Analyzing Threats to Financial Market Integrity - A Taxonomy of Financial Fake News Schemes

Oliver Rath
University of Cologne
rath@wim.uni-koeln.de

Frederic Haase
University of Cologne
haase@wim.uni-koeln.de

Johannes Melsbach
University of Cologne
melsbach@wim.uni-koeln.de

Jiarun Liu
University of Cologne
liu@wim.uni-koeln.de

Julia Lauten
University of Cologne
lauten@wim.uni-koeln.de

Detlef Schoder
University of Cologne
schoder@wim.uni-koeln.de

Abstract

Protecting financial market integrity is a key concern for regulators as disinformation-driven fraud based on financial fake news (FFN) is taking on a significant role in financial market manipulation. While existing research focuses on describing or categorizing financial fraud schemes more broadly, we aim to provide a taxonomy focusing specifically on FFN schemes. Drawing on U.S. Securities and Exchange Commission (SEC) litigation releases and underpinning theoretical tenets, we utilize an iterative taxonomy approach to systematically classify fraudulent FFN schemes. Our contribution is to provide a robust, comprehensive framework that enhances the body of knowledge about the diverse landscape of financial disinformation. The taxonomy provides practical benefits to market participants and market surveillance authorities by its ability to guide the development of fraud detection systems.

Keywords: financial fraud, financial fake news, disinformation, taxonomy, digital institutions

1. Introduction

Disinformation, defined as misinformation that is disseminated with intent (Søe, 2021), is the foundation for financial fraud schemes based on financial fake news (FFN) (Clarke et al., 2020). A remarkable number of fraudulent schemes related to disinformation are brought to courts by market surveillance institutions like the United States Securities and Exchange Commission (SEC) (SEC, 2023). The effort of such institutions to uphold market integrity require proactive monitoring and countermeasures. Yet, the changing tactics of fraudsters, an increasing number and variety of communication channels, as well as technological advances (Dupuis et al., 2023) increasingly complicate governmental efforts to trace complex fraudulent schemes (Siering et al., 2021). Consequently, governments require robust detection systems to mitigate economic losses caused by fraudulent financial activities (Harrison et al., 2022).

While there is an expanding body of research on fake news (e.g., Lazer et al., 2018) and how they spread (Vosoughi et al., 2018), there remains the need for deeper investigation of its application in financial fraud. Prior research in the field of FFN fraud has utilized machine learning and natural language processing to detect FFN articles (e.g., Zhang et al., 2022), broadly categorized financial fraud schemes (Siering et al., 2017), or delved into the role of manipulators and their impact on market efficiency (Aggarwal & Wu, 2003). However, to the best of our knowledge, there exists no taxonomy on the use of disinformation in financial fraud that enhances the understanding of such fraudulent schemes.

In our study, we follow the taxonomy development method by Nickerson et al. (2013), which allows us to incorporate both theoretical work in the research field as well as an analysis of 60 empirical documents from SEC litigations, outlining the effective use of disinformation in relevant court cases. Finally, we provide an evaluation of our proposed taxonomy and discuss its ability to enhance the configuration and development of fraud detection systems.

Our study is organized as follows. First, we review existing literature on governmental institutions, market integrity and financial fake news. Following this, we describe underpinning theoretical tenets that will provide the foundation for our taxonomy. We then detail our methodological approach, explain our data acquisition and taxonomy development approach. In the subsequent section, we present our findings, describe the proposed taxonomy, and provide an evaluation. We

URI: https://hdl.handle.net/10125/106650
978-0-9981331-7-1

further discuss the potential application of our taxonomy for the development and improvement of fraud detection systems. Finally, we discuss the implications of our taxonomy, provide future research, and conclude.

2. Related literature

Our research is underpinned based on two main streams of related literature: a) the responsibility of government institutions to protect financial market integrity in the digital age, and b) the advance of financial fake news and related challenges for regulators.

2.1. Government institutions and financial market integrity

As the digital era revolutionizes the landscape of financial markets, it simultaneously introduces multifaceted challenges to the preservation of financial market integrity. To navigate these complexities, governmental bodies need to foster new digital proficiencies, augment analytical skills, and harness innovative methods and tools. These measures will fortify trust in their institutions and ensure the reliability of information (Black, 2001; Dawes & Helbig, 2015; Siering et al., 2017).

Digital government (or e-government) is a multidisciplinary research field that applies various lenses on understanding, analyzing, and accompanying the digital transformation of government institutions through information and communication technologies (Scholl, 2022). Digital government research is concerned with the digitization of government services, optimizing internal operations (Charalabidis et al., 2019), or examining the successes and failures of digital government initiatives (Gil-Garcia and Flores-Zúñiga, 2020). The speed of such digital transformation can further increase in times of external shocks or crisis (Moser-Plautz & Schmidthuber, 2023).

