International Journal of Innovative Research and Scientific Studies, 8(2) 2025, pages: 3387-3402

IJIRSS
International Journal of Innovative Research & Scientific Studies

ISSN: 2617-6548

URL: www.ijirss.com

Gravitating towards technology-based emerging financial crime: A PRISMA-based systematic review

Provakar Ghose[1], Munira Parvin[2], Sadia Akter[3], Shakib Hassan Rakib[4], Mohammad Rakibul Islam Bhuiyan[5*]

[1]*Pompea College of Business, University of New Haven, West Haven, Connecticut, United States.*
[2]*Department of Business Administration, East West University, Dhaka-1212, Dhaka, Bangladesh.*
[3]*Masters of Business Administration in Management Information Systems, International American University, Los Angeles, California, United States.*
[4]*Department of Finance and Banking, Begum Rokeya University, Rangpur, Bangladesh.*
[5]*Department of Management Information Systems, Begum Rokeya University, Rangpur, Bangladesh.*

Corresponding author: Mohammad Rakibul Islam Bhuiyan (*Email: rakib@mis.brur.ac.bd*)

Abstract

This study explores the integration of emerging technologies into financial systems and their impact on financial crimes. The research aims to identify and categorize financial crimes, cyber breaches, and the role of digital evidence in financial technologies using the PRISMA technique. A systematic review was conducted, analyzing literature from multiple databases such as PubMed, Scopus, Web of Science, and Google Scholar, focusing on studies published between June 2021 and June 2023. Key terms, including "technology-based financial crime," "cybercrime," "financial fraud," and others, were incorporated to refine the search. After rigorous screening, 175 studies (150 papers and 25 reports) were selected for analysis. The study highlights the growing concern over the use of emerging technologies in facilitating financial crimes such as money laundering, tax evasion, and cyber fraud. It also examines the evolving nature of financial crimes due to technological advancements and the challenges of investigating and prosecuting such crimes. Further research is recommended to investigate the socio-economic factors influencing financial crime and to develop effective global collaboration mechanisms for addressing transnational financial offenses. This study contributes to a deeper understanding of how business entities and individuals handle financial misconduct in the digital era.

Keywords: Cyber breaches, digital evidence, emerging technology, financial crime, PRISMA, systematic review.

DOI: 10.53894/ijirss.v8i2.6014
Funding: This study received no specific financial support.
History: Received: 6 March 2025 / **Revised:** 4 April 2025 / **Accepted:** 7 April 2025 / **Published:** 8 April 2025

Competing Interests: The authors declare that they have no competing interests.
Authors' Contributions: All authors contributed equally to the conception and design of the study. All authors have read and agreed to the published version of the manuscript.
Transparency: The authors confirm that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.
Acknowledgement: Authors are also deeply grateful to Professor Dr. Md. Rakibul Hoque, for his valuable suggestions and recommendations from to maintain the quality publication.
Publisher: Innovative Research Publishing

1. Introduction

Financial crime continues to be a serious problem, with a value of one trillion dollars, and is a major danger for both the financial services industry (FSI) and society [1]. According to Ramesh [2], there has been substantial investment in the development of methods to identify, prevent, and discourage such crimes. Although organizations may be at different phases of technology adoption and have varying levels of interest and financial resources to undertake initiatives, all enterprises can get advantages from implementing technological solutions. Furthermore, the advantages of technology can be enhanced by fully embracing its utilization throughout the entire client lifecycle [2].

Romanosky [3] suggested that there is a possibility that the public's worries about the rising number of breaches and legal actions are exaggerated when considering the relatively small financial consequences for the affected firms. Public apprehensions regarding the escalating frequency of breaches and legal proceedings are at odds with our research findings, which indicate a comparatively lesser financial repercussion on companies affected by such incidents. McLeod and Dolezel [4] considered the report to be crucial to the healthcare industry as it highlights the potential dangers of healthcare data breaches, which include the exposure, corruption, or deletion of personal health information. The study utilized binary logistic regression to examine a model reflecting a data breach. The findings suggest that there are multiple factors related to exposure, security, and organization that are strongly linked to healthcare data breaches Bhuiyan et al. [5].

Blakely et al. [6] focused on data breaches, which are a specific form of cyber incident that can lead to the unauthorized disclosure of sensitive information. Cyber decision-makers rely on this information to adapt information security initiatives, guaranteeing they tackle pertinent risks and optimize the allocation of expenditures [7]. Additionally, it provides a comprehensive analysis of the existing cybersecurity reporting landscape and suggests modifications to the United States' national cyber policy to maximize advantages for both reporters and data consumers, Bhuiyan and Akter [8]. Fernandez De Arroyabe and Fernandez de Arroyabe [9] used the Cyber Security Breaches Survey data reveals that SMEs experience a diverse range of breaches, corroborating prior research findings. Furthermore, we have assessed the level of seriousness of breaches in small and medium-sized enterprises (SMEs) by considering the duration of disruption and associated expenses Poli et al. [10].

Ettredge et al. [11] found that organizations that disclose the presence of trade secrets are more likely to experience a breach compared to organizations that do not disclose this information. The strength of our results is more pronounced among younger enterprises, firms with a smaller workforce, and firms operating in industries with lower levels of concentration Akter et al. [12]. Hogan et al. [13] found that cyber breaches demonstrate temporal fluctuations as cybercriminals focus on particular firms, types of data, access points, and geographical areas. Following the announcement of cyber incidents, we witnessed considerable and rapid detrimental anomalous returns. Sectors that are targeted more frequently and suffer from attacks that expose personal financial data experience even greater negative returns [14].

Dolezel and McLeod [15] revealed that there are multiple connections between the nature of healthcare breaches and the data indicates that the number of people affected is higher in hacking/IT events and network server breaches, respectively. Additionally, the combination of the location of the network server breach and the type of unauthorized access or disclosure breach can be used to anticipate the impact. Rai and Mandoria [16] explored this text provides an introduction of cybercrime, including prevention strategies. It also delves into the most destructive cyber-attacks, the most notorious cyber criminals in history, and the countries with the highest rates of cybercrime and cyber breaches in the 21st century [17].

1.1. Research Gaps

Financial crime encompasses various crucial domains. Although detection technology has improved, there is a dearth of comprehensive studies on the long-term efficacy of preventing financial crimes [2]. Furthermore, there is a lack of thorough investigation of the convergence of financial criminal activities, specifically in relation to regulatory strategies and their effectiveness [1]. Further research is required to examine how socio-economic conditions, such as economic recessions or pandemics, affect the occurrence and characteristics of financial crimes. Insufficient study exists regarding the role of insider threats and the efficiency of internal controls in financial institutions [18]. Furthermore, there is a scarcity of research on global collaboration mechanisms and their efficacy in addressing transnational financial crimes [14]. It is crucial to address these deficiencies in order to create strong plans to fight financial crimes in a world that is becoming more digital and interconnected.

1.2. Research Objectives

The study was conducted to identify financial crimes and cyber breaches related to economic downturns and other socioeconomic factors. To be more specific, the objectives are subdivided into two categories.

ROI 1: To examine the criminal investigation and digital evidence in financial technologies.

ROI 2: To determine the categories of financial crimes through emerging technologies.

2. Literature Reviews

In their study, Abdullah and Said [19] investigated two main aspects. Firstly, an analysis was conducted on the attributes of the audit committee and its relationship with corporate financial crime in order to establish whether it still serves as an effective corporate governance mechanism. Secondly, their assessment focused on the efficacy of establishing a unique risk committee, apart from the audit committee, in mitigating corporate financial misconduct. The results indicated that there is little support for the influence of audit committee features. However, they do suggest a substantial correlation between the presence of a separate risk committee and instances of corporate financial crime. Multiple studies provide evidence of the

advantages of implementing a corporate governance structure that effectively deters fraudulent activities and deceptive behaviors [20].

In their study, Said et al. [21] provided a definition of corporate crime based on corporate governance and ethics, and examined the mechanisms via which such criminal activities take place [22]. Multiple studies provide evidence of the advantages of implementing a corporate governance framework that effectively safeguards against fraud and deceptive practices. According to Archambeault [23], audit committees in fraudulent organizations tend to have lower levels of financial literacy and less specific responsibilities outlined in their charters compared to audit committees in non-fraudulent companies. Furthermore, fraudulent companies are unlikely to uphold an impartial nomination committee. The study aimed to identify the internal control vulnerabilities of certain firms and compare them to the non-internal control deficiencies of other firms. In her conceptual work, Dion [24] conducted a study to determine the extent to which ethical relativism might be used to justify unethical practices. The study concluded that corruption should be regarded not only as a social construct and cultural occurrence, but also as a subject for ethical deliberation and moral evaluation [25].

