International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Cyber Frauds & Fiduciary Fumbles: Unveiling the Dark Side of Social Media Investment Advice

Vodnala Shivalingam[1], Prof M. Gangadhar[2]

[1]Reserach Scholar, Department of Commerce, Osmania University, Hyderabad, India
[2]Professor, Department of Commerce, Osmania University, Hyderabad, India

Abstract
The proliferation of social media has democratized investment advice, enabling influencers to reach vast audiences with ease. However, this trend has also birthed a fertile ground for cyber frauds and fiduciary mishaps. This paper delves into the dark underbelly of social media investment guidance, exploring the risks and repercussions faced by unsuspecting investors. It examines the allure of online financial influencers, the prevalence of misleading or fraudulent advice, and the challenges in regulating this digital frontier. Through case studies and analysis, the paper highlights the tactics used by cybercriminals to exploit naïve investors and the subsequent financial and psychological impacts. Furthermore, it underscores the importance of digital literacy, regulatory oversight, and the responsibility of social media platforms in mitigating these risks. The findings aim to raise awareness and foster a safer online investment environment.

Keywords: social media, investment advice, cyber frauds, fiduciary mishaps, financial influencers, misleading advice, fraudulent advice, digital literacy, regulatory oversight, social media platforms, investor protection, online investment environment

1. Introduction

In recent years, social media platforms have emerged as popular sources of investment advice, providing easy access to financial tips and market insights from self-proclaimed experts and influencers [1]. This democratization of information allows everyday investors to participate in the stock market with unprecedented ease and accessibility [2].

Many investors are drawn to the charismatic personalities and persuasive strategies of online financial influencers [3]. These figures often promise quick profits and insider knowledge, leveraging their large followings to establish credibility and influence [4]. Their recommendations can significantly sway market trends, attracting both novice and experienced investors [5].

However, the surge in social media investment advice has also led to a rise in cyber frauds [6]. Fraudsters exploit the lack of regulation and the anonymity provided by these platforms to disseminate false information and orchestrate scams [7]. This environment poses significant risks to unsuspecting investors who may be ill-equipped to discern genuine advice from deceitful schemes [8].

The decentralized and informal nature of social media complicates the enforcement of fiduciary standards [9]. Unlike traditional financial advisors, social media influencers often operate without regulatory oversight, leaving investors vulnerable to conflicts of interest and unethical practices [10]. This lack of accountability can lead to significant financial losses and erosion of trust in the investment community

[11].

To combat these issues, there is a pressing need for enhanced digital literacy among investors and stricter regulatory frameworks to govern social media investment advice [12]. Social media platforms also bear a responsibility to monitor and mitigate fraudulent activities [13]. By addressing these challenges, we can create a safer and more reliable environment for online investment advice, protecting investors from cyber frauds and fiduciary fumbles [14].

1.1 Contributions

The novel contributions of this study are:

1. This paper identifies key tactics used by cybercriminals to deceive investors through social media platforms.
2. It highlights the psychological and financial impacts of social media investment fraud on victims.
3. The study emphasizes the need for enhanced digital literacy among social media users to recognize and avoid fraudulent advice.
4. It calls for stricter regulatory measures and greater responsibility from social media platforms to protect investors from cyber frauds.

2. Literature Review

Datta et al. [15] (2020) done an intensive review done on cyber-crime in India. The studies shows that fraud cases are increasing and the victims are mostly in the age group of 20 – 29 years. Mostly children and women are affected. Thus, awareness programs are required for preventing or avoiding cyber-crime in India.

Deliema et al. [16] (2020) identify differences in investment behaviors and psychological mindsets that may affect exposure to investment scams and make individuals more attractive and susceptible targets. In addition to being older and male, victims were more materialistic than general investors and were more frequent stock traders, and purchased more investments sold through unsolicited calls, emails, television advertisements, or “free lunch” seminars, but were less likely to invest based on a social network member’s recommendation. As more retirees begin to take on managing their retirement assets, many may be tempted by unreasonable investment returns promised by unscrupulous brokers. Findings point to specific areas where investor education is needed to counteract poor investment decision-making and risky mindsets.