Fewer studies explore the critical capabilities digital governments require to strengthen their institutions across maintaining the integrity of financial markets. Such capabilities can increase efficiency, support trust in government, transparency as well as legitimation and participation (Bertot et al., 2010; Chen, 2012). Establishing functioning financial markets is an imperative challenge for economies and governments (Black, 2001; Comerton-Forde and Rydge, 2006). The main responsibilities for financial system regulation traditionally include ensuring "financial stability; market efficiency, transparency and integrity; and consumer protection" (Moloney, 2012). Regulators need to ensure that market participants receive good information on market conditions and company values (Black, 2001). Dawes and Helbig (2015) underline, how imperative it is for institutions to develop skill sets and tools in the realm of data and (dis-)information. Chen (2012) illustrates how the introduction of the eXtensible Business Reporting Language by the SEC and other regulatory bodies improved transparency, accountability, and efficiency in financial market reporting. Aitken et al. (2015) analyze how governments protect market integrity with respect to manipulation and insider trading. The team evaluated the effect of exchange trading rules, which are transparent to the public, and surveillance mechanisms, which are usually concealed, in 22 stock exchanges around the world showing that both measures are in fact protecting the market.

Further research into how fraudsters use manipulation techniques like the dissemination of financial fake news may help regulators to further improve regulation and surveillance mechanisms to strengthen market integrity.

2.2. Financial fake news

Financial fraud is a significant problem, including numerous schemes designed to mislead market participants, manipulate financial markets, and illegally acquire wealth.

Such schemes include pump-and-dump as well as paid promotions which both incorporate the use of disinformation. A pump-and-dump scheme involves luring investors into buying a stock to artificially inflate the price (Aggarwal & Wu, 2003). Spreading disinformation increases the buying activity, which raises the stock's price. The fraudsters then sell their shares at a high price, while other investors lose their money selling when the price drops. In a paid promotion, also called stock touting (Siering, 2019), an author or group of authors is paid to promote a specific stock, often writing misleading or untruthful information. The scheme does not necessarily result in a subsequent price drop.

The problem of disinformation, particularly in finance, referred to as FFN, has not been widely studied as in other areas such as politics or sports (Tandoc et al., 2021). Despite common characteristics with general disinformation, such as intentional deception (Clarke et al., 2020), FFN differs in its specific content, which often relates to financial information. For example, FFN involves the dissemination of false or distorted data about financial markets, companies, or investment prospects that can destabilize markets and undermine public trust (Fong, 2021). It ranges from speculative claims about corporate acquisitions to untrue statements about regulatory changes or financial results (Kogan et

al., 2021). Recent research on FFN has focused on using machine learning and natural language processing to detect FFN articles. For example, Zhi et al. (2021) introduced a multifactorial CNN-LSTM model to detect FFN based on textual content, while Zhang et al. (2022) developed a theory-based machine learning model with various features, including dissemination patterns in social media. Mohankumar et al. (2023) used crosswise networks for text-based FFN detection. While these approaches are promising, they require further investigation for improvement and verification. In addition, these methods do not provide a comprehensive taxonomy, necessary to advance the understanding of the underlying FFN schemes.

3. Theoretical background

We root our analysis of financial fraud disinformation into different theoretical tenets that are explained in the following.

Lasswell's communication model (Lasswell, 1948) is a widespread model to conceptualize communication. Lasswell (1948) breaks down the task of describing communication into five different questions: *Who? Says What? In Which Channel? To Whom? With What Effect?* Even though there are more modern and complex theories to communication, we intend to focus on the main building blocks and refrain from analyzing how constructs like feedback or noise (McQuail & Windahl, 1981) affect the communication process. Lasswell was a strong advocate for the analysis of communication and flows of information with respect to its impact on public policy and addressed potential influence by digital technologies at a very early stage (Lasswell, 1972).

The work by Aggarwal & Wu (2003) provides information on the communicator roles involved in FFN fraud schemes. The authors identified that several of such efforts were undertaken by larger teams with different roles involved, e.g. insiders and brokers, but also external writers like newspaper columnists.

Expanding on their work and Lasswell's model it is relevant to understand the "Why?", i.e., motives or intent of market manipulators. Becker's (1968) economic model of crime implies that crime is more likely to be committed if actors perceive the expected benefits to exceed the costs. Hence, policies that are put in place like trading rules or punishment, are a highly relevant factor to inhibiting crime. Literature on financial fraud also often refers to the fraud triangle based on the work by Cressey (1953). Precursors to fraudulent activity are perceived opportunity, perceived pressure, and rationalization. Opportunity refers to an individual's specific set of (general) knowledge and technical skills that makes it possible for that individual to take advantage of a situation. Pressure is associated with the real or perceived risk of financial distress but also includes a desire for status or lifestyle that is not met by reality. Rationalization refers to the perceived need of fraudsters to find a justification for why they enact in the fraud scheme (Fisher, 2015).

How disinformation and fake news can be used by fraudsters to manipulate their audience is explained by the information manipulation theory (IMT) (McCornack, 1992) which distinguishes four communication principles that are being used in deceptive behavior: information can be exaggerated or understated to hide or distort the truth; the quality of the information can be altered or not be true at all; information can be taken out of context; information can be communicated ambiguously to confuse the reader. Kogan et al. (2021) apply linguistic analysis to FFN content indicating how these communication principles are applied in financial fraud. In addition to unique linguistic characteristics, we borrow from research on financial journalism to further classify the news content. We expect to identify characteristics that are very specific to disinformation in financial markets, e.g., macroeconomic data and trends or corporate news (Timmermans, 2019).