2.1. Cyber Profile Attacks

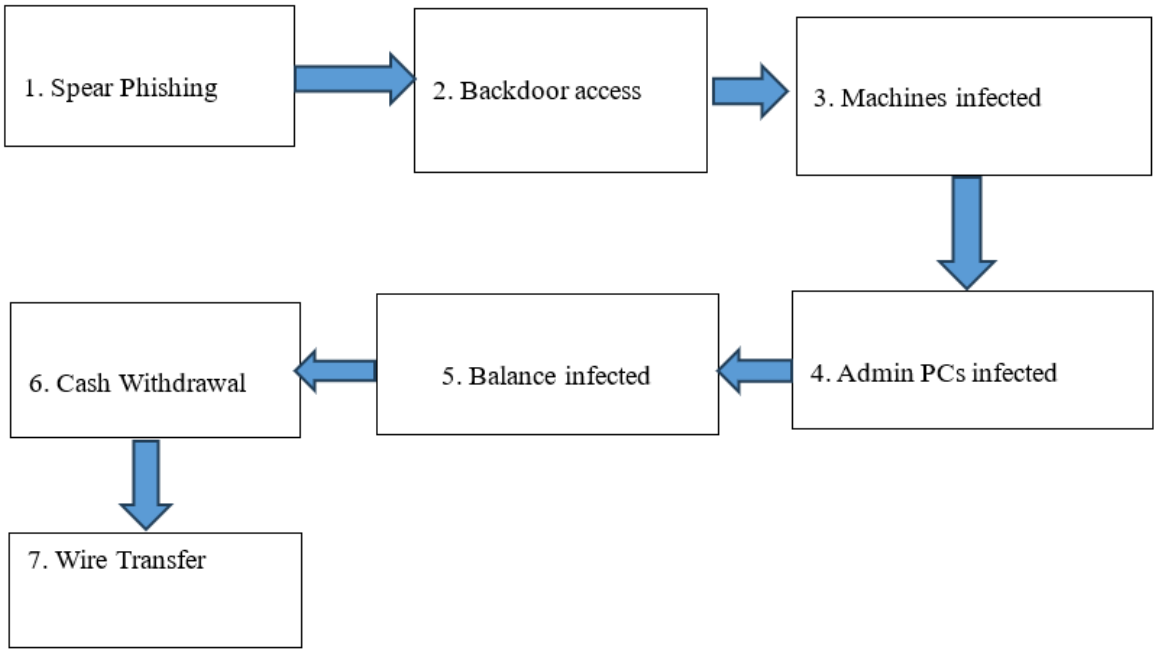

Figure 1.
Cyber Attack Lifecycle on Banking Systems.
Source: Hasham et al. [26].

Fraud and insider threats	Cyber breaches	Financial crimes
		
• Internal and external threats • Retail and non-retail threats • Insider threats • Market abuse and misbehavior	• Confidentiality • Integrity • Systems availability	• Money laundering • Bribery and corruption • Tax evasion and tax fraud

Figure 2.
Convergence of crimes.

2.2. Fraud and Insider Threats

The issue of insider threats is more elusive and complex compared to other types of threats. Evaluating the internal risk is the initial stage in gauging the probability of an insider assault [27]. Technical solutions are insufficient because insider threats are primarily a human problem. Hence, Sarkar [28] suggested a comprehensive strategy that includes evaluating technology, behavior, and organization to effectively anticipate and prevent insider threats. This approach enhances the security, ability to withstand challenges, and adaptability of the organization in the face of insider risks.

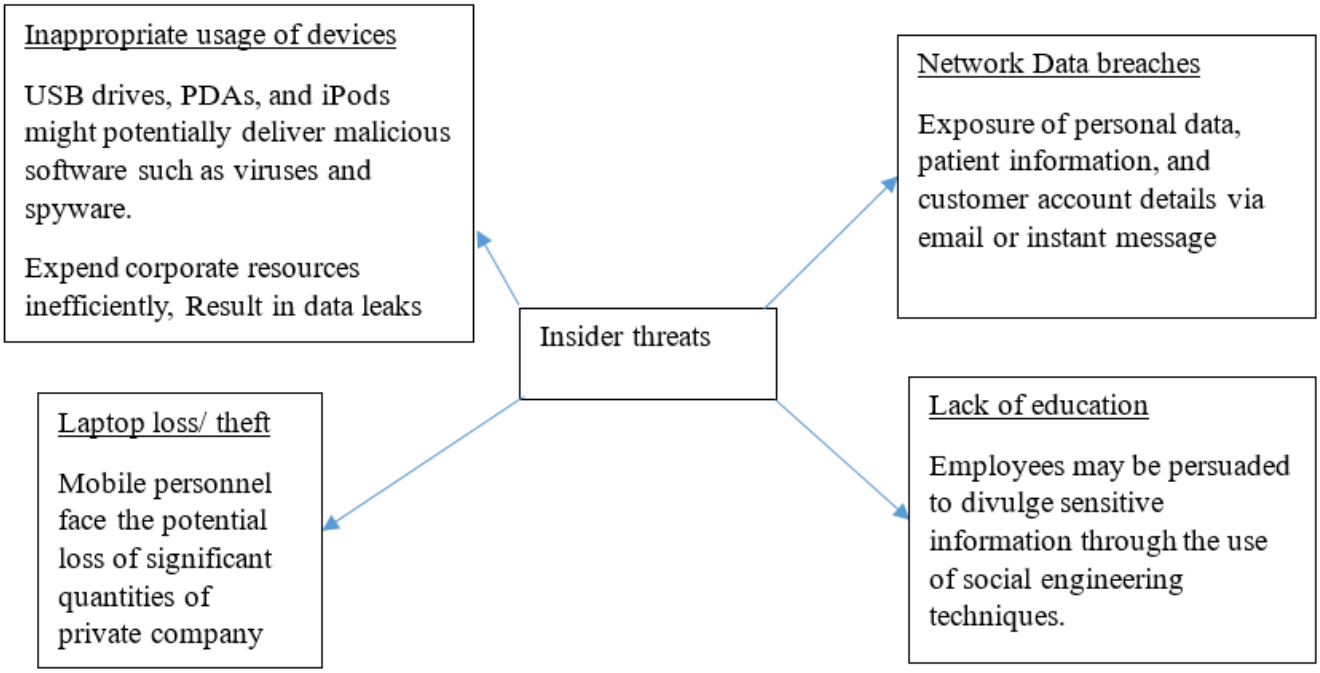

Figure 3.
Fraud and Insider threats.
Source: Sarkar [28]

According to Hasham et al. [26]. The mitigation of all risks related to financial crime entails three types of countermeasures: client identification and authentication, monitoring and detection of transaction and behavioral irregularities, and prompt response to minimize risks and address concerns. These operations, whether undertaken in reaction to instances of fraud, cybersecurity breaches, or attacks, or other forms of financial crimes, are facilitated by numerous analogous data and procedures [7].

In a study of Safa et al. [29] presented a novel theoretical framework to reduce the risk of insiders employing measures to discourage and prevent. Deterrence factors function as a deterrent to promote a culture that deters personnel from participating in information security misconduct within organizations; on the other hand, situational crime prevention elements serve as motivation for individuals to actively prevent instances of information security malfeasance. Our study findings demonstrate that the perceived certainty and severity of sanctions have a significant influence on individuals' views and function as a deterrent against engaging in information security breaches. Furthermore, the results indicated that escalating the level of exertion, peril, and diminishing the incentive (advantages of criminal activity) impact the employees' disposition towards averting information security misconduct [30].

The presence of insider threats is a significant obstacle in the realm of cyber security. The study conducted by Al-Mhiqani et al. [31] aims to achieve two main objectives. Firstly, to provide a better understanding of the insider threat by classifying it. Secondly, to present a novel classification system for insider threats that incorporates specific terminology. The paper introduces a hybrid classification system for insider threats that integrates multiple factors, including insider threat access, motive, indicators, types and behaviors, profile categorization, methods, and detection approaches [32].

Several businesses have implemented strategies to mitigate the danger of insider threats. The tactics have been categorized into hard and soft forms, depending on their likelihood to violate employees' personal boundaries. Jeong and Zo's [33] poll reveals that employees perceive the use of hard-form approaches as a privacy violation, which can result in a lack of moral responsibility for their actions and potentially lead to insider attacks. Hard-form practices might have a counterproductive impact that goes against their intended objective.

Yuan and Wu [34] first provided a concise overview of frequently utilized datasets for insider threats. Existing research indicates that deep learning models can improve the efficiency of identifying insider threats compared to conventional machine learning algorithms. Nevertheless, the utilization of deep learning to enhance the identification of insider threats is still constrained by various restrictions, including insufficient labeled data and susceptibility to adaptive attacks [35].

