



---

## Red Flags in Online Financial Trading: Prospect and Challenges of Online Financial Traders in Oshodi Isola Local Government Area, Lagos State, Nigeria

Umar ISAH<sup>a\*</sup>, Suleman Ahmed WAN<sup>b</sup>, Abdulrahman IBRAHIM<sup>c</sup>, Salihu Liman WAN<sup>d</sup>

<sup>a</sup>*Department of Sociology, Faculty of Social Science, Bayero University, Kano, Nigeria*

<sup>b</sup>*Department of Sociology, Faculty of Social Science, Ahmadu Bello University, Zaria, Nigeria*

<sup>c</sup>*Department of Sociology, Ahmadu Bello University Zaria, Distance Learning Center, Nigeria*

<sup>d</sup>*Department of General Studies, Auchi Polytechnic, Auchi, Nigeria*

\*Corresponding author: sawan@abu.edu.ng

### Abstract

The rising incidence of online financial market fraud presents critical challenges to traders, investors, and regulatory bodies, particularly within Oshodi-Isolo Local Government Area of Lagos State, Nigeria. This study examined the prospects and challenges of identifying red flags in online financial trading among traders in the area. The research was anchored on social engineering theory and persuasion theory, and it adopted a mixed-methods survey design. A total of 116 online traders were selected through multi-stage sampling to respond to structured questionnaires, while six respondents (four experienced traders and two investors) were purposively selected for in-depth interviews. Findings revealed that many participants engaged in online trading out of curiosity, driven by limited investment knowledge and speculative motives. Major challenges identified included the prevalence of fake brokers and trading platforms, hidden transaction fees, delayed withdrawals, poor customer support, and frequent exposure to phishing and hacking attempts. These issues reflect a trading environment marked by fraudulent activities, weak accountability, and elevated cyber risks. The study also found a general reluctance to report fraudulent experiences, leading to underreporting that hinders effective regulatory intervention. It was therefore recommended that stronger regulatory oversight, enhanced digital literacy, improved consumer protection frameworks, and simplified fraud reporting mechanisms are essential to safeguard traders and investors. Furthermore, regulatory agencies should prioritize building trust, curbing fraudulent practices, and promoting a safer digital trading ecosystem. Finally, emphasis should be placed on practical training to help traders recognize subtle red flags and to foster self-control and informed decision-making in financial transactions.

Keywords: online, traders, digital, red, flags

**Acknowledgments:** My profound gratitude goes to all participants in Oshodi-Isolo LGA, Lagos State, for their invaluable insights into online financial trading. Special thanks to the traders and investors who shared their experiences regarding fraudulent red flags and cyber risks.

This study's success was made possible by your cooperation. I hope these findings contribute to stronger regulatory oversight, enhanced digital literacy, and a safer trading ecosystem for all. Thank you for your trust and contribution.

**For citation:**

Isah. U., Wan, S. H., Ibrahim, H., Wan, S. L. (2026). Red Flags in Online Financial Trading: Prospect and Challenges of Online Financial Traders in Oshodi Isola Local Government Area, Lagos State, Nigeria. *Radinka in Social Science*, 1(2), 58-69.

**Introduction**

Globally, the rapid growth of online financial trading platforms has created new opportunities for wealth creation but has also exposed traders and investors to fraud, cyber risks, and systemic vulnerabilities (Meniago, 2025). Many traders, particularly in developing economies, operate in fragile digital environments characterized by weak regulatory oversight, poor investor education, and limited protection mechanisms (Donadelli & Van Der Heijden, 2024). Hence, traders often face challenges ranging from hidden transaction fees to outright fraudulent schemes (Trotta et al., 2026). Despite existing literature on financial fraud, there is a notable lack of localized studies focusing on the specific red flags indicative of fraud within the unique socio-economic and cultural context of Lagos State (Nguyen Thanh & Phan Huy, 2025).

Many individuals remain unaware of the warning signs, leading to significant financial losses and eroding trust in digital financial systems coupled with lack of detailed knowledge about the mechanics and warning signs (Moura et al., 2025). For Oshodi-Isolo, which is densely populated and likely to have many people using smartphones/internet, this gap may be quite pronounced. The transferability depends on local educational levels, internet literacy, socio-economic status (Ika Sari et al., 2024). Also, online/mobile channel fraud and ATM fraud have significant negative effects on bank performance showing correlation between bank fraud (both monetary loss and number of successful fraud cases) and economic growth negatively affecting GDP (Đorđević et al., 2025), through victimisation from Ponzi or pyramid schemes, cryptocurrency-related scams, forex scams, etc. Again, as digital banking, mobile money, online investment, and internet usage grow (Eriksson et al., 2021), so do the opportunities for fraud, with specific scams (investment fraud, phishing, crypto-scams) expanding in prevalence (Jules & Arnold, 2022).

