INVESTMENT AND TRADING SCAMS THROUGH SOCIAL MEDIA PLATFORMS: A CYBER-LEGAL ANALYSIS OF EMERGING CHALLENGES IN INDIA

John Claiton J, LL.M (Cyber Law), School of Law, Joy University

ABSTRACT

The increasing proliferation of social media has altered the manner in which people acquire financial information, communicate with the market players, and take decisions regarding investments. Media outlets such as WhatsApp, Telegram, Instagram, YouTube, and Facebook are now being widely used for promoting investment options, trading strategies, and financial advice. While the use of these networks makes access to financial information more convenient, it has simultaneously opened new avenues for investment and trading frauds. Scammers employ fake personas, imposters, false trading apps, misleading ads, doctored screenshots of profits, manipulated testimonies, and increasingly advanced artificially intelligent generated content to lure potential victims.

Social media-based frauds and scams in the fields of investments and trading pose a challenging legal issue, as it combines elements of cybercrime, securities law and consumer law along with issues of digital evidence. In India, some of the laws that can be applied to combat the menace include SEBI, Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and many others. But issues persist regarding the identification of anonymous offenders, preservation of digital evidence, fund-tracing, cross-border activities, and liability of social media platforms and financial institutions. The present paper will discuss the current trends of social media-based investment frauds in India, review the existing cyber-legal structure and the problems involved in their detection and enforcement.

Keywords: Social Media Fraud; Investment Fraud; Trading Scams; Cybercrime; SEBI; Investor Protection; Digital Evidence.

1. Introduction

Rapidly growing social media has changed the way people communicate, gather information and make financial decisions. Financial information that used to be available in the form of newspaper articles, through financial advisors, stockbrokers or specialized financial websites is nowadays widely spread through social media. WhatsApp, Telegram, Instagram, Facebook and YouTube have made it possible for financial information to be available to a lot of people within a short amount of time. While it has led to a greater engagement of the public in financial market transactions, it has also allowed fraudsters to advertise fraudulent investment scams quickly, anonymously and without geographical limitations.

Investment and trading scams performed via social networks have evolved into something that differs from regular frauds involving financial manipulations. The con artist can pretend to be a legitimate broker, financial adviser or a bank, form groups promising unique trading opportunities, promote fake trading apps or ask for a transfer of funds via online banking and digital payments systems. The scam may start with a demonstration of fake results to increase confidence and then ask for higher investments. The widespread use of artificial intelligence complicates the issue even more as it allows creating realistic images, videos, voice recordings and other types of manipulated material. Thus, the difference between legitimate financial communication and fraudulent marketing becomes hard to establish for an inexperienced investor.

Legally, the issue is as problematic as its practical side. Such a scheme can include cheating, impersonating, providing unauthorized investment advice, market manipulation, using of digital identities and illegal use of electronic communication means. Therefore, it requires joint efforts from securities regulators, cybercrime agency, banks, payment processors and social networks to investigate. On the other hand, such problems as anonymous profiles, deleting of the information quickly, foreign offenders, digital evidence and transferring funds through multiple accounts make the task hard.

Against such a backdrop, the current study explores the novel aspect of investment and trade scams via social media sites in India and analyses the sufficiency of the cyber-legal framework that exists in the country. In particular, the paper discusses the approach taken by the fraudsters, the applicability of securities law and cyber law, problems in the investigation process, and the obligations of digital platforms and financial intermediaries. This research utilizes the doctrinal

and analytical approach based on legislative provisions, regulations, judicial precedents, official documents and current trends.

2. Social Media and New Forms of Investment Scams

Social-media sites are now being used as a means for marketing investment offers because they enable fraudsters to target a broad base of victims using social-media sites at relatively affordable rates. Whereas financial crimes usually involve face-to-face contact between the victim and the fraudster, social-media-based fraud enables perpetrators to distribute fraudulent content through social-media posts, ads, private messaging, videos and groups. Fraudsters use accurate looking financial data along with fake data to create an illusion of legitimacy. Professional pictures, logos, fabricated registration details and terms used by the investment world can easily transform an ordinary social-media profile into a professional one.

The second type of fraud is the impersonation of the legitimate broker, investment adviser, analyst or financial institution. Impersonators use the identity, logo, picture or any other publicly available information to create an identical profile. Victims are then targeted to provide investment advice or are invited to join private groups to participate in trading offers.

Another scam method involves fraudulent trading sites and mobile applications. In this case, victims can be lured into downloading a specific application or logging into a site that seems to offer legit trading. Upon creating an account and making deposits, the account holder will observe a false balance or fake successful trades on the platform. In some cases, the scammers may allow a victim to withdraw a small sum of money to install confidence. As soon as the victim deposits a big sum of money into their account, more money is requested to be paid in the form of taxes, account verification, brokerage fees, and withdrawal fees. The money made will be fake, and after a certain period, the victim realizes that he/she cannot withdraw his/her money.

Trading groups on apps like WhatsApp and Telegram present another useful environment for scams. These groups usually have successful investors, trading experts, and administrators who are always sharing tips on investments or market forecasts. Some of these members may be fake profiles operated by the scammers. The success of these members will give social proof that convinces the newcomer to invest money. Group communication will make a member feel special since they will think that only few people have access to certain signals or opportunities.