Elmrabit et al. [36] introduced an innovative method for anticipating the likelihood of harmful insider threats prior to a breach occurring. The paper introduces a novel paradigm for predicting insider threat risk, incorporating technical, organizational, and human element perspectives. Additionally, a Bayesian network is utilized to apply this framework. An

analysis is conducted to identify any potential insider threat risk by assessing the risk level projections for each authorized user within the organization. The proposed insider threat prediction algorithm outperformed the subjective assessments of security experts.

Insider threats pose a greater risk compared to external threats because insiders have access to their organization's assets. Alsowail and Al-Shehari [37] provided a comprehensive framework that encompasses all facets of the insider threat scenario, such as technical, psychological, behavioral, and cognitive elements. The methodology employs a multi-tiered strategy that encompasses pre-, in-, and post-countermeasures to effectively address insider threats. It takes into account several aspects that influence the duration of insiders' employment, from the moment they first join an organization to the moment they leave [38].

AlSlaiman et al. [39] propose a unique approach for detecting insider threats that utilizes a deep learning network consisting of Long Short-Term Memory (LSTM) units. The detection system employs sentiment analysis to categorize the users' actions and leverages gray encoding to preserve the temporal relationship between activities [40]. Gray encoding was tested for its ability to preserve the temporal linkages between activities using different data representations, including binary encoding (BE) and real-valued data without encoding (WE).

An insider threat is done by the person called an insider, an individual who has been granted or previously had official permission to access an organization's network, system, or data and deliberately or accidentally misuses that can compromise the confidentiality, integrity, or availability of the organization's information systems. Sarala et al. [41] deal with the prediction of insiders in an organization by monitoring their activity for malicious patterns of usage and adapting to the changing behavior of the user by removing the user's access rights on an asset accordingly, Islam et al. [17].

Daubner et al. [42] proposed that FR-ISSRM is a risk management methodology that focuses on identifying the forensic readiness requirements specifically for addressing insider threats. Once implemented, the standards aid in reliably identifying the culprit, determining the root cause, assessing the damage caused by the attack, and enhancing the overall security posture. The methodology is thereafter illustrated in three instances, encompassing common insider attacks.

Giddens et al. [43] suggest that Managers' judgments of malicious intent vary systematically based on the gender of the subordinate employee. In particular, managers view security misbehavior by males as much more malevolent compared to that by females. These data indicate that gender biases influence managers' perceptions of employee security conduct.

Subhani et al. [44] mentioned that in today's progressively digitized organizations, unscrupulous personnel present a substantial risk. Due to the global changes in the corporate environment, the issue of insider threats has emerged as a significant concern for the majority of firms. The insider danger has risen since 2019, primarily due to the extensive implementation of cloud computing and bring-your-own-device regulations for remote work [45].

2.3. Cyber Breaches

Cyriac and Sadath [46] presented that financial institutions could potentially employ MECA (Model to Encounter Cyber Attacks). MECA suggests implementing IDS, security patches, and big data analytics intelligently to address cyber issues in financial organizations. The primary objective of MECA is to equip universities with the necessary technological capabilities to effectively manage and respond to evolving cyber breaches. Additionally, MECA aims to provide comprehensive training to employees, enabling them to proficiently utilize intelligent applications in order to combat cyberattacks. Ultimately, MECA seeks to cultivate these personnel as the initial line of defense against such attacks. The report also examines the individuals involved in a cyberattack and the primary technologies utilized to achieve their goal.

Cybersecurity breaches (CSBs) receive significant attention in the media and have led to the implementation of new regulations. However, academic research lacks agreement on whether these breaches have a significant economic impact. The findings of Haislip et al. [47] showed that peers who have not experienced a security breach in their industry face a notable decrease in the value of their investments when a cybersecurity breach is announced. Additionally, these peers also have to pay higher fees for audits during the year of the breach. Insurers with significant exposure to cybersecurity risks also see a decline in the value of their investments. Another study of He et al. [48] investigated the level of innovation exhibited by enterprises after implementing a customer satisfaction benchmark (CSB) is a crucial factor in determining the growth and profitability of the firm. Upon analyzing documented breaches spanning from 2005 to 2014, we have found a 10% decline in research and development expenditures in the year following a CSB. Furthermore, the overall findings indicate that CSBs are linked to forthcoming strategic choices regarding innovation and investment at the corporate level, Bhuiyan and Akter [8].

Wang et al. [49] revealed The Nigerian cybercrime industry has transitioned from low-tech cyber-enabled offenses to high-tech, intricate breaches, encompassing viruses, worms, Trojan infections, electronic spam messages, and hacking. These are the three most commonly encountered types of breaches [50]. Banking professionals have gotten sufficient support and training in terms of cyber security standards. The absence of sophisticated technologies for preventing and mitigating cyber security breaches, coupled with inadequate adherence to statutory requirements, seems to be the main causes contributing to the diminished cyber security capacity in our selected institutions [38].

3. Methodology

Researchers have successfully developed a comprehensive search strategy in order to effectively identify relevant studies. This strategy is designed to ensure that all relevant information is gathered and analyzed in a systematic and thorough manner. By utilizing various databases, search terms, and inclusion/exclusion criteria, researchers are able to narrow down the pool of potential studies and focus on those that are most pertinent to their research question [32]. This rigorous approach helps to minimize bias and increase the validity and reliability of the findings. The development of a comprehensive Utilize

various databases such as PubMed, Scopus, Web of Science, and Google Scholar for the purpose of information retrieval and literature review [18].

The present work utilized the PRISMA criteria, which were specifically designed for the purpose of performing systematic reviews and meta-analyses of observational data. Researchers conducted a comprehensive search for primary articles released from June 2021 to June 2023, encompassing worldwide databases. Utilize keywords such as "technology-based financial crime," "cybercrime," "financial fraud," "individuals," "organizations," and their respective variations to enhance the specificity and relevance of your search. It is advisable to incorporate grey literature and unpublished studies in order to mitigate the potential impact of publication bias [51].

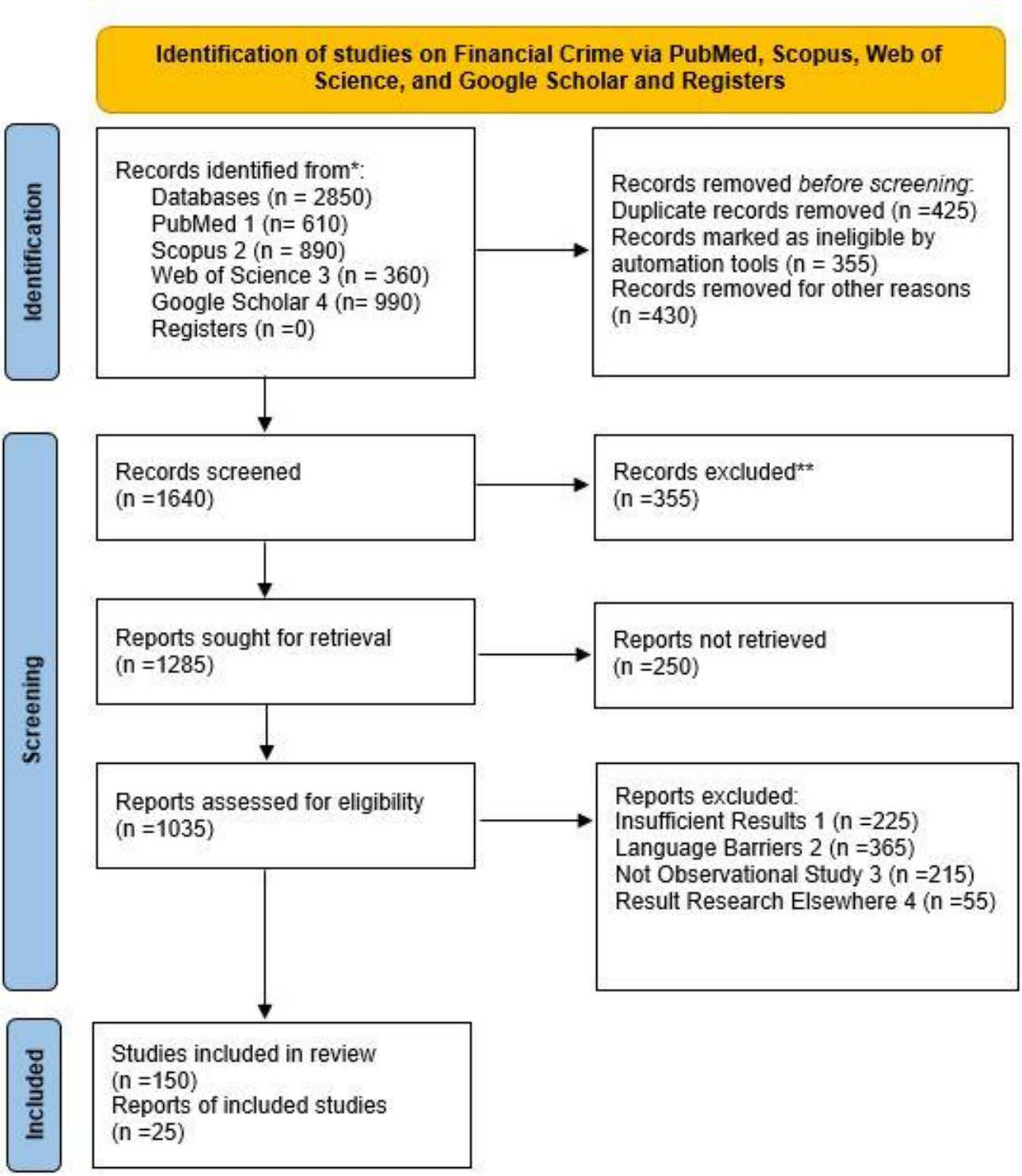

Figure 4.
PRIMA-Based Methodology.