Fraud poses not only direct financial losses to individuals, but also undermines trust in financial institutions and services, negatively affecting bank performance, possibly reducing uptake of financial technology, and having broader economic growth impacts. Weak linkages among regulatory agencies (CBN, SEC, EFCC, NCC, etc.), lack of strong legal sanctions or prosecution, limited resources, and insufficient local capacity to detect, investigate, and punish fraudsters (Ljungqvist & Sonesson, 2022). Hence, the study is set to examine the prospect and challenges of red flags in online financial trading to online financial traders in Oshodi Isola Local Government Area, Lagos State, Nigeria.

**Methodology***Location of the study area*

Oshodi-Isolo (Yoruba: Oṣòdì-Ìsọlò) is a Local Government Area (LGA) in the Ikeja Division of Lagos State, Nigeria, with an estimated population of 931,300 as of 2022 and a population density of approximately 21,000 persons per square kilometer. The LGA comprises eleven wards, including Oshodi/Bolade, Orile Oshodi, Mafoluku, Shogunle, Isolo, Ajao Estate, Ilasamaja, Okota, Ishagatedo,

Oke-Afa, and Ejigbo. In recent years, the area has witnessed a growing prevalence of online financial market fraud, largely driven by the expansion of digital banking and online investment activities. This has led to an upsurge in phishing, Ponzi schemes, and other cyber-enabled frauds, resulting in substantial financial losses for individuals.

Nigerian authorities, particularly the EFCC, have prosecuted individuals and firms involved in illegal capital market operations, identity theft, and cyberterrorism, emphasizing how fraudsters exploit stolen information for financial gain and economic disruption. Common schemes in the area include fraudulent investment promotions on social media that promise unrealistically high or fixed returns in sectors such as agriculture or foreign exchange trading. For example, cases involving companies like *Green Eagles Agri Business Solutions Limited* illustrate how investors are deceived through Ponzi-style mechanisms, where funds from new participants are used to pay earlier investors, ultimately leading to collapse and widespread losses.

### *Research design*

The study employed a survey research design and adopted a mixed-methods approach, combining both quantitative and qualitative techniques. Structured questionnaires were administered to online traders, while in-depth interviews (IDIs) were conducted with relevant stakeholders, including bank managers and experienced investors in the study area. This design was considered appropriate for collecting comprehensive data on the red flags in online financial market fraud in Oshodi-Isolo Local Government Area, Lagos State. The mixed-method approach provided a deeper understanding of participants' experiences and perceptions, thereby enhancing the validity and richness of the findings.

### *Sample size*

The study sample comprised 116 respondents drawn from the population of online traders in Oshodi-Isolo. Out of this number, 110 respondents participated in the questionnaire survey, while five key informants (four experienced online traders and two online investor) participated in in-depth interviews. Given the large population size and geographical spread of Oshodi-Isolo, it was not feasible to include all traders; hence, a representative sample was selected.

### *Sampling techniques*

A multi-stage sampling technique was adopted to select participants for the study. Oshodi-Isolo Local Government consists of eleven (11) wards, namely: Oshodi/Bolade, Orile Oshodi, Mafoluku, Shogunle, Shogunle/Alasia, Isolo, Ajao Estate, Ilasamaja, Okota, Ishagatedo, and Oke-Afa/Ejigbo. Stage One: Out of the eleven wards, five wards—Oshodi/Bolade, Orile Oshodi, Mafoluku, Isolo, and Ajao Estate were selected using simple random sampling. Stage Two: The selected wards were treated as clusters for the study. Stage Three: Using systematic sampling, two streets were selected from each ward, giving a total of ten streets. Stage Four: From each selected street, eleven respondents were chosen through the snowball (chain-referral) method, resulting in 110 participants for the questionnaire survey. Also, purposive sampling was employed to select four experienced online traders and one online investor for the in-depth interviews, as they possessed relevant knowledge and experience on the subject matter. This brought the total number of study participants to 116.

