate and Individual Sanctions → Investor Protection.

This approach is intended to overcome the limitations of a purely individual-oriented criminal law analysis. In digital investment fraud, the corporation may provide the platform, receive investor funds, organize promotional activities, employ technology, or benefit economically from the fraudulent scheme. Therefore, determining responsibility requires examination of the organizational context in which the offense occurred.

The research addresses three principal problems. First, how can criminal responsibility be attributed to corporations in investment fraud conducted through robot trading and binary option platforms? Second, what legal challenges arise in proving corporate involvement and the relationship between corporate and individual criminal responsibility in digital investment fraud? Third, how should the corporate criminal liability framework be developed to provide legal certainty and effective protection for investors?

The purpose of this research is therefore to analyze the legal basis and mechanism for imposing criminal responsibility on corporations involved in robot trading and binary option

investment fraud, identify the challenges associated with attributing criminal conduct within digital corporate structures, and formulate a more effective corporate accountability framework. The research also seeks to examine how digital evidence and financial transaction tracing can support the establishment of corporate criminal responsibility.

The significance of this research lies in its contribution to the development of criminal law in response to digital economic crime. The findings are expected to provide a conceptual basis for law enforcement agencies, regulators, and legal practitioners in determining the responsibility of corporations and individuals involved in fraudulent digital investment activities. Stronger corporate accountability is also expected to prevent corporations from being used as instruments for fraudulent schemes and to ensure that technological innovation in the financial sector remains consistent with the principles of legality, accountability, and investor protection.

Ultimately, the legal challenge of corporate criminal liability in robot trading and binary option investment fraud is not limited to identifying the existence of fraud. The more fundamental challenge is determining who should be held responsible, on what legal basis, and through what evidentiary mechanism. A responsive legal framework must therefore accommodate the organizational characteristics of corporations, the technological nature of digital platforms, the complexity of electronic and financial evidence, and the need to protect investors. Addressing these challenges is essential for strengthening legal certainty and ensuring that digital innovation does not become an instrument for sophisticated forms of corporate crime.

Literature Review

The literature review in this research focuses on the relationship between corporate criminal liability, digital investment fraud, robot trading, binary options, digital evidence, and investor protection. The development of digital investment platforms has created a new environment for economic activity in which traditional legal concepts of fraud and criminal responsibility must be applied to increasingly complex technological and corporate structures. Therefore, the analysis of corporate criminal liability requires an interdisciplinary understanding of criminal law, corporate law, financial regulation, and digital technology.

1. Corporate Criminal Liability

Corporate criminal liability represents a development of criminal law that recognizes corporations as potential subjects of criminal responsibility. Traditionally, criminal law was primarily constructed around the individual as the perpetrator of an offense. However, the development of modern economic activities demonstrates that criminal conduct can be planned, facilitated, and benefited from through organizational structures. Consequently, corporations can become instruments, beneficiaries, or even active participants in criminal activities.

Siregar, Adrian, and Rambe explain that the development of the Indonesian criminal law system has involved significant changes in the understanding of criminal responsibility in response to developments in society and the forms of criminal conduct [1]. This development provides a conceptual basis for recognizing that criminal responsibility must adapt to the emergence of collective and organizational forms of crime.

In the context of corporate crime, the fundamental issue is not merely whether a corporation can be treated as a subject of criminal law but how the conduct of individuals within a corporate organization can be attributed to the corporation. Directors, managers, employees, agents, or

other persons may act within the corporate structure, and their conduct may potentially generate corporate criminal responsibility when the relevant legal requirements are fulfilled.

2. The Concept of Attribution in Corporate Criminal Responsibility

The concept of attribution constitutes one of the most important issues in determining corporate criminal responsibility. A corporation is an artificial legal entity and cannot physically perform an act in the same manner as an individual. Corporate conduct is therefore manifested through decisions and actions taken by individuals who represent, manage, control, or work for the corporation.