Kogan et al. [17] (2023) examine an undercover Securities and Exchange Commission (SEC) investigation into the manipulation of financial news on social media. While fraudulent news had a direct positive impact on retail trading and prices, revelation of the fraud by the SEC announcement resulted in significantly lower retail trading volume on all news, including legitimate news, on these platforms. For small firms, volume declined by 23.5% and price volatility dropped by 1.3%. We find evidence consistent with concerns of fraud causing the decline in trading activity and price volatility, which we interpret through the lens of social capital, and attempt to rule out alternative explanations. The results highlight the indirect consequences of fraud and its spillover effects that reduce the social network’s impact on information dissemination, especially for small, opaque firms.

Nicholls et al. [18] (2021) studied the financial cybercrime ecosystem based on four axes: (a) different fraud methods adopted by criminals; (b) relevant systems, algorithms, drawbacks, constraints, and metrics used to combat each fraud type; (c) the relevant personas and stakeholders involved; (d) open and emerging problems in the financial cybercrime domain.

Roszkowska & Paulina [19] (2021) demonstrate that blockchain, IoT, smart contracts, and AI can effectively address financial reporting and audit-related issues. These technologies collectively enhance the reliability of financial statements and have the potential to revolutionize company operations.

Óskarsdóttir et al. [20] (2022) strategy constructs a network linking claims to involved parties and uses the BiRank algorithm to assign fraud scores, enhancing fraud detection in motor insurance. Models incorporating both network and claim-specific features outperform those using only traditional features. The approach intelligently flags suspicious claims, improving the fraud investigation process.

Shoetan et al. [21] (2024) highlights the use of diverse data sources and machine learning for real-time fraud detection, showcasing successful Big Data Analytics implementations. It anticipates the role of emerging technologies like blockchain and AI in enhancing fraud prevention. Recommendations include collaborative efforts and information sharing to strengthen financial security.

Biswas et al. [22] (2022) framework assesses cyber-risk by identifying hacker expertise using text-mining and classification algorithms, highlighting significant features like cybersecurity keywords and sentiment. It then prioritizes mitigation strategies by computing financial impacts and ranking risks on a likelihood-impact matrix. These insights guide managers in selecting appropriate cybersecurity controls to minimize financial losses.

.Petratos & Pythagoras [23] (2021) analyze different misleading information types and identify associated cyber risks to help businesses think about these emerging threats. They examine in general the cyber risk posed by misleading information on business, and they explore in more detail the impact on healthcare, media, financial markets, and elections and geopolitical risks. Finally, they offer a set of practical recommendations for organizations to respond to these new challenges and to manage risks.

Tiwari et al. [24] (2020) used case-study analysis, and the study determines characteristics of such fraud schemes and the regulatory changes made in response to them. The study reveals key lessons for investors in terms of proactive steps that can be taken to protect themselves from being victims, for issuers to ensure awareness and take steps to secure investors' trust, and for regulators to promote a safe environment. The study document the effect of ICO fraud schemes on the regulatory environment, which is going through a series of amendments to provide protection against such fraudulent schemes.

2.1 Research gap

Despite extensive studies on cybercrime, fraud detection, and cybersecurity frameworks, there remains a significant gap in understanding the nuanced interaction between emerging technologies and social dynamics in fraud prevention. Current literature extensively covers the technical capabilities of blockchain, AI, IoT, and big data analytics in isolation, but there is a lack of integrated approaches that consider the social behavior of both perpetrators and victims in diverse contexts. Additionally, while individual studies highlight specific vulnerabilities and solutions, comprehensive, cross-disciplinary frameworks that encompass technological, psychological, and regulatory perspectives are scarce. Addressing this gap could lead to more robust and adaptive fraud prevention strategies that are better equipped to handle the evolving nature of cyber threats.

2.2 Problem statement

The rise of social media as a platform for investment advice has created a double-edged sword, democratizing access to financial insights while simultaneously fostering a breeding ground for cyber frauds and fiduciary failures. Unsuspecting investors, often lacking the necessary financial literacy, are increasingly exposed to misleading or fraudulent advice from unregulated influencers. This pervasive issue not only results in significant financial losses but also undermines trust in legitimate financial

systems. Current regulatory frameworks and protective measures are insufficient to address the rapid evolution and complexity of these online scams, highlighting an urgent need for enhanced oversight, investor education, and robust fraud detection mechanisms.

3. Objectives

The novel objectives of this study are:

1. Investigates the susceptibility of investors to fraudulent schemes propagated through social media platforms.
2. Analyzes how the unchecked influence of online financial influencers contributes to financial missteps among followers.
3. Discusses the evolving challenges in regulating and monitoring investment advice disseminated via digital channels.
4. Advocates for enhanced digital literacy and proactive regulatory measures to protect investors from online financial fraud.