### *Method of data collection*

The study employed both quantitative and qualitative methods of data collection to obtain comprehensive and reliable information from respondents. Data were gathered from primary and secondary sources. Primary data were obtained through the administration of structured questionnaires and In-Depth Interviews (IDIs). A total of 110 questionnaires were administered to online traders, while in-depth interviews were conducted with four experienced online traders and one online investor. The questionnaire was designed in English and translated into Yoruba where

necessary to enhance understanding and participation. It contained both open-ended and close-ended questions, allowing respondents to provide detailed insights while ensuring measurable responses. While secondary data were sourced from relevant textbooks, academic journals, official reports, newspapers, magazines, and online publications to provide theoretical support and contextual background for the study.

#### *Method of data analysis*

The quantitative data obtained from the questionnaires were coded and analyzed using the Statistical Package for the Social Sciences (SPSS) version 24. Descriptive statistics, including frequencies, percentages, and tables, were employed to summarize and present the findings. While the qualitative data derived from interviews were translated, transcribed, and thematically analyzed to identify key patterns and insights. These findings were used to complement and interpret the quantitative results, thereby providing a more holistic understanding of the red flags in online financial market fraud in Oshodi-Isolo Local Government Area, Lagos State.

## **Results and Discussion**

### *The challenges of red flags in an online trading*

Table 1. Challenges Encountered While Trading Online

| Challenges                  | Yes (%)   | No (%)    | Total (%) |
|-----------------------------|-----------|-----------|-----------|
| Delayed withdrawal          | 65 (59.1) | 45 (40.9) | 110 (100) |
| Hidden transaction fees     | 72 (65.5) | 38 (34.5) | 110 (100) |
| Poor or no customer support | 61 (55.5) | 49 (44.5) | 110 (100) |
| Fake brokers or platforms   | 86 (78.2) | 24 (21.8) | 110 (100) |
| Hacking/phishing attempts   | 59 (53.6) | 51 (46.4) | 110 (100) |

Source: Field work, 2025

The Table 1 above shows that respondents experience a range of challenges in online trading. The most reported challenge is dealing with fake brokers or platforms (78.2%), followed by hidden transaction fees (65.5%) and delayed withdrawals (59.1%). Over half of respondents also indicated problems with poor or no customer support (55.5%) and hacking/phishing attempts (53.6%). This indicates that a majority of respondents face multiple overlapping issues, with fraudulent platforms and lack of transparency being the most significant. The prominence of fake brokers suggests weak regulation and limited due diligence among users, exposing traders to fraudulent platforms. Hidden fees and delayed withdrawals highlight non-transparent practices that erode trust and discourage participation in online trading. Poor customer service and unresolved complaints undermine user confidence and limit dispute resolution. The high percentage of hacking/phishing attempts reflects inadequate digital literacy and weak security infrastructure among traders. The combination of these challenges points to a fragile online trading environment characterized by fraud, lack of accountability, and cyber threats. Stronger regulatory oversight, user education, and reliable support systems are needed to protect investors. This aligned with an interview with investor, who revealed that:

*"One of the biggest challenges I've faced is delayed withdrawals. Sometimes it takes days before I can access my money, and that makes me feel unsafe trading online. Also, I didn't realize at first that there were so many hidden transaction fees. They deduct charges at every stage, and in the end, the profit I expected is much smaller. Sometime When I had issues with my account, the customer support was either*

*unresponsive or gave me automated answers. It feels like you're on your own when problems happen."*

In another interview with Online Investor revealed that:

*"I once registered with a broker who promised high returns, but the platform disappeared after a few months. I later discovered it wasn't registered with any regulatory body. Also, I've received fake emails and links asking me to 'verify' my trading account. If I wasn't careful, I could have lost my login details to hackers. Anytime I see a platform promising to double or triple my money in a few weeks, I know it's a red flag. Unfortunately, many people still fall for these promises."*

Furthermore, an Online Trader posited that

*"Honestly, I didn't even know we were supposed to check if a platform was regulated by SEC or CBN. Most of us just go by what friends recommend or what we see online. Some platforms don't even show who owns them or where they are based. For me, that's a clear red flag, but many people ignore it because they're desperate for profit".*

Again, an interview with Online Trader revealed that:

*A lot of people join platforms because friends or groups are trading there. The risk is that if the group is misled, everyone loses money together. The main challenge is that fraudsters are always creating new tricks. The only way to cope is to keep learning, attending financial literacy training, and being cautious of red flags."*