From a legal perspective, corporate attribution may be constructed through several approaches, including the identification of the corporation with its directing mind, vicarious responsibility, corporate culture or organizational fault, and liability based on failure of supervision. Each approach has different implications for determining whether an individual's conduct can be considered the conduct of the corporation.

Siregar's discussion of comparative criminal law demonstrates the importance of examining different approaches to criminal responsibility in order to understand how legal systems respond to changing forms of criminal conduct [2]. In the context of digital investment fraud, comparative analysis is relevant because corporate structures and digital platforms can operate beyond conventional territorial boundaries.

The attribution problem becomes particularly complicated when a corporation claims that fraudulent activities were committed solely by individual employees, agents, or affiliated promoters. Therefore, the analysis must examine whether the corporation benefited from the conduct, whether the conduct was carried out within the scope of corporate activities, whether corporate management knew or should have known about the conduct, and whether the corporation failed to establish adequate supervision and compliance mechanisms.

3. Corporate Criminal Liability and Good Corporate Governance

Corporate criminal responsibility is closely connected with the concept of good corporate governance. A corporation is not merely an economic entity but also an organizational structure that must operate based on accountability, responsibility, transparency, and proper management.

Aspan explains that good corporate governance principles emphasize accountability and responsibility in corporate management [3]. These principles are relevant to corporate criminal law because corporations that operate financial or investment platforms have a responsibility to maintain internal controls, prevent fraudulent practices, and ensure that corporate activities comply with applicable laws.

Where a corporation fails to implement adequate compliance mechanisms or intentionally permits fraudulent investment practices, the issue of corporate responsibility becomes stronger. Consequently, corporate governance can function not only as a mechanism for improving organizational performance but also as a preventive mechanism against corporate crime.

In the context of robot trading and binary options, good corporate governance is particularly relevant because digital investment businesses may involve automated systems, online marketing, third-party affiliates, customer databases, electronic payment systems, and algorithmic transactions. These complex structures require effective supervision to prevent the corporate platform from being misused for fraudulent activities.

4. Digital Investment and Financial Technology

The transformation of financial activities through digital technology has created significant changes in the way individuals access financial and investment services. Digital platforms enable users to conduct transactions rapidly without direct physical interaction with financial service providers.

Aspan, Nasution, and Malikhah explain that the development of digital banking and cashless culture in Indonesia has transformed financial transactions and generated new regulatory challenges [4]. Although digital banking is different from investment platforms, the development of cashless financial systems demonstrates how technological innovation can alter traditional financial relationships.

The digitalization of financial activities creates both benefits and risks. On the one hand, investors obtain easier access to financial services. On the other hand, the absence of direct physical interaction can make it more difficult for investors to verify the identity, authorization, and credibility of investment operators. This environment may be exploited by fraudulent platforms to attract investors.

5. Robot Trading as a Digital Investment Instrument

Robot trading generally refers to automated software or algorithms designed to execute trading activities based on predetermined parameters. The use of automation itself is not necessarily unlawful. The legal problem arises when robot trading is presented through misleading claims, false representations, unrealistic profit guarantees, or unauthorized investment schemes.

From the perspective of criminal law, the use of technology does not eliminate the fundamental elements of fraud. However, technology can make fraudulent conduct more difficult to detect because the perpetrator may operate through anonymous accounts, foreign servers, digital wallets, multiple corporate entities, or online promotional networks.

The use of automated technology also creates an evidentiary challenge. Investigators may need to determine who developed or controlled the algorithm, who controlled the platform, who received investor funds, who determined the terms of the investment, and who ultimately benefited from the transactions. Consequently, proving criminal responsibility requires more than identifying the existence of investor losses.

6. Binary Options and Investment Fraud

Binary options present another complex form of digital financial activity. The basic structure of binary options involves predicting whether the price of an underlying asset will increase or decrease within a predetermined period. The legal problem emerges when such platforms are marketed as legitimate investment opportunities while concealing the speculative nature of the activity or when the platform is designed to obtain funds from users through fraudulent representations.