Research investigations have been conducted to examine the occurrence of financial crimes that are facilitated by technology [14]. These crimes can involve both individuals and organizations as perpetrators. Various methodologies have been employed in these studies to gain a comprehensive understanding of the subject matter. The exclusion criteria for this

research study include the following: studies that are not directly related to financial crimes, studies that lack clear methodologies, and studies that are not in English.

The process of identifying, filtering, and including choices is carried out by categorizing them according to particular criteria and is represented in Figure 4. Any records that do not match the specified keywords or study subject are excluded. When deciding to reject articles and reports, several variables are considered, including insufficient data, papers written in different languages, varied outcomes, and unconnected effects and results [52]. A total of 175 studies, where 150 papers and 25 reports have been identified for inclusion in the research through the screening procedure.

While technological tools have made it easier to commit financial crimes, factors such as economic instability, corruption, and lack of regulatory oversight continue to play a significant role in enabling these crimes. Future studies should focus on understanding the intersection of socio-economic conditions and technological advancements, and how these elements together create an environment conducive to financial misconduct [52]. Additionally, the study advocates for global collaboration and the development of comprehensive international frameworks to address transnational financial crimes, which are increasingly facilitated by the anonymity and borderless nature of digital technologies.

4. Discussion

The discussion part described the PRISMA systematic review on technology-based financial crime affecting individuals and organizations, contributing to a comprehensive understanding of the existing literature in this important area. It included criminal investigation and digital evidence in financial technologies, research findings, and categories of financial crimes.

4.1. Financial Crime

Financial Crime refers to any illegal activity that involves the misuse or theft of financial assets, typically with the intention of gaining financial benefits or causing harm to others in the financial sector [52]. This can encompass a wide range of criminal activities, including fraud, money laundering, tax evasion, bribery, and corruption, which often involve the manipulation of financial systems, records, or institutions for illicit gain.

Financial crimes can occur in both the private and public sectors and can involve individuals, corporations, or even entire nations. Smith and Tiwari [53] documented this text discusses the possibility of national blockchain infrastructure to mitigate the financial crime concerns associated with digital currency and smart contracts. It emphasizes the necessity for governments to allocate resources towards the development of this infrastructure and the corresponding regulatory frameworks Khanom et al. [54]. Amara and Khlif [55] used based on a study of 120 nations, the authors discovered a strong correlation between the occurrence of financial crime and tax avoidance. When examining the moderating impact of corruption, they observe that the correlation between financial crime and tax evasion is particularly strong in highly corrupt settings [54].

Table-1.
Criminal Investigation and Digital Evidence in Financial Technologies.

Name	Explanation	Application	Source
Crypto and Virtual Currencies	Virtual currency is a subset of digital currency, while cryptocurrency is a subset of virtual currency. The central bank of a nation issues controlled digital currencies, which are convertible into sovereign currencies.	Cryptocurrencies serve as a very suitable means for aiding illicit activities such as money laundering, terrorism financing, and corruption. The current regulatory measures in the cryptocurrency business are insufficient.	Teichmann and Falker [56]
Online payment systems	Online payment systems refer to electronic systems that facilitate the transfer of funds over the Internet. They enable individuals and businesses to make and receive payments for goods and services digitally, without the need for physical cash or checks.	The characteristics of digital payment transactions, such as their instantaneous nature, absence of physical interaction, and capacity to cross national boundaries, create significant susceptibilities to financial crimes, including money laundering and the funding of terrorism. FinTech digital payments have been utilized as a method of online funding in multiple instances of terrorism financing.	Wiwoho, et al. [57]
Mobile Wallets	A digital wallet that securely holds payment card data on a mobile device, such as a smartphone or tablet. It allows users to make electronic transactions, both online and in physical stores, by using their mobile devices instead of carrying physical cards or cash.	The integration of smart card technology with mobile phones in smart wallets has the potential to enhance the risk of identity theft and financial crime, making them more attractive to thieves. Nevertheless, conducting market testing technology in Japan may not be appropriate for the purpose of crime prevention due to Japan's exceptionally low crime rate.	Whitehead and Farrell [58]
Rogue Mobile Banking Apps	These apps mimic legitimate mobile banking apps, but instead of	Two specific models are utilized, in addition to more conventional money	Custers, et al. [59]

	providing secure banking services, they capture examples of sensitive data that can be used for illegal purposes include login credentials, account numbers, and other personal information.	laundering techniques. The initial model entails the utilization of money mules and a rapid cash withdrawal. The second model highlights three primary methods of direct expenditure: online shopping for products, obtaining bitcoins through Bitcoin exchanges, or buying luxury goods directly.	
Traditional banking malware	A malicious software designed to target and exploit vulnerabilities in traditional banking systems and processes. The primary objective of this malware is to illicitly acquire confidential financial data, such as bank account particulars, login credentials, and credit card numbers, to facilitate unauthorized access to bank accounts and financial fraud.	Traditional banking malware is designed to steal consumer financial data. This encompasses sensitive data such as credit card numbers, bank account credentials, and personal identification information. this malware version has evolved and uses complex tactics to bypass security mechanisms and achieve its goals.	Custers, et al. [59]
Deepfake social engineering	The use of advanced artificial intelligence (AI) techniques to create highly realistic, synthetic media—such as video, audio, or images—that are used to deceive individuals or manipulate their behavior for malicious purposes. This form of social engineering exploits the realistic nature of DeepFakes to gain trust and trick targets into divulging sensitive information, transferring money, or taking other actions that benefit the attacker.	Deepfake detection systems are the most effective means of countering malevolent AI-generated media content. Through the implementation of deepfake identification, individuals and organizations can mitigate the dangers associated with misinformation, privacy infringements, and the potential manipulation of public sentiment.	Haislip, et al. [60]
PSD2 and bank APIs	PSD2 is the second European Payment Services Directive. This program aims to improve financial transaction client protection and company innovation. It offers merchants and fintechs attractive opportunities to enhance and simplify client solutions, but it also requires strict security requirements that we will detail in this summary.	A PSD2 banking API is a highly secure environment that can only be accessed by authorized parties and is regulated by a standardized set of rules and norms. The system translates requests made by the TPPs and executes a corresponding operation or provides a response.	Bhuiyan, et al. [61]
SWIFT infrastructure and other payment backbones	SWIFT handles most international money and security transfers. Financial institutions send and receive money transfer instructions swiftly, accurately, and securely using SWIFT, a massive messaging network.	SWIFT is an extensive communication network utilized by banks and other financial organizations to promptly, precisely, and securely exchange information, such as instructions for transferring money.	AIS [62]
Corporate payment applications	A payment method encompasses the diverse range of choices that customers have at their disposal to complete financial transactions while acquiring a product or service. Payment methods encompass a variety of options, whether one is shopping at a brick-and-mortar establishment or on the internet.	Corporate payment apps handle, secure, and streamline commercial financial transactions. Traditional banking malware poses concerns since these platforms handle enormous amounts of sensitive financial data and transactions.	Sabuj, et al. [63]