Table 2. On whether respondents avoid investing when notice a red flag

| Notice a Red Flag They Immediately Stop | Frequency | Percentage (%) |
|-----------------------------------------|-----------|----------------|
| Yes                                     | 92        | 83.6           |
| No                                      | 18        | 16.4           |
| Total                                   | 110       | 100            |

Source: Field Work, 2025

Table 2 above indicates that the majority of respondents, 83.6% (92 individuals), reported that they would immediately stop or avoid investing when they notice a red flag, such as unrealistic profit promises. A smaller portion, 16.4%, admitted that they would still proceed despite noticing red flags. The large majority (83.6%) demonstrates a strong protective behavior, suggesting that many respondents have developed some level of fraud awareness and take preventive action when clear red flags are spotted. The 16.4% who proceed despite noticing red flags represent a high-risk group. Their behavior may be influenced by desperation for quick profits, lack of alternatives, or overconfidence in beating the system. While most can identify and act on obvious red flags, earlier findings showed fewer respondents notice structural red flags (e.g., lack of regulation, anonymous ownership). This means awareness is still surface-level and incomplete. Financial literacy campaigns are working to some extent, but they need to address psychological factors (greed, peer pressure, risk-taking behavior) that make a minority ignore red flags. This result shows that while fraud prevention knowledge is relatively widespread, effective protection requires deeper training on subtle red flags and stronger emphasis on self-control in financial decision-making. This is in line with an interview with Online Trade, who revealed that:

*"The moment I see an investment platform promising returns like 50% in a week, I stop considering it altogether. From my experience, those are the biggest warning signs. I don't even wait to investigate further,*

*because I've learned that legitimate businesses don't make such promises. For me, once a red flag is spotted, that's the end of the conversation."*

Also, in an interview with Online Investor posited that:

*"When I notice a red flag, I don't jump in right away, but I don't discard it immediately either. I first ask around in my peer groups or check online forums to confirm if others have concerns too. If the warning signs are consistent—like lack of registration details or too-good-to-be-true profits—then I completely avoid investing. So, I rely on verification before making my final decision."*

Furthermore, Online Trade revealed that:

*"In the past, I ignored red flags and invested in a platform that eventually scammed me. Since then, I've changed my approach. Now, if I see anything suspicious, I pull back immediately. I don't wait to be convinced or tempted by the possibility of gains. My past loss has trained me to treat red flags as deal-breakers."*

Again, Online Trade opined that:

*"Sometimes I notice a red flag but still feel curious. In such cases, I avoid putting in large amounts. I might test with a very small sum, just to see how it works. But once I confirm it's unrealistic or risky, I don't continue. So I don't completely stop at first sight, but I proceed with extreme caution. My strategy is to minimize exposure."*

Another interview with Online Trade revealed that:

*"For me, unrealistic profit promises are the clearest indication of fraud. I don't waste time engaging with such platforms. I immediately block their contacts and delete their adverts. I prefer to miss out on an opportunity than risk losing my hard-earned money. Red flags are like traffic lights—when it's red, you stop."*

Table 3. Method of Verifying Platform Legitimacy

| Method of Verifying Platform Legitimacy | Frequency | Percentage (%) |
|-----------------------------------------|-----------|----------------|
| Online reviews/testimonies              | 40        | 36.4           |
| Regulation check (SEC, CBN)             | 30        | 27.3           |
| Word of mouth                           | 25        | 22.7           |
| I don't verify                          | 15        | 13.6           |
| Total                                   | 110       | 100            |

Source: Field work, 2025

Table 3 above indicates the most common method of verifying platform legitimacy among respondents is through online reviews and testimonies (36.4%), followed by regulation checks with bodies like SEC or CBN (27.3%). Another 22.7% rely on word of mouth, while 13.6% do not verify at all. This indicates that while some respondents use formal regulatory checks, a larger proportion depend on informal and less reliable methods such as reviews or personal recommendations. The reliance on online reviews (36.4%) and word of mouth (22.7%) suggests that many respondents value social proof over regulatory oversight, leaving them vulnerable to fake reviews or misleading testimonies. Only 27.3% use SEC or CBN checks, showing low awareness or trust in official regulatory channels, which are the most reliable means of verification. The 13.6% who do not verify at all form a critical risk group, exposing themselves fully to fraud. This behavior aligns with earlier

findings on losses due to fraudulent activities respondents who skip or use weak verification methods are more likely to encounter scams. There is a pressing need to strengthen financial literacy campaigns that teach traders how to use regulatory databases and official tools for verification. The findings highlight that weak verification culture, rooted in reliance on informal methods, is a major enabler of online financial fraud.