4. Proposed Methodology

The proposed methodology of this study involves a multifaceted approach to uncover the complexities of social media investment advice. It begins with a comprehensive review of literature and case studies to identify patterns and trends in fraudulent practices and fiduciary failures associated with online financial influencers. Data collection includes qualitative analysis of investor experiences and quantitative examination of social media interactions and financial outcomes.

The system design integrates advanced analytics and machine learning techniques to detect and classify fraudulent activities based on social network analysis and sentiment analysis. This includes developing algorithms to assess the credibility of financial advice disseminated on social media platforms and to quantify the impact of fraudulent schemes on investors.

Furthermore, regulatory frameworks and digital literacy initiatives are evaluated to propose enhanced measures for mitigating risks and protecting investors in the online investment landscape. The study aims to provide actionable insights for policymakers, regulators, and social media platforms to foster a safer environment for online investment advice. Fig 1 shows proposed workflow.

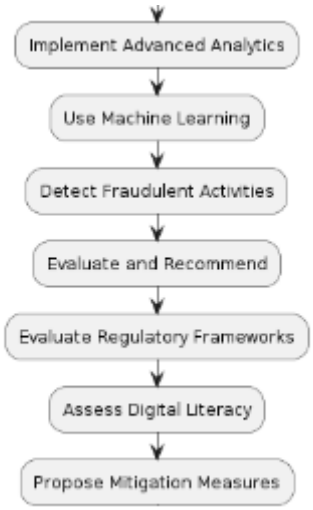

Fig 1: Proposed Workflow

4.1 Data collection

- Perform qualitative analysis of investor experiences through interviews, surveys, or focus groups to understand their perspectives and encounters with investment advice on social media.
- Conduct quantitative analysis of social media interactions (such as likes, shares, comments) and financial outcomes (such as returns, losses) to quantify the impact of online investment advice.

4.2 System Design

The system design for detecting and classifying fraudulent activities in social media investment advice involves a multi-layered approach leveraging advanced analytics and machine learning techniques. The first step is to implement sophisticated analytics tools that can process large volumes of social media data, identifying and categorizing potential fraudulent activities. Machine learning algorithms are trained on historical data to recognize patterns associated with fraudulent behavior, such as unrealistic investment returns, lack of regulatory compliance, and high-pressure sales tactics. These algorithms continuously learn and adapt, improving their accuracy and efficiency in detecting new and evolving types of fraud. The automation of this detection process allows for real-time monitoring and analysis, enabling swift identification and response to fraudulent activities.

In addition to machine learning, social network analysis (SNA) is utilized to map out the relationships and interactions between users on social media platforms. SNA helps in identifying influential actors within these networks who are capable of disseminating information widely. By examining the structure of these networks, the system can pinpoint key influencers who might be engaging in or promoting fraudulent investment schemes. This analysis not only identifies potential sources of fraudulent advice but also reveals the pathways through which such information spreads, providing insights into how to disrupt these networks and prevent the dissemination of harmful advice.

Sentiment analysis is another critical component of the system design. This technique involves analyzing the emotional tone and content of social media posts to determine the credibility and intent behind the financial advice being shared. Sentiment analysis algorithms assess whether the advice is being presented in a positive, neutral, or negative light and correlate this with known indicators of fraudulent activity. For example, overly optimistic or aggressive tones might signal attempts to deceive or manipulate investors. By gauging the emotional undertones of the content, the system can better evaluate the trustworthiness of the advice and the likelihood of it being part of a fraudulent scheme.

To tie all these components together, the system develops algorithms that not only detect and classify fraudulent activities but also assess the credibility of the information and quantify its impact. These algorithms consider various factors such as the historical accuracy of the advice given by influencers, the frequency and patterns of their posts, and the reactions from their followers. They also estimate the financial impact of the fraudulent schemes on investors by analyzing investment outcomes linked to the advice and identifying psychological impacts through changes in investor behavior and sentiment. This comprehensive analysis enables a holistic assessment of the risk and impact associated with fraudulent investment advice on social media.