Peer-to-peer payment systems	A P2P (peer-to-peer) payment refers to a digital transaction where individuals can send funds directly to each other without involving a financial intermediary, such as a bank, by utilizing mobile apps or web platforms.	Peer-to-peer payments, often known as P2P payments, enable the direct transfer of funds from one individual to another. P2P payment platforms, such as Venmo, PayPal, and Cash App, facilitate the transfer of funds between users using their mobile devices by connecting to their bank accounts or cards.	Hansen [64]
Credit card theft	Credit card theft refers to the unauthorized acquisition and use of someone else's credit card information to make fraudulent transactions or withdraw funds.	Identity theft is a very uncomplicated offense, but if left unaddressed, it can result in several criminal activities that have the potential to impact both individuals and corporations. Furthermore, when these criminal activities have an effect on corporations, they might indeed impede the whole economy.	Gupta and Kumar [65]
Payment card hardware attacks	Payment card hardware attacks are unauthorized and harmful operations attacking payment card hardware. These attacks aim to steal, manipulate, or misuse credit card data during valid POS, ATM, or other terminal transactions.	Emphasizes the undeniable connection between credit card forgery and many types of advanced criminal activities, which frequently overlap and present a significant challenge to the justice system and societal security.	Gottschalk [66]
Investigative honeypots	This computer system is fake to attract cyberattacks. It simulates a hacker target and leverages their infiltration efforts to learn about cybercriminals and their operations or divert them.	Production honeypots—decoy devices inside fully operational networks and servers—are commonly part of an intrusion detection system. They divert criminal attention from the real system while evaluating malicious activities to reduce vulnerabilities.	AIS [62]
Online money laundering	Money laundering is the act of disguising the source of unlawfully acquired funds by moving them through an intricate series of digital transactions in order to give the impression of legitimacy.	Money mules assist criminal syndicates in maintaining anonymity while transferring monies globally. Unemployment rates, teenage and juvenile engagement in internet usage, and involvement in money laundering crimes are increasing globally. Criminals are actively seeking out victims by taking advantage of their mental and financial vulnerabilities.	Raza, et al. [67]
Terrorism Financing	Terrorist financing entails the provision of financial resources to people and groups for the purpose of carrying out acts of terrorism. Terrorism funding bears similarities to money laundering, as it frequently necessitates criminals to clandestinely move funds through the normal financial system.	Like money laundering, terrorism financing often involves three stages: fundraising, transferring, and utilizing funds. Although terrorism financing may occur at various stages, the tactics employed are often comparable and, in certain instances, may even be indistinguishable from those utilized for money laundering.	Sabuj, et al. [63]

Hansen [64] investigated the perspective to aid in identifying remedies for the escalating ethical and societal problems of financial misconduct afflicting firms in the present day. The findings indicate that it is necessary to thoroughly analyze and make adjustments to the corporate structure, which includes closely examining official and informal communication and salary arrangements.

Nikkel [68] defined a new area of study under digital forensics that focuses specifically on financial technologies, often known as Fintech. The advent of the digital revolution is bringing about the emergence of innovative financial technology (Fintech) solutions for various financial activities such as payment processing, fund transfers, and various other financial transactions. Criminals are utilizing financial technologies to engage in deceptive activities, extortion, and money laundering, as well as to finance illicit operations in the criminal underworld. The study of Fintech and digital payment behavior should be acknowledged as a distinct technological topic within the digital forensics domain.

In their study, Dion [69] investigated the efficacy of Deferred Prosecution Agreements (DPAs) as a means to be within the jurisdiction of the criminal justice system cases of corporate misbehavior. This study examines the strengths and weaknesses of Deferred Prosecution Agreements (DPAs) by conducting detailed interviews with 24 legal practitioners and specialists in white-collar crime. It also suggests potential policy changes that could improve the implementation of DPAs. This study enhances the current body of literature by broadening the narratives employed by judicial authorities, the role of deferred prosecution agreements (DPAs) is a topic of interest among legal practitioners and scholars specializing in white-collar crime.

Gilsinan et al. [70] conducted a study on the involvement of the private sector in the regulation and enforcement of financial crime. They presented both empirical evidence and a theoretical framework to better comprehend the intricate conflicts that arise in this context. This research has identified five distinct roles that the private sector plays in combating financial crime. Each position has its own dynamics and repercussions, which are crucial for effectively suppressing illegal activities. The five characters consist of the reluctant informant, the zealous intelligence worker, the provocateur agent, the corrupt police officer, and the amiable officer. The role of the private sector is established by a careful calculation of rewards and penalties.

In his 2019 study, Dion [69] explored the capacity of Gadamer's [71] hermeneutic philosophy to reveal the correlation between corporate discourse on financial crimes, as articulated in codes of ethics, and the process of comprehension. Historically ingrained biases in three fundamental storytelling approaches (omission, selective focus, and thorough examination) about financial wrongdoing are linked to one's thinking, fundamental perspective on corporate self-interest, or a tendency to absolutize [63].

Abdullah and Said [72] examined the study examines the individual characteristics of directors and top management teams in connection to corporate governance and investigated how these features can influence the probability of corporate financial crime. The study suggests that the human governance component could be used as a potential strategy to enhance corporate governance and prevent such misconduct [73]. This chapter focuses on the personal traits of senior executives that can serve as indications of corporate financial crime. It also emphasizes the significance of human governance as a crucial method for preventing corporate financial crime within the framework of corporate governance [25].

Choi's study conducted in 2021 states that in order to attain justice through the examination of digital forensics, it is imperative to eliminate corporate offenses. This paper proposes numerous strategies to mitigate corporate crime, including the implementation of anti-forensic techniques, the utilization of cloud computing, and the establishment of a robust legal framework.

Table 2.
Summary of the Present Research Findings.

Main topics	The key to the main factor	Source
1. Anti-forensic Techniques	To summarize, the resolution of anti-forensic methods involves employing contemporary encryption software to safeguard data.	Islam et al. [17]
2. Cloud Computing Technique	It is imperative for digital forensic professionals to adopt contemporary cloud computing approaches to consolidate sensitive data into a cloud system.	Saha et al. [18]
3. Legal Frameworks and Guidelines	Utilization of a redundant storage system ensures regular monitoring of the cloud system.	AIS [62]
4. Data Collection	Creating software that ensures the protection of data during the process of gathering it. - Gathering a feasible amount of data	Islam et al. [20]
5. Change in technology	Adopting innovative technology, providing instruction on cutting-edge technology, and utilizing advanced software for the examination of confidential information	Sabuj et al. [63]

In their study, Baumann and Friehe [74] examined the correlation between the level of competition in the product market and the motivations of firms to engage in illicit practices as a means to reduce their production expenses. In pursuit of our objective, our framework integrates a crime model inspired by Becker with a Salop circle. When law enforcement incorporates a predetermined monetary penalty for unlawful behaviors, the presence of a larger number of firms in the industry leads to heightened competition, which in turn tends to decrease the occurrence of criminal activities [73]. However, when competition becomes more intense as a result of improved substitutability between products, the impact on crime rates may vary, potentially leading to an increase or decrease in criminal behavior.

4.2. Categories And Subcategories of Financial Crimes

In their study, Saha et al. [25] discovered that the issue of combating crypto fraudsters is a matter of significant concern for both developed and developing countries. Interestingly, this concern exists despite the absence of regulated guidelines that are uniformly implemented across these countries [8]. The focus of research has transitioned from studying malware, bitcoin, and blockchain to investigating crimes related to fintech, including money laundering, pump-and-dump operations, and phishing.

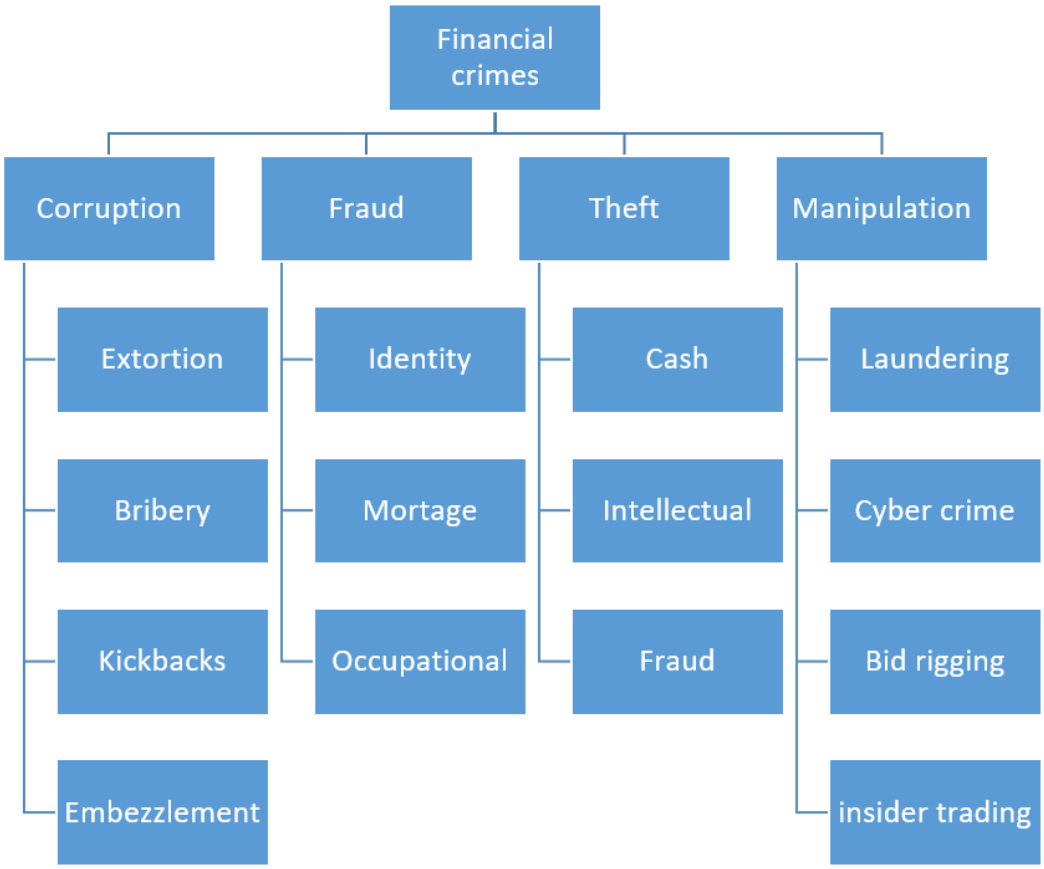

Figure 5.
Categories and subcategories of financial crimes.