On the receiver's side, behavioral science sheds light on why market participants can fall victim to disinformation or make irrational financial decisions. Product liability theory, for example, shows the influence of cognitive biases on economic agents' incentives (Hanson and Kysar, 1999). DiFonzo and Bordia (1997) demonstrate this through a simulation study in which they show how news manipulation can distort rational trading behavior even when the credibility of the news source is questionable.

4. Method

In our research, the first step was to create a dataset consisting of FFN scheme descriptions. Subsequently, we developed a taxonomy of FFN schemes utilizing the method proposed by Nickerson et al. (2013). Finally, we conducted an evaluation and demonstrated its potential application in the context of advancing the configuration and development of fraud detection systems. Figure 1 summarizes our research methodology.

4.1. Data acquisition

We utilized the SEC litigation database (SEC, 2023) for extracting cases on fraudulent schemes. SEC litigation releases (LRs) provide a rich source of data on fraudulent financial activities, as they are well-documented and verified enforcement actions on market manipulation. Furthermore, they provide detailed

descriptions of involved entities, activities, impacts, and outcomes. In total, we screened through all LRs on the SEC website from 1995 to 2022 resulting in ca. 11,000 releases and ca. 65,000 related documents e.g., complaints or proceedings.

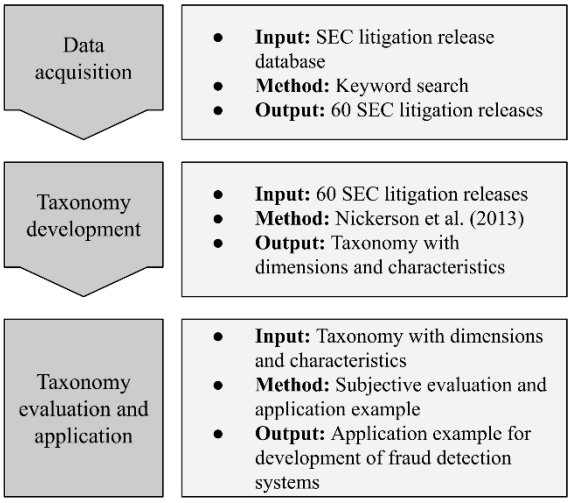

Figure 1. Overview of research design.

To select relevant cases from the SEC litigation database, we applied a keyword search using the following set of keywords based on terms from related literature on financial fake news: *fake news, false news, disinformation, misleading articles, misleading news, fake article, fake information, fake statements*. Our selection of keywords was narrowed down to select schemes that involved the use of FFN to execute a scam or fraud of market manipulation. We found 107 SEC filings related to our keywords. 28 of these filings were removed as duplicates because they were identified in multiple of our keyword searches. An additional 19 litigations found were removed, as they were not related to fake news but rather incidental cases of misinformation. Our final selection consisted of 60 unique LRs describing 60 FFN schemes.

Our sample of LRs contain fraud schemes ranging from 1983 to 2022, that were carried out for about three years on average. Most of these cases were executed after the year 2000, indicating an increased frequency of financial fraud cases in the more recent years. The amount scammed in the fraudulent schemes ranges from 350 dollars to 8.5 billion dollars, demonstrating a wide variety of scam sizes. Frauds that scam a very large amount often include multiple events over a long period of time such as 18 years for a 8.5 billion dollars fraud. However, the average scam amount lies at 181 million dollars with most scams falling into the million range.

4.2. Taxonomy development

We develop our taxonomy employing the methodology proposed by Nickerson et al. (2013), defining taxonomies as systems for groupings based on common dimensions. This method has been used extensively in the field of information systems (IS) research, for example to provide general taxonomies of financial market manipulations (Siering et al., 2017). Using this method increases our methodological rigor compared to an ad-hoc approach to taxonomy development (Nickerson et al. 2013). We consider objects as individual disinformation-driven fraud schemes and their dimensions serve to outline their distinctive characteristics. As meta-characteristic, we consider the disinformation techniques used in financial fraud, including for example participants and effects. We follow an iterative approach, where each iteration can be based on the conceptual-to-empirical or the empirical-to-conceptual approach (Nickerson et al. 2013). After each iteration, a taxonomy is derived consisting of

$$T = \{D_i, i = 1, \ldots, n \mid D_i = \{C_{ij}, j = 1, \ldots, k_i; k \geq 2\}\}$$

Where T describes the taxonomy with a set of n dimensions D_i, consisting of k_i exclusive characteristics C_{ij}, which are mutually exclusive and collectively exhaustive. The approach ends, when objective and subjective criteria have been fulfilled. As *objective* criteria, we require (a) the dimensions and characteristics to be mutually exclusive and collectively exhaustive to cover the diversity of FFN schemes, (b) require each characteristic to occur once in a FFM scheme in our sample, (c) no dimension or characteristic has been changed in the last iteration of our development. As *subjective* criteria, we require the taxonomy to be concise, robust, comprehensive, extendible, and explanatory (Nickerson et al., 2013). A summary of the dimension development is visualized in Figure 2.