Table 4. Experience of platform mismatch

| Experience of Platform Mismatch | Frequency | Percentage (%) |
|---------------------------------|-----------|----------------|
| Yes                             | 48        | 43.6           |
| No                              | 62        | 56.4           |
| Total                           | 110       | 100            |

Source: Field work, 2025

The table 4 above shows that 43.6% reported experiencing platform mismatch, while 56.4% said they had not. This means that nearly half of the respondents have encountered situations where the platform did not match their expectations, features, or promised services. With close to half of the respondents experiencing platform mismatch, this issue represents a significant challenge in online trading activities. Platform mismatch often reflects false advertising, hidden conditions, or discrepancies in service delivery, which undermines trust in online financial platforms. The relatively high percentage of “Yes” responses suggests that fraudulent or unregulated platforms are common, aligning with earlier findings on fake brokers and hidden transaction fees. The 56.4% who reported no mismatch may either exercise better verification practices or use more credible platforms, showing that careful selection can reduce risk. The findings highlight the importance of strengthening user awareness about red flags and improving regulatory oversight, to minimize cases where traders are misled by deceptive platforms. The experience of mismatch demonstrates how information asymmetry in online financial markets contributes to fraud risk, particularly among less cautious or inexperienced traders.

Table 5. Red flags identified before investing

| Red Flags                    | Frequency | Percentage (%) |
|------------------------------|-----------|----------------|
| Unclear terms and conditions | 30        | 27.3           |
| Unrealistic profit promises  | 40        | 36.4           |
| Lack of regulation           | 25        | 22.7           |
| Anonymous ownership/contacts | 15        | 13.6           |
| Total                        | 110       | 100            |

Source: Field work, 2025

Table 5 above present red flags identified before investing. It shows that the most frequently identified red flag was unrealistic profit promises (36.4%), followed by unclear terms and conditions (27.3%). Fewer respondents recognized lack of regulation (22.7%) and anonymous ownership/contacts (13.6%) as warning signs. This indicates that respondents are more likely to notice visible and obvious red flags (profit promises, vague terms) than structural or technical ones (regulation status, hidden ownership). Many respondents can spot obvious fraud tactics like “get rich quick” promises, but fewer identify deeper systemic red flags, such as lack of regulation or anonymity of owners. The low recognition of regulatory and ownership-related red flags reflects limited financial literacy and poor awareness of due diligence practices. Since many traders ignore critical but less visible warning signs, they remain susceptible to sophisticated scams that appear professional but

lack legal legitimacy. The lack of attention to regulatory red flags helps explain why nearly half of respondents experienced platform mismatch. Financial literacy initiatives should place stronger emphasis on teaching traders to check regulatory compliance, licensing, and ownership transparency, not just obvious promises. The findings show that fraud thrives not only because of fraudulent actors but also due to gaps in user awareness, creating a space where scams can flourish.

Table 6. Whether respondents reported an online fraud incident to regulatory agencies

| Reported an Online Fraud Incident | Frequency | Percentage (%) |
|-----------------------------------|-----------|----------------|
| Yes                               | 27        | 24.5           |
| No                                | 83        | 75.5           |
| Total                             | 110       | 100            |

Source: Field work, 2025

The table 6 above show that only 24.5% reported online fraud incidents to regulatory agencies such as SEC, CBN, EFCC, or the Police, while the vast majority, 75.5%, did not report their experiences. This indicates a very low rate of formal reporting of online fraud incidents among respondents. The large proportion of respondents who did not report fraud highlights a serious underreporting gap, which makes it difficult for regulators to track, investigate, and curb fraudulent activities. Possible reasons for non-reporting may include lack of awareness of reporting channels, fear of bureaucracy, or lack of trust in regulatory agencies' effectiveness. The failure to report incidents creates an environment where fraudsters operate with impunity, as cases got untracked and unpunished. This finding underscores the need for regulatory bodies to intensify public sensitization, provide simpler reporting mechanisms, and build trust in enforcement processes. The result suggests that tackling online financial fraud requires not only better regulations but also strategies to encourage victims to come forward, such as whistleblower protections and victim support services. This is in contrast to an interview with Online Investor, who revealed that:

*"When I realized I had been defrauded by a fake investment platform, I immediately reported the case to the Securities and Exchange Commission. I filled out their online complaint form and provided all my transaction receipts. The process took time, but I felt it was important to let regulators know. Even though I didn't recover my money, I was satisfied that my complaint contributed to investigations that might protect others."*