Research observations indicate that various illicit activities, such as Instances of fraudulent initial coin offerings (ICOs), illicit money laundering activities, deceptive Ponzi schemes, malicious phishing attempts, underground darknet market transactions, harmful ransomware attacks, and manipulative pumps and dumps, are prevalent in the realm of cryptocurrency [8, 25]. These criminal activities can be attributed to several factors; the factors contributing to this phenomenon include investor overconfidence, speculative expectations, straightforward market access, decentralization, and anonymity. These elements contribute to a conducive environment for criminal behavior within the cryptocurrency ecosystem. This study proposes an investigation into the socioeconomic effects of cryptocurrencies, emphasizing the need for universally accepted regulations and advocating for the incorporation of interdisciplinary approaches in research [66].

5. Recommendations

1. Strengthening Digital Security and Fraud Detection: As the study highlights the increasing use of emerging technologies in facilitating financial crimes, one of the primary recommendations is for financial institutions to enhance their cybersecurity measures. This can be achieved by adopting advanced technologies such as blockchain for transparency, artificial intelligence (AI) for fraud detection, and machine learning (ML) algorithms to detect anomalous financial behaviors [51]. Financial institutions should also invest in training their staff on emerging digital threats, ensuring that they are well-equipped to respond to and prevent fraud effectively [75].
2. Developing Comprehensive Regulatory Frameworks: With the rapid evolution of financial technologies, the regulatory landscape must adapt to the new challenges posed by cybercrimes. Governments and financial regulators should collaborate to create comprehensive, globally accepted regulatory frameworks that address digital payment systems, cryptocurrency transactions, and online financial platforms. These frameworks should include stricter Know Your Customer (KYC) and Anti-Money Laundering (AML) regulations to combat money laundering, terrorism financing, and tax evasion that often occur in digital environments [51].
3. Promoting Collaboration Between Financial Institutions and Law Enforcement: The study emphasizes the importance of digital evidence in investigating financial crimes. As such, it is recommended that financial institutions, law enforcement agencies, and technology providers work more closely to share relevant information and tools. Public-private partnerships can enhance the detection and prosecution of financial crimes, as financial institutions can provide critical data and insights, while law enforcement can offer expertise in legal procedures and criminal investigations [75].
4. Fostering International Cooperation to Address Transnational Financial Crimes: The study underscores the cross-border nature of financial crimes, particularly in cases involving online fraud, cyber-attacks, and money laundering. Therefore, there is a strong need for greater international cooperation. Countries should establish global frameworks

for information sharing, joint investigations, and coordinated actions against transnational financial crimes. This includes creating multinational task forces that can track and prosecute criminals who operate across multiple jurisdictions.

6. Implications

1. **Impact on Financial Institutions**: Financial institutions must adopt proactive measures to combat emerging financial crimes. Failure to do so can result in significant financial losses, damage to reputation, and legal consequences. As criminals become more sophisticated, institutions need to stay ahead by leveraging cutting-edge technologies such as artificial intelligence, machine learning, and blockchain to detect and prevent fraud in real time. The findings imply that businesses must allocate more resources to cybersecurity and invest in continual staff training to manage risks effectively [22].
2. **Policy and Governance Implications**: The findings have significant implications for policymakers and regulators. As the financial landscape evolves, it is essential for governments to develop policies that support the secure integration of new technologies while also preventing their misuse. The lack of uniformity in regulations across borders makes it challenging to combat global financial crimes, making international collaboration a crucial aspect of the response. Policymakers must ensure that they balance innovation with security by developing adaptive regulatory frameworks that are flexible enough to keep pace with technological advancements [61].
3. **Implications for Digital Forensics**: The role of digital forensics is more important than ever, as financial crimes are increasingly dependent on digital platforms. This study underscores the importance of integrating digital forensics into financial crime investigations. Financial institutions and law enforcement agencies need to invest in forensics tools and expertise to analyze digital transactions and uncover illicit activities. Digital evidence, such as blockchain records, online payment histories, and mobile banking data, is pivotal in tracking and prosecuting offenders. The integration of these tools into the investigative process will enhance the ability to detect, investigate, and prosecute financial criminals [75].
4. **Implications for Global Economic Stability**: The rise of financial crimes driven by technological advancements has the potential to destabilize global economies. Money laundering, tax evasion, and other forms of financial misconduct can divert resources away from legitimate economic activities, leading to negative consequences for businesses and governments alike. The study implies that continued advancements in digital technologies should be accompanied by robust financial crime prevention measures to safeguard economic stability. Failure to address this issue could lead to an increase in financial crises, regulatory challenges, and a lack of public trust in financial systems [61].

7. Conclusions

This study aimed to investigate the prevalence of financial wrongdoing committed by businesses in Bangladesh. This study establishes rational choice theory and social learning theory as the conceptual frameworks for comprehending the underlying motivations of criminal activity, after conducting a comprehensive analysis of scams. While most participants, including academics, supported its use, a few respondents expressed concerns regarding the implementation of these agreements [61]. The majority of academic responses, as well as a few from legal practitioners, emphasized that there is an inherent bias in them and that they should be implemented with caution. According to some respondents, larger organizations have a higher chance of receiving it compared to smaller ones. This implies that it is merely another method of favoring the privileged class, enabling them to evade legal responsibility. Conversely, this study asserts that economic and political issues significantly influence criminal behavior. The volatile environment and political instability of the Bangladeshi economy have made financial operators extremely cautious and prone to taking risks [66]. Consequently, they resort to illicit activities in order to gamble with money and generate substantial gains. In addition to its major contribution to literature through the examination of financial crimes in Bangladesh with a theoretical explanation, this study also has certain drawbacks. Significantly, the study reports a low number of financial crimes, potentially impacting the interpretation of the results. Hence, investigating a broader and more varied range of financial offenses might be a viable avenue for future research. Furthermore, future studies should also examine the demographics of offenders.

8. Limitations of the Study

This study incorporates several restrictions. Firstly, this study lacks comprehensiveness and fails to adequately represent the larger population, thereby restricting its generalizability. This qualitative study contributes to the current literature, and its findings have broad applicability across various contexts. This comparison poses an additional limitation on the study because criminal justice practitioners operate in both state and federal jurisdictions. One additional obstacle in the present study, which is also anticipated to pose a challenge for future researchers, is the arduous task of obtaining access to specialists in a highly specialized area of criminal justice, such as federal prosecutors, officials from the Department of Justice, federal judges, and top-tier corporate defense attorneys. In the study, various challenges emerged, especially in the process of recruiting volunteers in order to obtain a sufficiently large sample size for conducting meaningful analysis [51]. As a consequence, the reduced sample size yielded comprehensive and detailed data that reached a point of saturation among the participants.

9. Future Direction

The current study highlights the necessity of conducting experimental investigations to assess the benefits and drawbacks of such agreements in financial crime. Future studies on the topic are difficult due to the absence of a centralized database that offers comprehensive information on it. The future study suggests that the ultimate conclusion about it is uncertain, as more than half of the criminal justice specialists involved in the study advocate for its continued and potentially increased use. Further research might explore the possible link between particular elements of an organization's history and the way in which it addresses instances of financial misbehavior in accordance with corporate ethical standards [61]. Subsequent investigations could aim to establish a historical correlation between certain clauses in the code of ethics and instances of financial misconduct, whether they originated within the business or the industry as a whole [75]. Subsequent research might investigate how the collective memory of an organization has shaped its understanding of significant instances of financial misconduct, based on past events and experiences inside the organization.