4.2.1. First iteration: Using the findings of our theoretical background, we first applied the conceptual-to-empirical approach as a starting point to probe against the SEC litigation cases. We utilized the communication dimensions proposed by Lasswell (1948) to differentiate the communication patterns underlying different fraudulent schemes. Additionally, we built on the fraud triangle inspired by Cressey (1953) to structure the motivation dimension of our taxonomy and made use of the findings by Aggarwal & Wu (2003) with respect to the various roles expected to be involved on the sender side. Timmermans (2019) work on financial journalism served as reference on which content to expect in financial fake news. The IMT (McCornack, 1992) provided a theoretical foundation to

categorize the type of disinformation that is utilized for fraudulent schemes. Lastly, the analysis of linguistic features as applied by Kogan et al. (2021) motivated a more thorough look at the style of writing applied to the FFN content. To complete our first iteration of our taxonomy, we included the cognitive bias dimension as we assumed the disinformation used in financial fraud is encouraging specific irrational (trading) behavior by the audience making use of such biases. Table 1 summarizes our initially proposed dimensions for the taxonomy.

Table 1. Proposed taxonomy dimensions.

Dimensions	Source	Description
Motivation to Commit Fraud	Cressey (1953)	Why do the senders engage into a disinformation campaign?
Sender	Lasswell (1948); Aggarwal & Wu 2003)	Who is involved on the sender side?
Content	Lasswell (1948); Timmermans (2019)	What is the content of the message?
Type of Disinformation	McCornack (1992)	How is the information manipulated?
Linguistic Features	Kogan et al. (2021)	Which linguistic specifics are applied?
Channel	Lasswell (1948)	Which channels are used to disseminate the message?
Receiver	Lasswell (1948)	Who is the receiver?
Cognitive Bias	Hanson and Kysar (1999)	Which cognitive bias is targeted on the receiver side?
Effect	Lasswell (1948)	What is the (intended) effect of the message?

4.2.2. Second iteration: In our second iteration, we followed the empirical-to-conceptual approach starting with a random subset of 15 articles from our dataset of LRs. We applied the initial taxonomy as a guiding scheme for coding the releases by five researchers independently. Each of the researchers was assigned a random set of 3 articles. We used the free and open-source software *taguette*[1] to coordinate the coding activities. We discussed the initial results to assess if the initial taxonomy can be applied to the dataset.

The research team noted that all LRs in the subset provide insufficient information on the linguistic cues that senders applied in FFN articles. Since this does not allow us to empirically support our assumptions on this dimension, we removed the dimension and characteristics from the taxonomy. Several LRs in the subset were spanning multiple years and iterations in their execution. We therefore added a temporal dimension to differentiate such cases from one-time events. Furthermore, we changed the names of the sender and receiver dimensions into sender roles and receiver roles, to emphasize the various roles participants may play in FFN schemes. We checked our ending conditions and agreed that neither the objective nor subjective criteria were fulfilled at this point.

4.2.3. Third iteration: Following the second iteration, we increased our sample of articles to include the full set of LRs. We distributed all 60 articles randomly across the five researchers under the condition that each researcher had to review a similar number of pages (318 pages each). Findings from the second iteration affected both characteristics but also dimensions of our taxonomy. With respect to characteristics, we noted that the LRs were providing too little information to structure the *Motive/Intent* dimension along the fraud triangle, especially with respect to pressure and the personal background of the senders, but instead, provided unique characteristics on the motive of fraudsters. We further decided to deviate from the four elements of the IMT in the *Type of Disinformation* characteristics.

At the dimension level we opted to add the underlying type of fraud utilizing FFN, such as pump-and-dump or pyramid scheme. We also added the type of asset being targeted by disinformation schemes, given that these appear to vary significantly, ranging from cryptocurrencies to securities or stocks. A lack of access to the complete FFN articles disseminated in most LRs precluded our ability to analyze the specific *Cognitive Bias* leveraged. Since we identified the need for changes in the taxonomy, we entered in the fourth iteration.

4.2.4. Fourth iteration: For the fourth iteration, we provided each member of the research team with the coding of another researcher with the task to reflect on the quality of the results of the third iteration. We also checked how far the current results met the ending conditions. We made minor refinements to the description and naming of the characteristic to increase the precision and understanding of the terms. The research team jointly considered the taxonomy mutually exclusive and collectively exhaustive. Its characteristics occur only once per dimension, and we had no structural changes to dimensions or characteristics in this iteration. The research team was also confident to meet the subjective criteria we applied to our ending conditions. Therefore, we conclude the taxonomy development with our fourth iteration.