While Online Trade posited that:

*"Since the fraud involved my bank account, I reported to the Central Bank of Nigeria (CBN). They advised me to lodge a complaint through my bank first. After I escalated, the bank froze the recipient's account, although the funds were already withdrawn. It taught me the importance of reporting quickly. Even if recovery isn't guaranteed, CBN's involvement pressures banks to take such issues seriously."*

Another Online Trade revealed that:

*"I took my case to the Economic and Financial Crimes Commission (EFCC) after losing a large sum to a cryptocurrency scam. They interviewed me and collected all my evidence, including WhatsApp chats and payment records. The case is still under investigation, but I believe EFCC has the mandate to handle such criminal cases. For me, reporting wasn't just about recovery it was about holding fraudsters accountable."*

Also, in an interview with Online Trade revealed that:

*"The first agency I went to was the police station. They took my statement and promised to investigate. Although progress was slow, reporting gave me a formal record of the incident. Later, I used that police report to escalate the case with my bank and also to file a complaint with the SEC. So, for me, the police act as an entry point for other agencies."*

Also, in an interview with Online Trade revealed that:

*"I have reported online fraud twice—once to the police and once to SEC. In both cases, the feedback was limited. However, I don't regret reporting because it helps create official statistics and might lead to future crackdowns on fraudulent platforms. Many victims remain silent, which only encourages scammers. So even though I didn't get my money back, I believe reporting is necessary for collective protection."*

### *Prospect of red flags in an online trading*

Table 7. On whether respondents attended financial literacy awareness training

| Financial Literacy or Online Fraud Awareness | Frequency | Percentage (%) |
|----------------------------------------------|-----------|----------------|
| Yes                                          | 32        | 29.1           |
| No                                           | 78        | 70.9           |
| Total                                        | 110       | 100            |

Source: Field Work, 2025

Table 7 above shows that only 29.1% reported having attended or participated in financial literacy or online fraud awareness training, while a large majority, 70.9%, had never taken part in such training. This reveals a low level of exposure to structured education on financial literacy and online fraud prevention among the respondents. The low participation rate suggests that most respondents lack formal training in recognizing red flags, understanding risks, or applying safe practices in online trading. With 70.9% lacking awareness training, respondents are more vulnerable to fraud, phishing, and scams, which explains the high prevalence of fake brokers, delayed withdrawals, and hidden charges in earlier findings. The result points to a systemic gap in public sensitization, as financial literacy campaigns appear insufficiently widespread or accessible. There is a need for regular, targeted financial literacy programs, particularly for youths and low-income earners who dominate online trading activities. This finding reinforces the argument that weak financial knowledge and lack of structured awareness are major enablers of online financial market fraud. This is in contrast to an interview with Online Investor, who posited that:

*"Before I invest in any platform, I now check whether it is registered with SEC or CBN. That's the only way I feel safe putting in my money. I rely on my friends and trader forums. Whenever someone has a bad experience, they share it, and that helps the rest of us avoid the same mistake. Anytime I notice a red flag, like unrealistic profit promises or unclear terms, I immediately stop and look for another platform. I don't take chances anymore."*

Also, in an interview with Online Trade revealed that:

*"I attended an online fraud awareness workshop. It really helped me to understand the risks and how to identify fraudulent schemes before they trap me. I also, have reduced the number of platforms I use. Now*

*I only trade on popular and established platforms like Binance and MetaTrader, instead of experimenting with unknown ones, and I never put all my money in one platform. Even if one turns out to be fake, I don't lose everything at once."*

Furthermore, an interview with Online Trade revealed that:

*"My coping strategy is to start small. I test a platform with little money first. If it works well, I can then increase my investment gradually. If I encounter fraud, I try to report to EFCC or SEC. Even though the response is slow, I feel it's better than keeping quiet. I usually read online reviews and testimonies before joining a platform. If too many people complain about scams, I don't bother signing up."*

Again, Online Trade opined that:

*"The solution for me is self-control. I avoid any platform that looks suspicious, even if my friends are making quick profits. It's better to be safe than sorry."*