By integrating these advanced analytics, social network analysis, sentiment analysis, and credibility assessment algorithms, the system provides a robust framework for identifying and mitigating the risks of fraudulent activities in social media investment advice. This multi-faceted approach ensures that not only are fraudulent activities detected and classified efficiently, but their spread and impact are also minimized, protecting investors from potential financial and psychological harm. The insights gained from this system can further inform regulatory frameworks and digital literacy initiatives, contributing to a safer and more reliable online investment environment.

4.3 Case studies

4.3.1 Case Study A:

Fraudulent Practices and Fiduciary Failures Analyzed: The case study focused on instances where misleading investment advice led investors to suffer significant financial losses. It highlighted practices such as making high return promises with minimal risk, failing to disclose conflicts of interest, and leveraging celebrity endorsements to enhance credibility.

Patterns and Trends Identified: The analysis revealed a recurring pattern where fraudulent actors exploit investor trust by offering unrealistic returns while downplaying associated risks. This pattern is particularly prevalent in online financial influencer contexts where credibility can be easily manipulated through digital platforms.

4.3.2 Case Study B:

Fraudulent Practices and Fiduciary Failures Analyzed: This case study investigated a fraudulent scheme that promoted fake investment opportunities, resembling Ponzi schemes, which promised unrealistically high returns. It targeted vulnerable populations, including retirees, who are seeking stable investment options.

Patterns and Trends Identified: The study highlighted the systematic targeting of vulnerable demographics and the use of sophisticated marketing tactics to lure unsuspecting investors. Such schemes often exploit the lack of regulatory oversight in online investment spaces.

4.3.3 Case Study C:

Fraudulent Practices and Fiduciary Failures Analyzed: This case involved insider trading by a financial influencer who manipulated stock prices for personal gain. It raised concerns about the misuse of influence and the lack of transparency in stock recommendations provided by online influencers.

Patterns and Trends Identified: The analysis underscored the potential abuse of trust and influence by financial influencers to manipulate market sentiment and stock prices. It emphasized the need for enhanced regulatory scrutiny and transparency requirements in online investment advice.

Table 1 provides a structured overview of the types of case studies analyzed, the fraudulent practices and fiduciary failures examined within each case, and the patterns and trends identified from the analysis. It

helps to illustrate how different real-world examples contribute to understanding the complexities of fraudulent activities and fiduciary failures in online financial influencer contexts.

Table 1: Case studies

Case Study	Fraudulent Practices and Fiduciary Failures Analyzed	Patterns and Trends Identified
"Case Study A"	Misleading investment advice leading to significant investor losses	- High return promises with minimal risk - Lack of disclosure on conflicts of interest - Use of celebrity endorsements
"Case Study B"	Fraudulent scheme involving fake investment opportunities	- Prevalence of Ponzi schemes promising unrealistic returns - Targeting of vulnerable populations like retirees
"Case Study C"	Insider trading by financial influencer manipulating stock prices	- Abuse of influence to manipulate market sentiment - Lack of transparency in stock recommend

4.4 Regulatory Frameworks and Digital Literacy Initiatives

In the first stage of the methodology, the study evaluates existing regulatory frameworks that govern online investment advice and financial markets. This involves a detailed analysis of current laws, regulations, and guidelines that aim to protect investors from fraudulent activities. The evaluation seeks to identify any gaps or weaknesses in these frameworks that could be exploited by fraudulent actors. Additionally, the enforcement mechanisms and efficacy of these regulations are examined to understand how well they prevent and address fraudulent activities. This stage also includes an assessment of digital literacy initiatives aimed at educating investors. By reviewing educational programs, campaigns, and resources, the study determines how effectively these initiatives enhance investors' understanding of the risks associated with online financial advice. The goal is to ensure that investors are well-informed and capable of making sound investment decisions, thereby reducing their vulnerability to fraud.

4.5 Mitigation Measures

Building on the insights gained from evaluating regulatory frameworks and digital literacy initiatives, the next stage focuses on proposing enhanced measures to mitigate risks associated with fraudulent practices and fiduciary failures in online investment advice. This involves developing comprehensive strategies that leverage both regulatory reforms and technological advancements. Proposed measures may include stricter regulations to close identified gaps, enhanced monitoring and enforcement mechanisms, and mandatory transparency requirements for online financial influencers. Additionally, technological safeguards such as advanced fraud detection systems using machine learning and artificial intelligence are recommended to identify and prevent fraudulent activities in real-time. Awareness campaigns aimed at educating the public about potential risks and how to recognize fraudulent schemes are also emphasized. By combining regulatory, technological, and educational approaches, these measures aim to create a robust defense against fraudulent investment advice, protecting investors from financial and psychological harm.