References

[1] N. Pardhey, "Financial systemic frauds in banking sector and money laundering cataclysm: Indian realism wits," 2021.

[2] P. N. Ramesh, "Data Visualization in Financial Crime Detection: Applications in Credit Card Fraud and Money Laundering," 2023.

[3] S. Romanosky, "Examining the costs and causes of cyber incidents," *Journal of Cybersecurity,* vol. 2, no. 2, pp. 121-135, 2016.

[4] A. McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," *Decision Support Systems,* vol. 108, pp. 57-68, 2018.

[5] M. R. I. Bhuiyan, M. W. Ullah, S. Ahmed, M. K. Bhuyan, T. Sultana, and A. Amin, "Information security for an information society for accessing secured information: A PRISMA based systematic review," *International Journal of Religion,* vol. 5, no. 11, pp. 932-946, 2024. https://doi.org/10.61707/frfnr583

[6] B. Blakely, J. Kurtenbach, and L. Nowak, "Exploring the information content of cyber breach reports and the relationship to internal controls," *International Journal of Accounting Information Systems,* vol. 46, p. 100568, 2022.

[7] S. Alam, M. R. I. Bhuiyan, S. Tabassum, and M. T. Islam, "Factors affecting users' intention to use social networking sites: A mediating role of social networking satisfaction," *Can. J. Bus. Inf. Stud,* vol. 4, no. 5, pp. 112-124, 2022. https://doi.org/10.34104/cjbis.022.01120124

[8] M. R. I. Bhuiyan and M. S. Akter, "Assessing the potential usages of blockchain to transform Smart Bangladesh: A PRISMA based systematic review," *Journal of Information Systems and Informatics,* vol. 6, no. 1, pp. 245-269, 2024.

[9] I. Fernandez De Arroyabe and J. C. Fernandez de Arroyabe, "The severity and effects of Cyber-breaches in SMEs: a machine learning approach," *Enterprise Information Systems,* vol. 17, no. 3, p. 1942997, 2023.

[10] T. Poli *et al.*, "Tourism And Climate Change: Mitigation And Adaptation Strategies In A Hospitality Industry In Bangladesh. Educational Administration: Theory and Practice, 30 (5), 7316-7330," ed, 2024.

[11] M. Ettredge, F. Guo, and Y. Li, "Trade secrets and cyber security breaches," *Journal of Accounting and Public Policy,* vol. 37, no. 6, pp. 564-585, 2018. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

[12] M. S. Akter, M. Bhuiyan, T. Poli, and R. Hossain, "Web-based banking services on E-customer satisfaction in private banking sectors: A cross-sectional study in developing economy," *Migration Letters,* vol. 20, no. S3, pp. 894-911, 2023.

[13] K. M. Hogan, G. T. Olson, J. D. Mills, and P. A. Zaleski, "An analysis of cyber breaches and effects on shareholder wealth," *International Journal of the Economics of Business,* vol. 30, no. 1, pp. 51-78, 2023.

[14] M. R. I. Bhuiyan, M. S. Akter, and S. Islam, "How does digital payment transform society as a cashless society? An empirical study in the developing economy," *Journal of Science and Technology Policy Management,* no. ahead-of-print, 2024.

[15] D. Dolezel and A. McLeod, "Cyber-analytics: identifying discriminants of data breaches," *Perspectives in health information management,* vol. 16, no. Summer, p. 1a, 2019.

[16] M. Rai and H. Mandoria, "A study on cyber crimes cyber criminals and major security breaches," *Int. Res. J. Eng. Technol,* vol. 6, no. 7, pp. 1-8, 2019.

[17] J. Islam, S. Saha, M. Hasan, A. Mahmud, and M. Jannat, "Cognitive modelling of bankruptcy risk: A comparative analysis of machine learning models to predict the bankruptcy," in *2024 12th International Symposium on Digital Forensics and Security (ISDFS)*, 2024: IEEE, pp. 1-6.

[18] S. Saha, P. C. Bishwas, U. Das, and A. S. Arshi, "Is fintech just an innovation? Impact, current practices, and policy implications of fintech disruptions," *International Journal of Economics, Business and Management Research,* vol. 8, no. 4, pp. 174-193, 2024.

[19] W. N. Abdullah and R. Said, "Audit and risk committee in financial crime prevention," *Journal of Financial Crime,* vol. 26, no. 1, pp. 223-234, 2019. https://doi.org/10.1108/JFC-11-2017-0116

[20] Z. Islam, M. R. I. Bhuiyan, T. A. Poli, R. Hossain, and L. Mani, "Gravitating towards internet of things: Prospective applications, challenges, and solutions of using IoT," *International Journal of Religion,* vol. 5, no. 2, pp. 436-451, 2024.

[21] R. Said, D. Crowther, and A. Amran, "Introduction: corporate crime and its constraint," in Ethics, governance and corporate crime: challenges and consequences: Emerald Group Publishing Limited, 2014, pp. 1-17.

[22] L. Mani, "An analysis of loan portfolio of Janata Bank Limited," *Available at SSRN 4644687,* 2019.

[23] D. S. Archambeault, *The relation between corporate governance strength and fraudulent financial reporting*. The University of Alabama, 2000.

[24] M. Dion, "Corruption and ethical relativism: what is at stake?," *Journal of financial crime,* vol. 17, no. 2, pp. 240-250, 2010.

[25] S. Saha, A. R. Hasan, A. Mahmud, N. Ahmed, N. Parvin, and H. Karmakar, "Cryptocurrency and financial crimes: A bibliometric analysis and future research agenda," *Multidisciplinary Reviews,* vol. 7, no. 8, pp. 2024168-2024168, 2024. https://doi.org/10.31893/multirev.2024168

[26] S. Hasham, S. Joshi, and D. Mikkelsen, "Financial crime and fraud in the age of cybersecurity," *McKinsey & Company,* vol. 2019, 2019.

[27] M. R. I. Bhuiyan, D. K. Uddin, and M. N. U. Milon, "Prospective Areas of Digital Economy: An Empirical Study in Bangladesh," *MDPI AG, Jul,* 2023.