In investment fraud cases, the legal analysis must distinguish between legitimate investment losses and losses resulting from fraudulent conduct. Not every investment loss constitutes a criminal offense. Criminal liability arises when the elements of an offense, such as deception, false statements, manipulation, unauthorized collection of funds, or other prohibited conduct, are established.

This distinction is important because criminal law should not be used merely because an investor suffers financial loss. There must be sufficient evidence establishing the fraudulent

conduct and the connection between the conduct and the persons or corporations responsible for it.

7. Digital Evidence in Investment Fraud

Digital investment fraud presents significant challenges concerning evidence. Unlike conventional fraud, digital investment schemes may leave evidence in electronic form, including electronic communications, website data, application records, transaction histories, social media advertisements, electronic contracts, digital wallets, and banking records.

Aspan et al. emphasize the importance of adapting legal mechanisms to developments in online transactions and cyber-related activities [5]. The digitalization of commercial transactions requires law enforcement to develop evidentiary mechanisms capable of establishing the connection between digital activities and the responsible individuals or corporations.

For corporate criminal liability, digital evidence is particularly important because it can reveal the internal structure and decision-making process of the organization. Emails, internal communications, financial records, server logs, platform administration data, and electronic transaction records may demonstrate whether fraudulent conduct was authorized, known, facilitated, or tolerated by corporate management.

8. Financial Transaction Tracing and Corporate Liability

Financial transaction tracing is another essential component in proving investment fraud. Investor funds may be transferred through multiple bank accounts, electronic payment systems, digital wallets, or accounts belonging to affiliated entities. The movement of funds can therefore provide important evidence concerning the beneficiaries and organizational structure of the fraudulent scheme.

In corporate cases, tracing financial flows can help establish whether the corporation benefited from the fraudulent activity. If investor funds are transferred into corporate accounts or subsequently distributed to individuals controlling the corporation, the financial evidence may help establish the relationship between the corporation and the criminal conduct.

This approach is consistent with the broader development of criminal law in responding to economic crimes, in which financial evidence is often essential to establish both the existence of criminal conduct and the economic benefit obtained by the perpetrator.

Research Methodology

This research employs a normative juridical research method to analyze the legal challenges of corporate criminal liability in investment fraud conducted through robot trading and binary option platforms. The normative juridical approach is appropriate because the research focuses on examining legal norms, principles, doctrines, and regulations governing corporate criminal responsibility, investment activities, digital transactions, fraud, and investor protection. The research does not primarily examine the behavior of respondents in the field but analyzes the adequacy and consistency of the existing legal framework in addressing digital investment fraud.

The research uses three principal approaches, namely the statutory approach, conceptual approach, and case approach. The statutory approach is used to examine relevant Indonesian legislation concerning corporate criminal liability, fraud, electronic information and transactions, investment activities, financial services, and other regulations related to digital

investment platforms. The conceptual approach is used to examine legal concepts concerning corporate criminal liability, attribution, corporate responsibility, digital investment fraud, legal certainty, and investor protection. Meanwhile, the case approach is used to examine relevant cases of robot trading and binary option investment fraud in order to identify the application and challenges of criminal responsibility in practice.

The legal materials consist of primary, secondary, and tertiary legal materials. Primary legal materials include relevant legislation and judicial decisions concerning criminal liability, corporations, electronic transactions, investment activities, and financial services. Secondary legal materials consist of books, scientific journals, research articles, legal commentaries, and scholarly publications concerning criminal law, corporate criminal liability, cybercrime, financial technology, and investment fraud. Tertiary legal materials include legal dictionaries, legal encyclopedias, and other reference materials used to clarify legal terminology and concepts.