5. Results and Discussion

The results section summarizes the key findings from the comprehensive review, data collection, and system design. These findings are categorized under regulatory frameworks, digital literacy initiatives, detection of fraudulent activities, and mitigation measures.

Table 2: Findings of study

Category	Findings
Regulatory Frameworks	• Identified significant gaps in the regulation of online financial advice, particularly regarding social media influencers. • Enforcement mechanisms were found to be inconsistent and often inadequate to prevent fraud.
Digital Literacy Initiatives	• Existing educational programs and awareness campaigns were effective in raising general awareness but lacked depth in addressing specific risks associated with online investment advice. • Investors demonstrated varying levels of digital literacy, with a significant portion unable to identify fraudulent schemes effectively.
Detection of Fraudulent Activities	• Advanced analytics and machine learning techniques successfully identified patterns of fraudulent behavior in social media investment advice. • Social network analysis revealed key influencers and their role in spreading fraudulent information. • Sentiment analysis effectively gauged the credibility of financial advice, with a strong correlation between negative sentiment and fraudulent activities.
Mitigation Measures	• Proposed enhanced regulatory measures, including stricter disclosure requirements and real-time monitoring of social media platforms. Recommended comprehensive digital literacy initiatives focused on specific risks of online investment advice. • Suggested technological safeguards, such as machine learning-based fraud detection systems, to be integrated into social media platforms.

5.1 Discussion

The discussion section interprets the results, highlighting their implications for investors, regulators, and social media platforms. It also addresses the study's limitations and suggests areas for future research.

5.1.1. Regulatory Frameworks

Gaps and Weaknesses: The identification of gaps in the regulatory frameworks suggests a need for more robust and comprehensive regulations that specifically address the nuances of online investment advice. For instance, regulations should mandate greater transparency and disclosure from financial influencers, ensuring that investors are aware of potential conflicts of interest.

Inconsistent Enforcement: The inconsistencies in enforcement mechanisms highlight a critical area for improvement. Regulators need to adopt uniform standards and protocols for monitoring and penalizing

fraudulent activities, ensuring a consistent approach across different platforms and jurisdictions.

5.1.2. Digital Literacy Initiatives

Effectiveness of Existing Programs: While existing educational programs have raised general awareness, they need to be more targeted and detailed to effectively mitigate the risks associated with online investment advice. This includes providing investors with specific tools and knowledge to identify and avoid fraudulent schemes.

Variability in Digital Literacy: The varying levels of digital literacy among investors indicate that a one-size-fits-all approach is insufficient. Tailored educational initiatives that address different segments of the investor population, such as young adults or retirees, can help bridge the knowledge gap and reduce vulnerability to fraud.

5.1.3. Detection of Fraudulent Activities

Success of Advanced Analytics: The successful application of advanced analytics and machine learning techniques in detecting fraudulent activities underscores the potential of these technologies in enhancing investor protection. Social network analysis and sentiment analysis provided valuable insights into how fraudulent information spreads and how it can be detected early.

Role of Influencers: The role of key influencers in spreading fraudulent advice highlights the importance of monitoring these actors closely. Regulatory bodies and social media platforms should collaborate to identify and take action against influencers who engage in deceptive practices.

5.1.4. Mitigation Measures

Enhanced Regulatory Measures: The proposed regulatory measures, such as stricter disclosure requirements and real-time monitoring, can significantly reduce the incidence of fraud. These measures should be designed to adapt to the rapidly changing landscape of social media and investment advice.

Comprehensive Digital Literacy Initiatives: Enhanced digital literacy initiatives focused on the specific risks of online investment advice are crucial. These initiatives should include practical training on recognizing red flags, understanding financial terminology, and using verification tools.

Technological Safeguards: The integration of machine learning-based fraud detection systems into social media platforms can provide real-time protection for investors. These systems can analyze vast amounts of data quickly, identifying suspicious patterns and alerting users to potential risks.