[1] https://www.taguette.org/

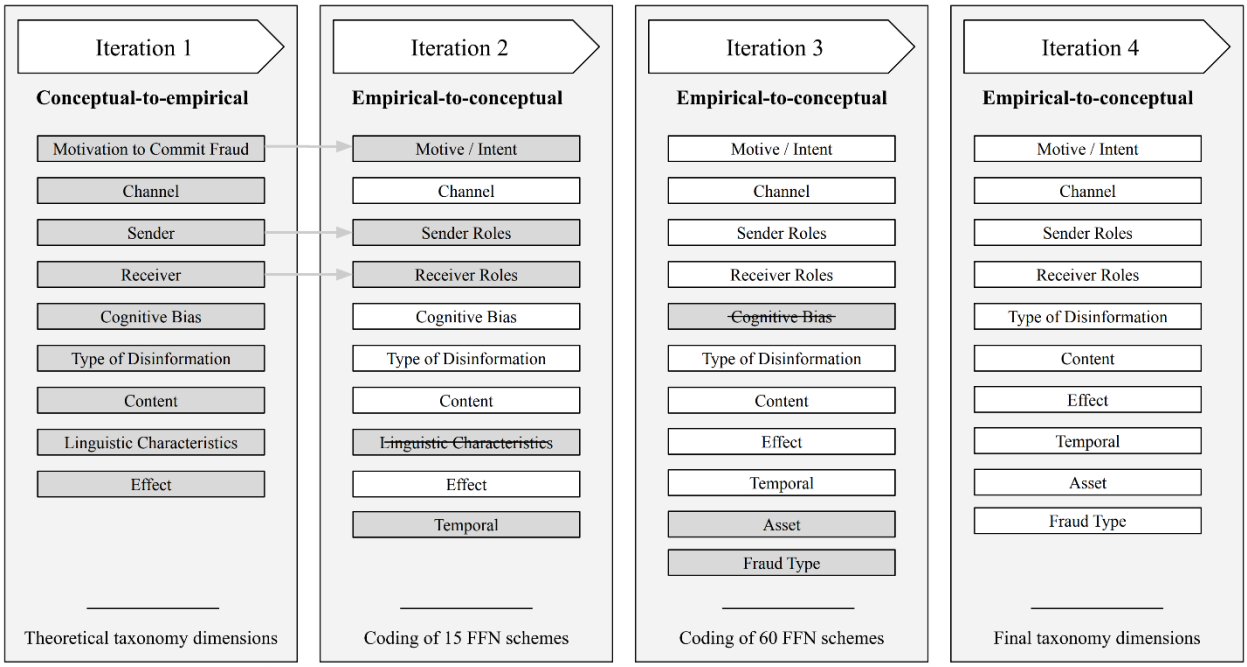

Figure 2. Iterative taxonomy dimension development.

5. Results

5.1. Taxonomy of FFN schemes

Our proposed taxonomy of FFN schemes includes 10 dimensions (see Table 2). Each dimension represents a particular aspect of FFN and provides a robust tool for understanding its structure, prevalence, and potential impact.

Motive/Intent: At the core of any FFN scheme is an intent or motive. This may be self-benefit, the concealment of dubious activity, or a tactical move to damage an asset for personal gain, such as short selling. Uncovering these underlying motives helps to understand the nature of FFN schemes.

Channel: FFN schemes feature a wide range of distribution channels. From conventional media such as print, broadcast, and news websites to digital channels such as social media platforms, messaging applications, blogs, forums, and even direct communication channels such as emails or text messages, each channel has its own impact on the reach and impact of disinformation.

Asset: Targeted assets in FFN schemes are remarkably diverse, ranging from traditional financial instruments like stocks and securities to newer innovations like cryptocurrencies.

Sender Roles: Identifying the entities responsible for creating and disseminating FFN provides valuable insight into their origins, potential biases, and credibility. The taxonomy identifies several possible senders, including professional traders, promotion firms, insiders, and external authors.

Receiver Roles: The receivers or victims of FFN play a critical role in determining their overall impact. This includes a wide range of market participants such as institutional and retail investors, analysts, employees, and clients. Identifying such groups helps in developing appropriate safeguards.

Temporal: The time factor is also very relevant in FFN schemes. Disinformation can be disseminated as a one-time event or as part of an ongoing campaign, each of which has different implications for the extent and duration of its impact.

Type of Disinformation: FFN schemes include a variety of disinformation types, such as outright false news, rumors, exaggerated or misleading details, manipulated content, and omission of important information. Recognizing these variations enables a more nuanced approach to detection and mitigation.

Content: Specific FFN content varies widely and includes transactions (such as deals, mergers), scientific breakthroughs, management changes, financial reports, partnerships, testimonials, and other important market events. Each content type can affect the credibility and perceived impact of the FFN.

Effect: Finally, the taxonomy considers the real-world consequences of FFN, such as fluctuating asset prices, changing trading volumes, or triggered corporate actions. Understanding these effects is critical to understanding the broader impact of FFN on market integrity.

Table 2. Taxonomy of FFN schemes.