The study revealed that respondents experienced a range of challenges in online trading, including fake brokers or platforms, hidden transaction fees, delayed withdrawals, poor or no customer support, and frequent hacking or phishing attempts. These findings highlight a fragile online trading environment marked by fraud, lack of accountability, and persistent cyber threats. This is aligned with the lens of Social Engineering Theory, which explains how fraudsters exploit human psychology to deceive individuals into compromising confidential information or making risky financial decisions (Washo, 2021). Online fraudsters often manipulate trust and authority cues to impersonate legitimate trading platforms or customer service agents, thereby influencing investors' behaviors. Similarly, persuasion theory, as developed by (Jabir et al., 2025), provides insight into how scammers employ psychological principles such as authority, scarcity, reciprocity, social proof, and commitment to attract victims into fraudulent online trading schemes (Zimba et al., 2025). For example, fake brokers may create a sense of urgency ("limited-time investment offer") or false credibility ("licensed trading partner") to persuade users to invest quickly without proper verification. The study underscores the need for stronger regulatory oversight, user education, and robust support systems to mitigate manipulation and deception in online trading. Educating investors about persuasion tactics and cyber hygiene can enhance their resistance to fraud and foster a safer digital trading environment (Dupont et al., 2023).

The study found that the vast majority of respondents did not report their experiences of online trading fraud, indicating a very low rate of formal reporting among victims (Zhan et al., 2024). This underreporting highlights a serious gap that impedes the ability of regulatory agencies to track, investigate, and determine fraudulent activities (Lee et al., 2023). Several factors may explain this pattern, including a lack of awareness about official reporting channels, perceived bureaucratic hurdles, or distrust in the effectiveness of enforcement institutions (Pourhabibi et al., 2020). As a result, fraudsters continue to operate with relative impunity, exploiting the absence of accountability mechanisms. This is in line with the study of (Muslim, 2025) which differently emphasizes how fraudsters manipulate human emotions such as fear, shame, or embarrassment to discourage victims from reporting (Turksen et al., 2024). Victims may internalize blame for being deceived or fear reputational damage, which reinforces silence. Similarly, persuasion theory explains that fraudsters exploit psychological principles such as authority and liking, building a false sense of trust that later dissuades victims from questioning or disclosing fraudulent actions (Gkegkas et al., 2025).

## Conclusion

Non-reporting is not merely a behavioral lapse but an outcome of deliberate psychological manipulation embedded within online fraud schemes. The study therefore underscores the urgent need for regulators to strengthen public sensitization, simplify fraud reporting procedures, and build institutional trust. Empowering users with knowledge of persuasion and social engineering tactics can assist them in recognizing manipulative cues early, resisting deception, and confidently reporting fraudulent encounters.

## Conflicts of Interest

The authors declare no conflict of interest.

## Funding

The research and writing of this article were funded by personal funds.

## Author contribution

**Umar Isah:** Conceptualization, Methodology, Software.; **Suleman Ahmed Wan,** and **Abdulrahman Ibrahim:** Data curation, Writing-original draft preparation.; **Salihu Liman Wan** Visualization, Investigation.; **Umar Isah** and **Suleman Ahmed Wan:** Supervision, Software.; **Abdulrahman Ibrahim:** Validation, Writing-reviewing, and editing.

## Declaration of generative AI in scientific writing

During the preparation of this work, the author(s) used Grammarly in order to improve language and readability. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the content of the publication.

## References

- Donadelli, F., & Van Der Heijden, J. (2024). The regulatory state in developing countries: Redistribution and regulatory failure in Brazil. *Regulation & Governance*, 18(2), 348–370. <https://doi.org/10.1111/regg.12459>
- Đorđević, B., Milanović Zbiljić, S., & Radosavljević, M. (2025). Impact of the Digital Skills on Employability: Cross-Sectional Analysis. *Economies*, 13(7), 196. <https://doi.org/10.3390/economies13070196>
- Dupont, B., Shearing, C., Bernier, M., & Leukfeldt, R. (2023). The tensions of cyber-resilience: From sensemaking to practice. *Computers & Security*, 132, 103372. <https://doi.org/10.1016/j.cose.2023.103372>
- Eriksson, K., Lindvall, J., Helenius, O., & Ryve, A. (2021). Socioeconomic Status as a Multidimensional Predictor of Student Achievement in 77 Societies. *Frontiers in Education*, 6, 731634. <https://doi.org/10.3389/educ.2021.731634>
- Gkegkas, M., Kydros, D., & Pazarskis, M. (2025). Using Data Analytics in Financial Statement Fraud Detection and Prevention: A Systematic Review of Methods, Challenges, and Future Directions. *Journal of Risk and Financial Management*, 18(11), 598. <https://doi.org/10.3390/jrfm18110598>