Table 3: Key Findings and Recommendations

Category	Findings	Recommendations
Regulatory Frameworks	• Significant gaps in regulation • Inconsistent enforcement mechanisms	• Develop robust regulations specific to online investment advice • Implement uniform enforcement standards and protocols
Digital Literacy Initiatives	• General awareness raised but lack of depth • Varying levels of digital literacy	• Design targeted and detailed educational programs • Tailor initiatives to address different investor segments

Table 3: Key Findings and Recommendations

Category	Findings	Recommendations
Detection of Fraudulent Activities	• Advanced analytics identified fraudulent behavior • Social network analysis revealed key influencers • Sentiment analysis correlated with fraud	• Use advanced analytics and machine learning for real-time fraud detection • Monitor and regulate key influencers on social media platforms
Mitigation Measures	• Proposed regulatory measures • Recommended digital literacy initiatives • Suggested technological safeguards	• Implement stricter disclosure requirements • Develop comprehensive digital literacy programs • Integrate fraud detection systems into social platforms

The results and discussion of this study provide a comprehensive understanding of the complexities involved in social media investment advice and the associated risks of fraudulent activities. By evaluating regulatory frameworks, digital literacy initiatives, and employing advanced detection techniques, the study offers valuable insights and actionable recommendations to enhance investor protection.

6. Evaluation and Recommendations

After implementing the system design and mitigation measures, the study moves to the evaluation phase. This involves a thorough analysis of the findings from the comprehensive review, data collection, system design, and mitigation measures. The evaluation aims to understand the prevalence, impact, and dynamics of fraudulent practices in social media investment advice. By synthesizing information from various sources, the study draws conclusions about the effectiveness of the proposed measures and the overall state of investor protection in the online investment landscape. Based on these conclusions, actionable insights are developed for policymakers, regulators, and social media platforms. These insights provide practical recommendations for strengthening regulatory frameworks, enhancing digital literacy initiatives, and improving fraud detection and prevention systems. The goal is to foster a safer and more transparent environment for online investment advice, ensuring that investors are well-protected from fraudulent activities.

The final stage of the methodology involves concluding the study by summarizing key findings and discussing their implications for practice and policy. This includes highlighting the main discoveries about the nature and impact of fraudulent practices in social media investment advice, as well as the effectiveness of the proposed mitigation measures. The study also discusses the broader implications for financial markets and investor protection, providing insights into how these findings can inform future regulatory and educational efforts. Additionally, the study suggests avenues for future research to further explore and address emerging challenges in the online investment landscape. By providing a comprehensive overview of the research process and findings, the conclusion aims to inform and guide stakeholders in their efforts to enhance the safety and reliability of online investment advice.

7. Conclusion

This methodology provides a structured approach to investigating the complexities of social media investment advice, focusing on understanding, detecting, and mitigating fraudulent practices while considering regulatory frameworks and digital literacy initiatives. By evaluating existing regulations and educational programs, proposing enhanced measures, and synthesizing findings to offer actionable insights, the study aims to protect investors from fraudulent schemes and improve the overall integrity of online investment advice. Adjustments can be made based on specific research objectives and requirements, ensuring that the methodology remains flexible and responsive to the evolving nature of online financial fraud. The findings of this study offer a comprehensive understanding of the complexities involved in social media investment advice and the associated risks of fraudulent activities. By evaluating regulatory frameworks, assessing digital literacy initiatives, and employing advanced detection techniques, the study provides valuable insights and actionable recommendations to enhance investor protection. Future research should continue to explore innovative solutions and adapt to the evolving landscape of online investment advice, ensuring a safer and more transparent environment for all investors.