Dimension	Description	Characteristics	
Motive / Intent	The underlying reasons and objectives that motivate the dissemination of FFN.	• Self-Benefit • Damage Asset • Conceal Activities	
Channel	Relates to the medium through which the FFN is propagated.	• Traditional Media (print, broadcast) • Social Media (platforms, messaging, blogs, forums)	• Direct Communication (e-mail, text messages) • Websites • Videos (platforms)
Sender Roles	Represents the identity and role of the entities that create and disseminate FFN.	• PT = Professional Trader • RT = Retail Trader • EA = External Author • IN = Insider • BR = Broker	• UW = Underwriter • PF = Promotion Firm • LS = Large Shareholder • MM = Market Maker • OW = Owner
Receiver Roles	Describes the entities that receive and potentially act upon the FFN.	• II = Institutional Investors • PT = Professional Trader • RT = Retail Trader	• EM = Employees • CL = Clients • AN = Analysts
Type of Dis-information	Refers to the nature of the fake news itself.	• False News (e.g., false, or fabricated content) • Rumors (e.g., speculation or gossip)	• Manipulated News (e.g., over / understating) • Omissions (e.g., in reports)
Content	Describes the specific content of the FFN.	• Transaction (e.g., deal, merger, spin-off, sale, acquisition) • Breakthrough (e.g., scientific discovery, trial study) • Management (e.g., new hires) • Financial (e.g., revenue growth)	• Partnership (e.g., customers, suppliers) • Testimonial (e.g., manager interviews) • Reporting (e.g., accounting, filings, advisory statements)
Effect	Represents the actual or potential impact of the FFN scheme.	• Price change • Trading increase	• Corporate action (e.g., transaction canceled)
Asset	Refers to the financial instrument targeted by FFN.	• Stocks • Securities	• Cryptocurrencies
Temporal	Considers the temporal diffusion of the FFN scheme.	• Single Event • Long-Term Scheme	
Fraud Type	Refers to the underlying fraudulent scheme where disinformation is used.	• Pump-and-dump • Paid Promotion • Kickback Scheme	• Pyramid Scheme • Ponzi Scheme • Short Attack

5.2. Taxonomy evaluation

In this section, we provide the subjective evaluation of the taxonomy classifying FFN schemes following the criteria from Nickerson et al. (2013).

Conciseness: According to Nickerson et al. (2013), too detailed a taxonomy weakens their effectiveness. A taxonomy that tries to cover all possible dimensions and characteristics can overwhelm the user's cognitive abilities. With 10 dimensions and at maximum 10 characteristics per dimension, this taxonomy is manageable and is unlikely to overwhelm users' cognitive load.

Robustness: A robust taxonomy can clearly distinguish between different objects based on their characteristics and dimensions. Our FFN taxonomy allows for a clear distinction between the variety of FFN schemes from our dataset, as each dimension comprises characteristics which, if changed, result in a substantially different approach to fraud.

Comprehensive: A comprehensive taxonomy should ideally cover all dimensions and objects in its scope. Considering real-world cases and theoretical background ensured a broad coverage. Our taxonomy,

developed both conceptually and empirically, covers all common FFN schemes and all relevant dimensions that characterize these types in our dataset of 60 unique LRs and is therefore comprehensive.

Extensibility: A taxonomy should be adaptable to future developments as new objects or dimensions expand its scope. Although it is difficult to predict future FFN schemes, our taxonomy is mostly built on non-contemporary dimensions grounded in theoretical tenets that can be extended with new elements.

Explanatory power: Finally, a taxonomy should facilitate understanding of its scope without the need to describe each object in detail. Our FFN taxonomy provides a clear framework for understanding the different FFN schemes and their properties. It sets out what market surveillance authorities should consider when monitoring and countering financial fake news.

5.3. Taxonomy application

To illustrate how our taxonomy can be used for real cases, we apply it to an exemplary litigation case. In addition, we explain how our FFN scheme taxonomy can be used to develop and improve fraud detection systems.

Analyzing one of the pump-and-dump scheme litigations (SEC, 2006), we extract the characteristics for the dimensions of our FFN taxonomy. This case involves a long-term fraud scheme (temporal) that began in late 2004 and continued through March 2006. Two retail traders (sender role) aggressively pushed retail investors (receiver role) to buy microcap stocks of a company immediately based on false data (type of misinformation) to increase the stock's price. The defendants illegally gained over $873,000 in profits showing a clear motive of self-benefit (motive/intent). They used multiple channels to spread their disinformation, such as social media, particularly internet message boards, and direct communication with specific investors by sending emails to internet user groups (channel). The messages and emails involved transaction-related misinformation about significant business contracts, mergers and alliances or partnerships with major corporations (content). The messages resulted in increased trading volume and a stock price increase (effect).

Our taxonomy can be used as a guide for the configuration and development of fraud detection systems. Given the example disinformation-driven fraud scheme described before (SEC, 2006), an effective fraud detection system should therefore analyze various sources of financial news. The intentions behind such an FFN scheme can be different, e.g., self-benefit, as the case for pump-and-dump schemes. Therefore, an effective fraud detection system should consider various possible motives to appropriately understand the context of the disinformation. It especially needs to consider both positive and negative polarity of content, as self-benefit and damage assets result in different FFN polarities. In addition, the effects of FFN can vary significantly, including for example price changes or increased trading volume. For example, in the case of pump-and-dump schemes, a rapidly increasing price and trading volume might be indicative of fraudulent schemes. Therefore, fraud detection systems should be designed to monitor these different effects and detect anomalies that might indicate possible FFN schemes. The taxonomy also differentiates between different sender roles, such as retail traders, promotion firms, underwriters, and insiders. Identifying these roles for articles could help fraud detection systems identify FFN sources and understand the context of disinformation. Moreover, the temporal dimension of our taxonomy, which distinguishes between single events and long-term schemas, necessitates the incorporation into fraud detection systems. The mechanisms needed to detect long-term running disinformation schemes differ significantly from those required for disinformation related to single events.