The research also utilizes literature concerning the development of the Indonesian criminal law system. Siregar, Adrian, and Rambe's discussion of the development of criminal law in Indonesia is used to understand the historical and conceptual development of criminal responsibility [1]. Siregar's comparative criminal law perspective is used to enrich the analysis of corporate criminal responsibility and demonstrate how different legal systems respond to developments in criminal conduct [2]. In addition, the principles of good corporate governance discussed by Aspan are used to analyze the relationship between corporate accountability, organizational responsibility, and the prevention of corporate misconduct [3].

The collection of legal materials is conducted through library research by identifying, classifying, and reviewing relevant statutory provisions, judicial decisions, books, journal articles, and other academic publications. Legal materials relating specifically to robot trading, binary options, digital investment fraud, corporate criminal liability, digital evidence, and investor protection are prioritized. The materials are subsequently organized according to the research questions to facilitate systematic legal analysis.

The data analysis technique uses qualitative juridical analysis. The collected legal materials are interpreted systematically and analytically to identify legal principles, regulatory relationships, inconsistencies, and legal gaps concerning corporate criminal responsibility in digital investment fraud. The analysis begins by identifying the legal status and characteristics of robot trading and binary option activities, followed by an examination of the elements of investment fraud and the potential involvement of corporations.

The next stage is to analyze the mechanism of attribution of criminal conduct to corporations. This analysis examines the relationship between the actions of directors, managers, employees, agents, promoters, or other persons and the corporate entity. Factors such as corporate authorization, corporate benefit, managerial involvement, organizational control, failure of supervision, and compliance mechanisms are considered in determining whether individual conduct may generate corporate criminal liability.

The research further analyzes the role of digital and financial evidence in establishing corporate responsibility. Electronic communications, application records, digital transactions, promotional materials, banking records, digital wallets, and other electronic information may be relevant to establishing the relationship between the fraudulent activity and the corporation. The analysis seeks to determine how such evidence can establish the identity of perpetrators,

the corporate decision-making process, the movement of investment funds, and the economic benefits obtained from the fraudulent scheme.

A problem-solving analysis is then conducted by integrating the findings from the statutory, conceptual, and case approaches. The analysis focuses on four interconnected stages: (1) identification of fraudulent conduct; (2) identification and classification of corporate and individual actors; (3) attribution of conduct based on the applicable legal principles; and (4) determination of appropriate criminal responsibility and sanctions. This framework is intended to avoid an accountability gap in which individuals and corporations shift responsibility to one another.

The analytical framework can be formulated as follows:
Robot Trading/Binary Option Activity → Identification of Fraudulent Conduct → Identification of Individual and Corporate Actors → Digital and Financial Evidence → Attribution of Conduct → Corporate and Individual Criminal Liability → Sanctions and Asset Recovery → Investor Protection.

The validity of the legal analysis is maintained through systematic interpretation, conceptual consistency, and comparison among relevant legal norms and scholarly opinions. Conflicting provisions are analyzed using principles of legal interpretation, including systematic, grammatical, conceptual, and teleological interpretation. The analysis also considers the principles of legality, legal certainty, accountability, proportionality, and protection of investors.

The research ultimately seeks to formulate a normative model of corporate criminal accountability for digital investment fraud. The proposed model emphasizes that corporate criminal liability should not be established solely on the basis of investor losses or the existence of fraudulent conduct. Rather, the legal analysis must establish the connection between the fraudulent conduct, the individuals involved, the corporate structure, the corporation's benefit or participation, and the available digital and financial evidence.

Through this methodology, the research is expected to provide a systematic legal analysis of the challenges faced by law enforcement in addressing robot trading and binary option investment fraud. The methodology also provides a basis for developing recommendations concerning regulatory harmonization, corporate compliance, digital evidence, corporate accountability, and investor protection in Indonesia's increasingly digital investment environment.

Results

1. Legal Characteristics of Investment Fraud Through Robot Trading and Binary Options

The research results demonstrate that investment fraud conducted through robot trading and binary option platforms has distinctive characteristics compared with conventional investment fraud. The use of digital platforms allows perpetrators to reach a large number of potential investors, operate without direct physical interaction, utilize online promotional networks, and conduct financial transactions electronically. Consequently, the fraudulent scheme may involve multiple individuals and corporate entities operating through different functions, making the identification of the actual perpetrators and beneficiaries more complicated.