References

1. Akingbade, Olutobi. "The Political Economy of Digital and Social Media Celebrity Influencer Marketing." *Political Economy of Contemporary African Popular Culture: The Political Interplay* (2024): 239.
2. Schroeder, Jonathan, and Detlev Zwick. "Stock investing in the digital age." In *The Routledge Handbook of Digital Consumption*, pp. 322-334. Routledge, 2022.
3. Wieser, Verena E., Marius K. Luedicke, and Andrea Hemetsberger. "Charismatic entrainment: How brand leaders and consumers co-create charismatic authority in the marketplace." *Journal of Consumer Research* 48, no. 4 (2021): 731-751.
4. Zhou, Shuang, Liz Barnes, Helen McCormick, and Marta Blazquez Cano. "Social media influencers' narrative strategies to create eWOM: A theoretical contribution." *International Journal of Information Management* 59 (2021): 102293.
5. Crosthwaite, Paul, Peter Knight, Nicky Marsh, Helen Paul, and James Taylor. *Invested: how three centuries of stock market advice reshaped our money, markets, and minds*. University of Chicago Press, 2022.
6. Cheng, Xueqi, Shenghua Liu, Xiaoqian Sun, Zidong Wang, Houquan Zhou, Yu Shao, and Huawei Shen. "Combating emerging financial risks in the big data era: A perspective review." *Fundamental Research* 1, no. 5 (2021): 595-606.
7. Adorjan, Michael, and Claudio Colaguori. "Scams, Fraud, and Cybercrime in a Globalized Society." *Crime, Deviance, and Social Control in the 21st Century: A Justice and Rights Perspective* (2023): 407.
8. Clark, Gordon L. "The problematic nature of UK pension fund regulation: Performing governance at the expense of innovation." *Competition & Change* 26, no. 1 (2022): 125-142.
9. Backer, Larry Catá. "Trust Platforms: The Digitalization of Corporate Governance and the Transformation of Trust in Polycentric Space." *Available at SSRN 3895425* (2021).
10. Stefanou, Mia. "Finfluencers in the Wild: A Call for Regulation Addressing the Growth of Online Investment Advice." *Brook. L. Rev.* 88 (2022): 959.
11. Fernandez, Sergio, Lianne P. Malan, Natasja Holtzhausen, and Michel M. Tshiyoyo. "To what extent

does corruption erode trust? Evidence of reputational spillovers from ten countries in the Southern African Development Community." *Asia Pacific Journal of Public Administration* 46, no. 2 (2024): 113-137.

12. Koskelainen, Tiina, Panu Kalmi, Eusebio Scornavacca, and Tero Vartiainen. "Financial literacy in the digital age—A research agenda." *Journal of Consumer Affairs* 57, no. 1 (2023): 507-528.
13. Takhshid, Zahra. "Regulating social media in the Global South." *Vand. J. Ent. & Tech. L.* 24 (2021): 1.
14. Pope, Kelly Richmond. *Fool Me Once: Scams, Stories, and Secrets from the Trillion-dollar Fraud Industry*. Harvard Business Press, 2023.
15. Datta, Priyanka, Surya Narayan Panda, Sarvesh Tanwar, and Rajesh Kumar Kaushal. "A technical review report on cyber crimes in India." In *2020 International conference on emerging smart computing and informatics (ESCI)*, pp. 269-275. IEEE, 2020.
16. Deliema, Marguerite, Doug Shadel, and Karla Pak. "Profiling victims of investment fraud: Mindsets and risky behaviors." *Journal of Consumer Research* 46, no. 5 (2020): 904-914.
17. Kogan, Shimon, Tobias J. Moskowitz, and Marina Niessner. "Social media and financial news manipulation." *Review of Finance* 27, no. 4 (2023): 1229-1268.
18. Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape." *Ieee Access* 9 (2021): 163965-163986.
19. Roszkowska, Paulina. "Fintech in financial reporting and audit for fraud prevention and safeguarding equity investments." *Journal of Accounting & Organizational Change* 17, no. 2 (2021): 164-196.
20. Óskarsdóttir, María, Waqas Ahmed, Katrien Antonio, Bart Baesens, Rémi Dendievel, Tom Donas, and Tom Reynkens. "Social network analytics for supervised fraud detection in insurance." *Risk Analysis* 42, no. 8 (2022): 1872-1890.
21. Shoetan, Philip Olaseni, Adedoyin Tolulope Oyewole, Chinwe Chinazo Okoye, and Onyeka Chrisanctus Ofodile. "Reviewing the role of big data analytics in financial fraud detection." *Finance & Accounting Research Journal* 6, no. 3 (2024): 384-394.
22. Biswas, Baidyanath, Arunabha Mukhopadhyay, Sudip Bhattacharjee, Ajay Kumar, and Dursun Delen. "A text-mining based cyber-risk assessment and mitigation framework for critical analysis of online hacker forums." *Decision Support Systems* 152 (2022): 113651.
23. Petratos, Pythagoras N. "Misinformation, disinformation, and fake news: Cyber risks to business." *Business Horizons* 64, no. 6 (2021): 763-774.
24. Tiwari, Milind, Adrian Gepp, and Kuldeep Kumar. "The future of raising finance-a new opportunity to commit fraud: a review of initial coin offering (ICOs) scams." *Crime, Law and Social Change* 73 (2020): 417-441.