A look at a previous study developing a fraud detection system for financial disinformation detection (Zhang et al., 2022), can confirm the usefulness of our taxonomy. This study considers dimensions for FFN detection, such as sender properties and the information content. However, it is for example missing to monitor various channels and does only consider single event fraud schemes.

In summary, using our FFN taxonomy when configuring and developing fraud detection systems can provide valuable insights for the design and improvement of FFN detection systems. The taxonomy is consistent with the design of existing systems and provides more comprehensive guidance for future system improvements.

6. Discussion

As demonstrated by the application of our taxonomy in the context to develop and improve fraud detection systems, our taxonomy serves as a practical tool in categorizing schemes of disinformation-driven financial fraud. The comprehensiveness of the taxonomy, derived from both existing literature and analysis of actual LRs, provides a holistic understanding of such schemes.

However, we are aware of some limitations. First, our case data is limited to cases listed in the SEC's litigation filings. This results in likely missing a number of fraud cases that may not have gone to court, particularly those involving newer assets such as non-

fungible tokens (NFTs). Second, the nature of disinformation tactics is inherently dynamic and constantly evolving, for example with the emergence of new forms of social media such as Discord and TikTok. This poses an ongoing challenge to maintain the comprehensiveness of the taxonomy. Finally, while the taxonomy helps to configure and develop fraud detection systems for detecting disinformation schemes, certain dimensions such as sender roles can prove difficult for automatic detection, as senders might act anonymously. Furthermore, our taxonomy does not provide concrete guidelines for the development of fraud detection systems, but rather guidance on which dimensions and characteristics should be considered.

However, these limitations also provide motivation for future research. It would be valuable to use the insights from our taxonomy to derive concrete design principles for fraud detection systems that specifically address disinformation fraud. This could be complemented by the instantiation of fraud detection system design instances, which then can be evaluated for their usefulness, especially in digital governments. In addition, the taxonomy could be used to derive actionable recommendations for market surveillance authorities to effectively combat financial fraud caused by disinformation.

7. Conclusion

In summary, the research conducted in this study develops a taxonomy of the use of disinformation in financial fraud. By examining a wide range of cases and founded in theoretical tenets, our taxonomy contributes significantly to the understanding of this field. The taxonomy not only helps to classify these complex fraudulent schemes, but also serves as an important tool to guide the configuration and development of fraud detection systems for market surveillance authorities. However, our findings also confirm the complexity of efficient fraud detection systems due to the multi-dimensional facet of fraudulent schemes.

8. Acknowledgments

This work is part of the research project AFFIN funded by the German Federal Ministry of Education and Research (Grant no.: 01IS21045B).

9. References

Aggarwal, R. K., & Wu, G. (2003). Stock Market Manipulation—Theory and Evidence. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.474582

Aitken, M., Cumming, D., & Zhan, F. (2015). Exchange trading rules, surveillance and suspected insider trading. *Journal of Corporate Finance*, *34*(C), 311–330.

Becker, G. S. (1968). Crime and Punishment: An Economic Approach. *Journal of Political Economy*, *76*(2), 169–217.

Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. *Government Information Quarterly*, *27*(3), 264–271. https://doi.org/10.1016/j.giq.2010.03.001

Black, B. (2001). The legal and institutional preconditions for strong securities markets. *UCLA Law Review. University of California, Los Angeles. School of Law*, *48*, 781–855.

Charalabidis, Y., Loukis, E., Alexopoulos, C., & Lachana, Z. (2019). The Three Generations of Electronic Government: From Service Provision to Open Data and to Policy Analytics. In I. Lindgren, M. Janssen, H. Lee, A. Polini, M. P. Rodríguez Bolívar, H. J. Scholl, & E. Tambouris (Eds.), *Electronic Government* (pp. 3–17). Springer International Publishing. https://doi.org/10.1007/978-3-030-27325-5_1

Chen, Y.-C. (2012). A comparative study of e-government XBRL implementations: The potential of improving information transparency and efficiency. *Government Information Quarterly*, *29*(4), 553–563. https://doi.org/10.1016/j.giq.2012.05.009

Clarke, J., Chen, H., Du, D., & Hu, Y. J. (2020). Fake news, investor attention, and market reaction. *Information Systems Research*, 32(1), 35-52.

Comerton-Forde, C., & Rydge, J. (2006). Market Integrity and Surveillance Effort. *Journal of Financial Services Research*, *29*(2), 149–172. https://doi.org/10.1007/s10693-006-5923-z

Cressey, D. R. (1953). *Other people's money; a study of the social psychology of embezzlement*. Free Press.

Dawes, S., & Helbig, N. (2015). The Value and Limits of Government Information Resources for Policy Informatics. In E. W. Johnston (Ed.), *Governance in the Information Era: Theory and Practice of Policy Informatics* (pp. 25–34). Routledge.

DiFonzo, N., & Bordia, P. (1997). Rumor and prediction: Making sense (but losing dollars) in the stock market. *Organizational Behavior and Human Decision Processes*, *71(3)*, 329–353. https://doi.org/10.1006/obhd.1997.2724

Dupuis, D., Smith, D., & Gleason, K. (2023). Old frauds with a new sauce: digital assets and space transition. *Journal of Financial Crime*, *30*(1), 205-220.