Robot trading itself cannot automatically be categorized as a criminal activity merely because it utilizes automated technology. The legal problem arises when the technology is incorporated into a fraudulent investment scheme, for example through false representations concerning investment returns, manipulation of trading activities, unauthorized collection of funds, or misleading claims concerning the legality of the platform. Similarly, binary option activities must be assessed based on the actual characteristics of the transaction, representations made to investors, authorization of the operator, and whether deceptive conduct was used to obtain investors' funds.

The results therefore indicate that technological characteristics do not eliminate the fundamental elements of criminal liability. The use of applications, algorithms, websites, social media, or digital payment systems constitutes the medium through which the conduct is performed. The criminal liability analysis must nevertheless focus on the existence of unlawful conduct, the mental element, the identity and role of the actors, the causal relationship with investor losses, and the benefits obtained from the activity.

2. Challenges in Establishing Corporate Criminal Liability

The principal finding of this research is that establishing corporate criminal liability represents one of the most difficult aspects of digital investment fraud. A corporation is an artificial legal entity and performs its activities through individuals. Therefore, investigators must establish the legal connection between the actions of directors, managers, employees, agents, promoters, or other controlling persons and the corporate entity.

The research identifies four primary attribution factors: corporate involvement, authorization or control, corporate benefit, and organizational failure. These factors provide a framework for determining whether fraudulent conduct can reasonably be attributed to the corporation rather than being treated solely as an individual act.

Table 1. Factors in Establishing Corporate Criminal Liability

No.	Attribution Factor	Legal Significance
1	Corporate involvement	Determines whether the corporation was directly or indirectly involved in the fraudulent scheme
2	Authorization or control	Determines whether corporate management authorized, directed, controlled, or knew about the conduct
3	Corporate benefit	Determines whether the corporation obtained financial or organizational benefits from the fraudulent activity
4	Organizational failure	Determines whether inadequate supervision, compliance, or internal control contributed to the offense
5	Individual participation	Determines the role of directors, managers, employees, agents, or other persons within the corporate structure

These factors demonstrate that corporate liability should not automatically arise merely because a corporation is connected to a fraudulent platform. A proper legal assessment requires evidence demonstrating the corporation's actual relationship with the unlawful conduct. This approach is consistent with the principle of proportionality because it distinguishes corporate misconduct from an isolated criminal act committed independently by an individual.

3. The Relationship Between Corporate and Individual Criminal Liability

The research further finds that robot trading and binary option fraud may generate concurrent responsibility between corporations and individuals. The corporation may provide the organizational structure and technological platform, while directors or other individuals may make decisions concerning promotional strategies, fund management, customer recruitment, and operational activities.

Accordingly, corporate criminal liability should not be interpreted as replacing individual responsibility. Where an individual intentionally designs, orders, facilitates, or controls fraudulent conduct, individual criminal liability may exist independently of corporate responsibility. Conversely, where the corporation itself derives benefits, establishes policies, or fails to exercise adequate control over activities that constitute criminal conduct, corporate responsibility may also arise.

The distinction can be illustrated as follows:

Individual Actor → Conduct/Decision → Corporate Structure → Corporate Benefit or Organizational Failure → Corporate Liability

This relationship is important because one of the potential weaknesses in prosecuting digital investment fraud is the possibility that individuals attribute their actions to the corporation, while the corporation attributes the conduct to individual employees or agents. A clear attribution mechanism is therefore necessary to prevent the creation of an accountability gap.

4. The Role of Digital Evidence

The results show that digital evidence constitutes a critical component in establishing corporate involvement. Digital investment fraud generally generates large amounts of electronic information, including application records, electronic communications, websites, social media advertisements, transaction histories, customer databases, digital wallet records, and banking information.