- Ika Sari, G., Winasis, S., Pratiwi, I., Wildan Nuryanto, U., & Basrowi. (2024). Strengthening digital literacy in Indonesia: Collaboration, innovation, and sustainability education. *Social Sciences & Humanities Open*, 10, 101100. <https://doi.org/10.1016/j.ssaho.2024.101100>
- Jabir, R., Le, J., & Nguyen, C. (2025). Phishing Attacks in the Age of Generative Artificial Intelligence: A Systematic Review of Human Factors. *AI*, 6(8), 174. <https://doi.org/10.3390/ai6080174>
- Jules, T. D., & Arnold, R. (2022). The International Transfer of Education Models: Crafting the Neoliberal Citizen Through Regionalization and Rewesternization in Trinidad and Tobago. In B. Akgün & Y. Alpaydın (Eds.), *Education Policies in the 21st Century* (pp. 269–292). Springer Nature Singapore. [https://doi.org/10.1007/978-981-19-1604-5\\_11](https://doi.org/10.1007/978-981-19-1604-5_11)
- Lee, Y. Y., Gan, C. L., & Liew, T. W. (2023). Thwarting Instant Messaging Phishing Attacks: The Role of Self-Efficacy and the Mediating Effect of Attitude towards Online Sharing of Personal Information. *International Journal of Environmental Research and Public Health*, 20(4), 3514. <https://doi.org/10.3390/ijerph20043514>
- Ljungqvist, M., & Sonesson, A. (2022). Selling out Education in the Name of Digitalization: A Critical Analysis of Swedish Policy. *Nordic Journal of Studies in Educational Policy*, 8(2), 89–102. <https://doi.org/10.1080/20020317.2021.2004665>
- Meniago, C. (2025). Digital Financial Inclusion and Economic Growth: The Moderating Role of Institutions in SADC Countries. *International Journal of Financial Studies*, 13(1), 4. <https://doi.org/10.3390/ijfs13010004>
- Moura, L., Barcaui, A., & Payer, R. (2025). AI and Financial Fraud Prevention: Mapping the Trends and Challenges Through a Bibliometric Lens. *Journal of Risk and Financial Management*, 18(6), 323. <https://doi.org/10.3390/jrfm18060323>
- Muslim, M. (2025). The Failure of Governance and Internal Controls in Preventing Fraud in the Company. *Advances in Managerial Auditing Research*, 3(1), 15–29. <https://doi.org/10.60079/amar.v3i1.418>
- Nguyen Thanh, C., & Phan Huy, T. (2025). Predicting financial reports fraud by machine learning: The proxy of auditor opinions. *Cogent Business & Management*, 12(1), 2510556. <https://doi.org/10.1080/23311975.2025.2510556>
- Pourhabibi, T., Ong, K.-L., Kam, B. H., & Boo, Y. L. (2020). Fraud detection: A systematic literature review of graph-based anomaly detection approaches. *Decision Support Systems*, 133, 113303. <https://doi.org/10.1016/j.dss.2020.113303>
- Trotta, A., Gallucci, C., Rania, F., Strano, E., & Tipaldi, R. (2026). The “black box” of digital finance: An umbrella review of the challenges and drawbacks in advancing financial inclusion. *Research in International Business and Finance*, 81, 103188. <https://doi.org/10.1016/j.ribaf.2025.103188>
- Turksen, U., Benson, V., & Adamyk, B. (2024). Legal implications of automated suspicious transaction monitoring: Enhancing integrity of AI. *Journal of Banking Regulation*, 25(4), 359–377. <https://doi.org/10.1057/s41261-024-00233-2>
- Washo, A. H. (2021). An interdisciplinary view of social engineering: A call to action for research. *Computers in Human Behavior Reports*, 4, 100126. <https://doi.org/10.1016/j.chbr.2021.100126>
- Zhan, Y., Ahmad, S. F., Irshad, M., Al-Razgan, M., Awwad, E. M., Ali, Y. A., & Ahmad Ayassrah, A. Y. A. B. (2024). Investigating the role of Cybersecurity’s perceived threats in the adoption of health information systems. *Heliyon*, 10(1), e22947. <https://doi.org/10.1016/j.heliyon.2023.e22947>
- Zimba, A., Phiri, K., Kashale, C., & Phiri, M. (2025). Unveiling deception: A socio-economic analysis of smishing attacks on mobile money transaction users. *Humanities and Social Sciences Communications*, 12(1), 1880. <https://doi.org/10.1057/s41599-025-06141-8>