Fisher, K. (2015). The Psychology of Fraud: What Motivates Fraudsters to Commit Crime? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2596825

Fong, B. (2021). Analysing the behavioural finance impact of 'fake news' phenomena on financial markets: a representative agent model and empirical validation. *Financial Innovation*, 7(1), 1-30.

Gil-Garcia, J. R., & Flores-Zúñiga, M. Á. (2020). Towards a comprehensive understanding of digital government success: Integrating implementation and adoption factors. *Government Information Quarterly*, *37*(4), 101518. https://doi.org/10.1016/j.giq.2020.101518

Hanson, J. D., & Kysar, D. A. (1999). Taking Behavioralism Seriously: The Problem of Market Manipulation. *New York University Law Review*, *74*(3), 630-749.

Harrison, T. M., & Luna-Reyes, L. F. (2022). Cultivating trustworthy artificial intelligence in digital government. *Social Science Computer Review*, 40(2), 494-511.

Kogan, S., Moskowitz, T. J. & Niessner, M. (2021). Social Media and Financial News Manipulation Available at SSRN: https://ssrn.com/abstract=3237763 or http://dx.doi.org/10.2139/ssrn.3237763

Lasswell, H. D. (1948). The structure and function of communication in society. In Bryson (Ed.), *The Communication of Ideas*. Harper and Brothers.

Lasswell, H. D. (1972). Communications Research and Public Policy. *The Public Opinion Quarterly*, *36*(3), 301–310. http://www.jstor.org/stable/2747438

Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., Metzger, M. J., Nyhan, B., Pennycook, G., Rothschild, D., Schudson, M., Sloman, S. A., Sunstein, C. R., Thorson, E. A., Watts, D. J., & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094–1096.

McCornack, S. (1992). Information manipulation theory. *Communication Monographs*, *59*, 1–16. https://doi.org/10.1080/03637759209376245

McQuail, D., & Windahl, S. (1981). *Communication Models for the Study of Mass Communications*. Longman Publishing Group.

Mohankumar, P., Kamal, A., Singh, V. K., & Satish, A. (2023). Financial Fake News Detection via Context-Aware Embedding and Sequential Representation using Cross-Joint Networks. *2023 15th International Conference on COMmunication Systems & NETworkS (COMSNETS)*, 780-784.

Moloney, N. (2012). The legacy effects of the financial crisis on regulatory design in the EU. In E. Ferran, J. G. Hill, J. Coffee John C., & N. Moloney (Eds.), *The Regulatory Aftermath of the Global Financial Crisis* (pp. 111–202). Cambridge University Press. https://doi.org/10.1017/CBO9781139175821.003

Moser-Plautz, B., & Schmidthuber, L. (2023). Digital government transformation as an organizational response to the COVID-19 pandemic. *Government Information Quarterly*, *40*(3), 101815. https://doi.org/10.1016/j.giq.2023.101815

Nickerson, R. C., Varshney, U., & Muntermann, J. (2013). A method for taxonomy development and its application in information systems. *European Journal of Information Systems*, 22(3), 336-359.

Scholl, H. J. (2022). The Digital Government Reference Library (DGRL). Versions 18.0—18.5. Retrieved from http://faculty.washington.edu/jscholl/dgrl/

SEC. (2006). *SEC Complaint*. https://www.sec.gov/litigation/complaints/2006/comp19642.pdf

SEC. (2023). *Litigation Releases*. https://www.sec.gov/litigation/litreleases.htm

Siering, M., Clapham, B., Engel, O., & Gomber, P. (2017). A taxonomy of financial market manipulations: establishing trust and market integrity in the financialized economy through automated fraud detection. *Journal of Information Technology*, 32(3), 251-269.

Siering, M. (2019). The economics of stock touting during Internet-based pump and dump campaigns. *Information Systems Journal*, *29*(2), 456–483. https://doi.org/10.1111/isj.12216

Siering, M., Muntermann, J., & Grčar, M. (2021). Design Principles for Robust Fraud Detection: The Case of Stock Market Manipulations. *Journal of the Association for Information Systems*, 22(1), 156-178.

Søe, S. O. (2021). A unified account of information, misinformation, and disinformation. *Synthese*, 198(6), 5929-5949.

Tandoc Jr, E. C., Thomas, R. J., & Bishop, L. (2021). What is (fake) news? Analyzing news values (and more) in fake stories. *Media and Communication*, *9*(1), 110-119.

Timmermans, J. (2019). Financial Journalism. In *Oxford Research Encyclopedia of Communication*. https://doi.org/10.1093/acrefore/9780190228613.013.812

Vosoughi, S., Roy, D., & Aral, S. (2018). The spread of true and false news online. *Science*, 359(6380), 1146-1151.

Zhang, X., Du, Q., & Zhang, Z. (2022). A theory-driven machine learning system for financial disinformation detection. *Production and Operations Management*, *31*(8), 3160-3179.

Zhi, X., Xue, L., Zhi, W., Li, Z., Zhao, B., Wang, Y., & Shen, Z. (2021). Financial Fake News Detection with Multi fact CNN-LSTM Model. *2021 IEEE 4th International Conference on Electronics Technology*, 1338–1341. https://doi.org/10.1109/ICET51757.2021.945092