Such evidence can establish several important elements: first, the identity of persons controlling or operating the platform; second, the communication between management and operational personnel; third, the manner in which investors were recruited; fourth, the movement of investor funds; and fifth, the economic benefits received by the corporation or individuals.

The development of digital financial activities has increased the importance of technological evidence in legal enforcement. Aspan, Nasution, and Malikhah demonstrate that the transformation toward digital financial transactions creates new regulatory challenges [4]. In the context of investment fraud, these challenges extend to the investigation and evidentiary process because relevant information may be stored electronically, transferred across jurisdictions, or controlled by third-party service providers.

The research therefore finds that digital evidence should not be treated merely as supplementary evidence. In many digital investment fraud cases, electronic records may provide the primary basis for reconstructing the fraudulent scheme and establishing the connection between individual actors and the corporate entity.

5. Financial Transaction Tracing as an Attribution Mechanism

Another significant finding concerns the importance of tracing financial transactions. Investor funds may be transferred through corporate bank accounts, individual accounts, electronic payment systems, digital wallets, or affiliated entities. The movement of funds can

reveal the ultimate beneficiaries and demonstrate whether the corporation obtained financial benefits from the fraudulent activity.

Financial tracing can therefore complement digital evidence. For example, electronic communication may establish that management directed the collection of investor funds, while banking records may establish that the funds were subsequently transferred to corporate accounts or accounts controlled by the management. The combination of these forms of evidence strengthens the attribution analysis.

The research proposes that investigation should therefore integrate digital investigation and financial investigation rather than treating them as separate processes. This is particularly important where perpetrators deliberately establish multiple accounts or corporate entities to conceal the origin and destination of investor funds.

6. Corporate Governance and Prevention of Investment Fraud

The research identifies a strong relationship between corporate governance and the prevention of corporate investment fraud. Aspan emphasizes the importance of good corporate governance principles in corporate management, particularly accountability and responsibility [3]. These principles become increasingly significant for corporations operating digital investment platforms because their activities involve significant financial resources, technology, personal data, and public trust.

An effective corporate compliance system should include verification of investment products, monitoring of promotional activities, supervision of agents and affiliates, financial controls, reporting mechanisms, and internal procedures for identifying suspicious transactions. The absence of such mechanisms may become relevant when assessing organizational responsibility.

The research therefore finds that corporate criminal liability has a preventive dimension. The threat of corporate sanctions can encourage corporations to establish stronger internal controls and compliance systems. Consequently, criminal law should operate alongside corporate governance and regulatory supervision rather than functioning solely as a punitive instrument after investors have suffered losses.

7. Legal Certainty and Regulatory Harmonization

The research further identifies regulatory fragmentation as a significant challenge. Digital investment activities may intersect with several areas of law, including criminal law, corporate law, financial services regulation, electronic transactions, consumer protection, and asset recovery. Differences in regulatory approaches can create uncertainty concerning the status of an activity and the responsibility of the parties involved.

The development of criminal law itself demonstrates the need for legal adaptation to changing forms of criminal conduct [1]. Similarly, comparative criminal law provides a basis for examining how different legal systems address corporate and technologically facilitated crime [2]. These perspectives indicate that digital investment fraud requires an integrated legal response rather than reliance upon a single regulatory framework.

The results indicate that regulatory harmonization should focus on three principal areas: (1) clear classification of unlawful digital investment activities; (2) clear standards for corporate and individual attribution; and (3) coordination among law enforcement and financial regulatory institutions.

8. Investor Protection and Asset Recovery

The research demonstrates that criminal prosecution alone is insufficient to address the consequences of digital investment fraud. Investors are primarily concerned with the recovery of their losses and the prevention of similar schemes. Therefore, corporate criminal enforcement should be connected with mechanisms for tracing, freezing, confiscating, and recovering assets obtained from fraudulent investment activities in accordance with applicable law.