[28] K. R. Sarkar, "Assessing insider threats to information security using technical, behavioural and organisational measures," *information security technical report,* vol. 15, no. 3, pp. 112-133, 2010.
[29] N. S. Safa *et al.*, "Deterrence and prevention-based model to mitigate information security insider threats in organisations," *Future Generation Computer Systems,* vol. 97, pp. 587-597, 2019.
[30] M. S. Akter, M. R. I. Bhuiyan, S. Tabassum, S. A. Alam, M. N. U. Milon, and M. R. Hoque, "Factors affecting continuance intention to use E-wallet among university students in Bangladesh," *International journal of engineering trends and technology,* vol. 71, no. 6, pp. 274-288, 2023. https://doi.org/10.14445/22315381/IJETT-V71I6P228
[31] M. N. Al-Mhiqani *et al.*, "A new taxonomy of insider threats: an initial step in understanding authorised attack," *International Journal of Information Systems and Management,* vol. 1, no. 4, pp. 343-359, 2018.
[32] C. Molla, L. Mani, M. R. I. Bhuiyan, and R. Hossain, "Examining the Potential Usages, Features, and Challenges of Using ChatGPT Technology: A PRISMA-Based Systematic," *Migration Letters,* vol. 20, no. S9, pp. 927-945, 2023.
[33] M. Jeong and H. Zo, "Preventing insider threats to enhance organizational security: The role of opportunity-reducing techniques," *Telematics and Informatics,* vol. 63, p. 101670, 2021.
[34] S. Yuan and X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," *Computers & Security,* vol. 104, p. 102221, 2021.
[35] M. R. I. Bhuiyan, "The challenges and opportunities of post-COVID situation for small and medium enterprises (SMEs) in Bangladesh," *PMIS review,* vol. 2, no. 1, pp. 145-163, 2023. https://doi.org/10.56567/pmis.v2i1.14
[36] N. Elmrabit, S.-H. Yang, L. Yang, and H. Zhou, "Insider threat risk prediction based on Bayesian network," *Computers & Security,* vol. 96, p. 101908, 2020.
[37] R. A. Alsowail and T. Al-Shehari, "A multi-tiered framework for insider threat prevention," *Electronics,* vol. 10, no. 9, p. 1005, 2021.
[38] M. R. I. Bhuiyan, M. T. Islam, S. A. Alam, and N. S. Sumon, "Identifying passengers satisfaction in transportation quality: An empirical study in Bangladesh," *PMIS Review,* vol. 2, no. 1, pp. 27-46, 2023.
[39] M. AlSlaiman, M. I. Salman, M. M. Saleh, and B. Wang, "Enhancing false negative and positive rates for efficient insider threat detection," *Computers & Security,* vol. 126, p. 103066, 2023.
[40] A. Amin, M. R. I. Bhuiyan, R. Hossain, C. Molla, T. A. Poli, and M. N. U. Milon, "The adoption of Industry 4.0 technologies by using the technology organizational environment framework: The mediating role to manufacturing performance in a developing country," *Business Strategy & Development,* vol. 7, no. 2, p. e363, 2024.
[41] R. Sarala, G. Zayaraz, and S. Aravindanne, "Prediction of insider threats for effective information security risk assessment," *International Journal of Applied Engineering Research,* vol. 10, no. 20, p. 2015, 2015.
[42] L. Daubner, M. Macak, R. Matulevičius, B. Buhnova, S. Maksović, and T. Pitner, "Addressing insider attacks via forensic-ready risk management," *Journal of Information Security and Applications,* vol. 73, p. 103433, 2023.
[43] L. Giddens, L. C. Amo, and D. Cichocki, "Gender bias and the impact on managerial evaluation of insider security threats," *Computers & Security,* vol. 99, p. 102066, 2020.
[44] A. Subhani, I. A. Khan, and A. Zubair, "Review of insider and insider threat detection in the organizations," *Journal of Advanced Research in Social Sciences and Humanities,* vol. 6, no. 4, pp. 167-174, 2021.
[45] M. N. Mia, L. Mani, M. M. Rahman, M. N. U. Milon, and R. Hossain, "Gravitating towards Community Based Tourism (CBT): Community Empowerment and Reducing Poverty in Tourism Sector Development in Bangladesh," *International Journal of Religion,* vol. 5, no. 6, pp. 848-864, 2024.
[46] N. T. Cyriac and L. Sadath, "Is Cyber security enough-A study on big data security Breaches in financial institutions," in *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, 2019: IEEE, pp. 380-385.
[47] J. Haislip, K. Kolev, R. Pinsker, and T. Steffen, "The economic cost of cybersecurity breaches: A broad-based analysis," in *Workshop on the economics of information security (WEIS)*, 2019, vol. 1, p. 37.
[48] C. Z. He, T. Frost, and R. E. Pinsker, "The impact of reported cybersecurity breaches on firm innovation," *Journal of Information Systems,* vol. 34, no. 2, pp. 187-209, 2020.
[49] V. Wang, H. Nnaji, and J. Jung, "Internet banking in Nigeria: Cyber security breaches, practices and capability," *International Journal of Law, Crime and Justice,* vol. 62, p. 100415, 2020.
[50] M. R. Kabir, R. Hossain, M. M. Rahman, M. M. H. Sawon, and L. Mani, "Impact of E-Marketing on Book Purchase Tendencies: An Empirical Study on University Undergraduate Students," *Journal of Ecohumanism,* vol. 3, no. 3, pp. 612-631, 2024.
[51] M. Milon, "Gravitating towards artificial intelligence on anti-money laundering a PRISMA based systematic review," *International Journal of Religion,* vol. 5, no. 7, pp. 303-315, 2024.
[52] A. T. Oyewole, O. B. Adeoye, W. A. Addy, C. C. Okoye, and O. C. Ofodile, "Enhancing global competitiveness of US SMES through sustainable finance: A review and future directions," *International Journal of Management & Entrepreneurship Research,* vol. 6, no. 3, pp. 634-647, 2024.
[53] M. Smith and M. Tiwari, "The implications of national blockchain infrastructure for financial crime," *Journal of Financial Crime,* vol. 31, no. 2, pp. 236-248, 2024. https://doi.org/10.1108/JFC-01-2023-0006
[54] K. Khanom, M. T. Islam, A. A.-T. Hasan, S. M. Sumon, and M. R. I. Bhuiyan, "Worker satisfaction in health, hygiene and safety measures undertaken by the readymade garments industry of Bangladesh: A case study on Gazipur," *Journal of Business Studies,* vol. 3, no. 01, pp. 93-105, 2022.
[55] I. Amara and H. Khlif, "Financial crime, corruption and tax evasion: a cross-country investigation," *Journal of Money Laundering Control,* vol. 21, no. 4, pp. 545-554, 2018.
[56] F. M. J. Teichmann and M.-C. Falker, "Cryptocurrencies and financial crime: solutions from Liechtenstein," *Journal of Money Laundering Control,* vol. 24, no. 4, pp. 775-788, 2021.
[57] J. Wiwoho, D. B. Kharisma, and D. T. K. Wardhono, "Financial crime in digital payments," *Journal of Central Banking Law and Institutions,* vol. 1, no. 1, pp. 47-70, 2022. https://doi.org/10.21098/jcli.v1i1.7
[58] S. Whitehead and G. Farrell, "Anticipating mobile phone 'smart wallet'crime: Policing and corporate social responsibility," *Policing: A Journal of Policy and Practice,* vol. 2, no. 2, pp. 210-217, 2008.
[59] B. H. Custers, R. L. Pool, and R. Cornelisse, "Banking malware and the laundering of its profits," *European Journal of Criminology,* vol. 16, no. 6, pp. 728-745, 2019. https://doi.org/10.1177/1477370818788007

[60] J. Haislip, K. Kolev, R. Pinsker, and T. Steffen, "The economic cost of cybersecurity breaches: A broad-based analysis," in *Workshop on the Economics of Information Security*, 2019, vol. 1, p. 37.
[61] M. R. I. Bhuiyan, M. R. Faraji, M. N. Tabassum, P. Ghose, S. Sarbabidya, and R. Akter, "Leveraging Machine Learning for Cybersecurity: Techniques, Challenges, and Future Directions," *Edelweiss Applied Science and Technology,* vol. 8, no. 6, pp. 4291-4307, 2024.
[62] D. AIS, "Firm-specific financial determinants of non-performing loan in the banking sector of developing countries: Evidence from the listed commercial banks in Bangladesh," *Journal of Economics and Business,* vol. 1, no. 4, pp. 555-563, 2018.
[63] S. Sabuj, A. Arif, and B. Momotaz, "Audit expectation gap: Empirical evidence from Bangladesh, SSRG," *International Journal of Economics and Management Studies,* vol. 6, no. 5, pp. 32-36, 2019.
[64] L. L. Hansen, "Corporate financial crime: Social diagnosis and treatment," *Journal of Financial Crime,* vol. 16, no. 1, pp. 28-40, 2009.
[65] A. Mimi and L. Mani, "Gravitating the Gig Economy for Reshaping the Careers Using Technological Platform in the Digital Age in an Emerging Economy," *Journal of Information Systems and Informatics*, vol. 6, no. 4, pp. 3129–3161, Dec. 2024, doi: https://doi.org/10.51519/journalisi.v6i4.966.
[66] P. Gottschalk, "Theories of financial crime," *Journal of Financial Crime,* vol. 17, no. 2, pp. 210-222, 2010.
[67] M. S. Raza, Q. Zhan, and S. Rubab, "Role of money mules in money laundering and financial crimes a discussion through case studies," *Journal of Financial Crime,* vol. 27, no. 3, pp. 911-931, 2020.
[68] B. Nikkel, "Fintech forensics: Criminal investigation and digital evidence in financial technologies," *Forensic Science International: Digital Investigation,* vol. 33, p. 200908, 2020.
[69] M. Dion, "A Gadamerian perspective on financial crimes: An issue of historically-rooted prejudices and narrative strategies," *Journal of Financial Crime,* vol. 26, no. 3, pp. 836-860, 2019.
[70] J. F. Gilsinan *et al.*, "The role of private sector organizations in the control and policing of serious financial crime and abuse," *Journal of Financial Crime,* vol. 15, no. 2, pp. 111-123, 2008.
[71] H.-G. Gadamer, *Hans-Georg Gadamer on education, poetry, and history: Applied hermeneutics*. Suny Press, 1992.
[72] W. N. Abdullah and R. Said, "The influence of corporate governance and human governance towards corporate financial crime: A conceptual paper," in Redefining Corporate Social Responsibility, vol. 13, 2018, pp. 193-215.
[73] S. Saha, A. R. Hasan, K. R. Islam, and M. A. I. Priom, "Sustainable Development Goals (SDGs) practices and firms' financial performance: Moderating role of country governance," *Green Finance,* vol. 6, no. 1, pp. 162-198, 2024.
[74] F. Baumann and T. Friehe, "Tax evasion and tacit collusion," *Public Finance Review,* vol. 41, no. 5, pp. 633-657, 2013.
[75] M. Khatun, R. Islam, S. Kumar, R. Hossain, and L. Mani, "The Impact of Artificial Intelligence on Educational Transformation: Trends and Future Directions," *Journal of Information Systems and Informatics,* vol. 6, no. 4, pp. 2347-2373, 2024.