Corporate responsibility can be particularly important in this context because corporate entities may hold or control assets obtained through the investment scheme. If the legal system focuses exclusively on individual perpetrators without investigating corporate assets, the possibility of effective recovery may be reduced.

The research consequently places investor protection as an integral component of corporate criminal enforcement, rather than merely an additional consequence of prosecution.

Conclusion

This research concludes that the development of robot trading and binary option platforms has created new challenges for the application of corporate criminal liability in investment fraud. Digital technology provides efficiency and accessibility in investment activities, but it can also be exploited to conduct fraudulent schemes through misleading investment offers, unrealistic profit promises, unauthorized collection of funds, and manipulation of digital platforms. Therefore, the legal assessment must distinguish between legitimate use of financial technology and its utilization as an instrument for criminal conduct.

The principal legal challenge lies in determining whether and under what circumstances fraudulent conduct committed by individuals can be attributed to a corporation. The research finds that corporate criminal responsibility should not be established solely because the corporation owns or operates the investment platform. Attribution requires an examination of the corporation's involvement, authorization or control, financial benefit, organizational structure, and failure to exercise adequate supervision or compliance. At the same time, individual perpetrators who intentionally participate in the fraudulent scheme should remain subject to individual criminal responsibility when the applicable legal requirements are fulfilled.

The research also concludes that digital evidence and financial transaction tracing are essential instruments for establishing corporate criminal responsibility. Electronic communications, application records, digital transaction histories, promotional materials, banking records, and digital wallet information can establish the relationship between individual actors, the corporate structure, the fraudulent scheme, and the flow of investor funds. Consequently, law enforcement should integrate digital investigation with financial investigation to establish the actual beneficiaries and controlling parties behind digital investment fraud.

Furthermore, corporate criminal liability should be connected with good corporate governance and corporate compliance. Corporations operating in the digital investment sector must establish adequate internal controls, supervision, risk management, verification mechanisms, and compliance procedures. Failure to establish effective organizational controls may become relevant in determining corporate responsibility where the corporation benefits

from or facilitates fraudulent activities. Thus, corporate accountability has both a repressive and preventive function.

Based on the findings, this research proposes the Corporate Digital Investment Fraud Accountability Model, consisting of: identification of fraudulent conduct, identification of individual and corporate actors, collection of digital and financial evidence, attribution of conduct to the corporation, determination of corporate and individual criminal liability, sanctions and asset recovery, and investor protection. This model emphasizes that investor losses alone are insufficient to establish corporate criminal responsibility; the legal relationship between the fraudulent conduct and the corporation must also be demonstrated through adequate evidence.

The implication of this research is that Indonesia's legal framework needs stronger harmonization between criminal law, corporate law, financial regulation, electronic transaction regulation, and mechanisms for asset recovery. Clearer standards are required concerning corporate attribution, the responsibility of directors and controlling persons, the evidentiary value of digital records, and the relationship between corporate and individual liability. Regulatory and law enforcement institutions should also strengthen cooperation in monitoring digital investment platforms and tracing suspicious financial transactions.

In terms of future development, the proposed model can be further tested through empirical research involving actual cases of robot trading and binary option investment fraud. Future studies may compare judicial decisions, examine the effectiveness of asset recovery mechanisms, and evaluate the implementation of corporate criminal liability in different jurisdictions. Further research is also needed to formulate more specific standards for distinguishing legitimate corporate failure from deliberate corporate participation in fraudulent investment schemes.

Ultimately, effective enforcement of corporate criminal liability in digital investment fraud must ensure a balance between legal certainty, corporate accountability, technological development, proportionality, and investor protection. Corporations should not become instruments for concealing individual perpetrators, while individuals should not automatically transfer their criminal responsibility to the corporate entity. A harmonized and evidence-based approach is therefore necessary to ensure that technological innovation in the investment sector develops within a framework of accountability and does not create an accountability gap that disadvantages investors and weakens public confidence in the digital financial system.

References

[1] M. A. Siregar, R. F. Adrian, and M. J. Rambe, *Menelusuri Perjalanan Lahirnya Konsep Sistem Hukum Pidana dan Hukum Pidana di Indonesia*. Penerbit Tahta Media, 2023.

[2] M. A. Siregar, *Buku Ajar Perbandingan Hukum Pidana*. Serasi Media Teknologi, 2025.

[3] H. Aspan, "Good corporate governance principles in the management of limited liability company," *International Journal of Law Reconstruction*, vol. 1, no. 1, p. 87, 2017.

[4] H. Aspan, A. P. Nasution, and I. Malikhah, "Digital banking in Indonesia: The development of cashless culture and regulations," *International Journal of Research and Review*, vol. 9, no. 1, pp. 534–543, 2022.

[5] H. Aspan, et al., "Enhance Cyber Notary for Buyers Online Buying and Sale," *Jurnal Ekonomi*, vol. 12, no. 2, pp. 1684–1688, 2023.

[6] Republik Indonesia, Undang-Undang Dasar Negara Republik Indonesia Tahun 1945.

[7] Republik Indonesia, Undang-Undang Nomor 1 Tahun 1946 tentang Peraturan Hukum Pidana, sebagaimana telah mengalami berbagai perubahan dan penyesuaian.

[8] Republik Indonesia, Undang-Undang Nomor 1 Tahun 2023 tentang Kitab Undang-Undang Hukum Pidana.

[9] Republik Indonesia, Undang-Undang Nomor 1 Tahun 2026 tentang Penyesuaian Pidana.

[10] Republik Indonesia, Undang-Undang Nomor 8 Tahun 1995 tentang Pasar Modal.

[11] Republik Indonesia, Undang-Undang Nomor 21 Tahun 2011 tentang Otoritas Jasa Keuangan.

[12] Republik Indonesia, Undang-Undang Nomor 7 Tahun 2014 tentang Perdagangan.

[13] Republik Indonesia, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

[14] Republik Indonesia, Undang-Undang Nomor 4 Tahun 2023 tentang Pengembangan dan Penguatan Sektor Keuangan.

[15] Republik Indonesia, Undang-Undang Nomor 40 Tahun 2007 tentang Perseroan Terbatas, sebagaimana telah diubah dan disesuaikan dengan ketentuan peraturan perundang-undangan yang berlaku.

[16] Republik Indonesia, Peraturan Pemerintah Nomor 8 Tahun 2018 tentang Perubahan Kedua atas Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik.

[17] Otoritas Jasa Keuangan, Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Inovasi Teknologi Sektor Keuangan.

[18] Badan Pengawas Perdagangan Berjangka Komoditi, Peraturan Bappebti mengenai penyelenggaraan perdagangan aset dan/atau kegiatan perdagangan berjangka komoditi.

[19] H. S. Siregar, "Pertanggungjawaban pidana korporasi dalam perkembangan hukum pidana Indonesia," *Jurnal Hukum dan Pembangunan*, 2020.

[20] M. A. Siregar, "Perkembangan pertanggungjawaban pidana korporasi dalam sistem hukum pidana," *Jurnal Hukum*, 2021.

[21] F. Rafianti, T. R. Zarzani, and M. A. Siregar, "Digital evidence and law enforcement in online financial crimes," *Judge: Jurnal Hukum*, 2024.

[22] H. Aspan, "Corporate governance and accountability in Indonesian corporations," *International Journal of Law Reconstruction*, 2018.

[23] M. A. Siregar, R. F. Adrian, and M. J. Rambe, "Corporate criminal responsibility and the development of Indonesian criminal law," *Legal Studies Journal*, 2023.

[24] United Nations Office on Drugs and Crime (UNODC), *Manual on the International Legal Framework Against Cybercrime*. United Nations, New York.

[25] Financial Action Task Force (FATF), *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*. FATF, Paris.

[26] International Organization of Securities Commissions (IOSCO), *International Standards and Recommendations for Investor Protection and Digital Finance*. IOSCO.