The other way through which the fraudsters may make use of unrealistic expectations is by making promises of instant gains. This could take the form of guaranteed gains, high gains, or no risk trading. The promise could be made to people who do not know much about financial markets. This kind of communication creates a sense of urgency in such a way that the opportunity is available for a short while.

Manipulated advice and coordinated advertising may influence securities trading as well. Misleading or overestimated information may be spread to generate artificial demand for certain security. Investing in securities on the basis of misleading information leads to the purchase of securities at inflated prices without awareness of the associated risks. Later when the promoters of the scheme sell out their investments, the remaining investors face losses. Social media may facilitate these fraudulent schemes since information can be quickly spread on many social media accounts and groups.

The advent of artificial intelligence has opened up a new realm of frauds as well. Fraudsters can manipulate photographs, voices and videos to make false investment schemes seem like celebrity or professionally endorsed schemes. This information can be accompanied by sponsored ads and online communications. It is thus not only the misstatement in writing anymore but technological means have made audio visual representations possible.

All these factors show that social media investment fraud is more complex than just asking for money; rather, it is an effort to build up credibility, manipulate the expectations of investors, and exploit the digital technology to ensure that things appear legitimate. Social media's reach, pace, and interactive nature help the perpetrators of investment and trading frauds lure their victims even before any reliable information about the scheme can be obtained, thereby making social media a prominent site of investment and trading frauds.

3. Indian Legal framework

There is no specific law in India dealing with the issue of investment and trading fraud through social media. The acts may come under violations of securities laws, cheating, impersonation, improper use of electronic communications, and digital information. Thus, the framework to deal with such acts will comprise securities law, criminal law, IT law, and regulatory guidance working in combination. It is also important that the framework works effectively not only because there are offences but also because there is proof of the link between the two.

The Securities and Exchange Board of India (SEBI) has an important role in cases of fraudulent activities associated with the securities market. The SEBI Act, 1992 lays down the statutory basis for the regulation of the securities market and protection of investors. SEBI can conduct investigation into market violations and take regulatory action against any person indulging in fraudulent or manipulative practices. Any scheme based on social media in connection with investments could fall within this regulatory regime where individuals give unauthorized investment advice or make misrepresentations regarding securities or other interference with the securities market. The investment advisers and research analyst regulatory framework is of particular importance since giving financial advice from a social-media account, by itself, does not qualify the unregistered individual as a financial professional.

SEBI has also addressed the rising trend of employing social media for fraudulent activities in the securities market. Regulatory policy in this area has been geared towards investor education, verification of registered intermediaries, and regulation of any misleading or fraudulent communication done through the internet. This is because an investor could easily believe an online trading advice account that identifies itself through the use of the name/logo/identity of a recognized financial institution. Regulatory efforts at greater authentication of financial advertisements and registered firms thus serve both a preventive and an enforcement role.

Criminal liability could arise under the Bharatiya Nyaya Sanhita, 2023 in cases where the acts of the offender constitute offences of cheating, criminal impersonation, forgery, or any other form of dishonesty. The basic question of criminal liability is whether there was an intention on the part of the accused to deceive the victim into handing over his property or do something that results in him suffering a loss. Social media investment fraud is often conducted through electronic communication, although the underlying criminal act still matters. Thus, the use of the digital platform will simply alter the way the offence is committed without altering the essence of the offence itself.

The Information Technology Act, 2000 serves to supplement the existing criminal law by taking care of acts performed using computers and electronic communication. The provisions of the act become relevant where there is fraud in connection with unauthorised use of digital identities, manipulation of electronic resources, or any other act that falls within the purview of the act. The importance of the act lies in the fact that there are electronic records made by

social-media investment fraud that might be very relevant in the future. But the mere presence of electronic communication does not prove the identity and intent of the person.

It is thus important to take into consideration the evidentiary element. Electronic messages, emails, screen shots, transactions, applications, website addresses and other electronic evidence could help investigators in unravelling the fraud. The Bharatiya Sakshya Adhiniyam, 2023 is the present legal regime governing the evidentiary element for electronic and digital information. Collection, preservation and authentication of this information is important because the electronic content could be deleted, altered or transferred from one medium to another. Any criminal case filed on the basis of electronic evidence would need not only to prove the communication but also, wherever necessary, the link between the electronic evidence and the defendant.

The digital nature of these frauds also throws up issues pertaining to personal data. Names, telephone numbers, identification proofs, bank account details and other personal information could be collected by fraudsters by communicating deceptively with individuals. The Digital Personal Data Protection Act, 2023 applies to the general sphere of personal data processing and protection although it cannot be seen in place of criminal or securities law. It is particularly relevant in situations where the misappropriation of personal information has resulted in impersonation and fraud.

The intermediary structure is yet another crucial element. Social-media networks serve as conduits where fraudulent advertisements, profiles, messages and groups could be published. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 mandate due-diligence responsibilities of intermediaries within the ambit of their statutory provisions and relevant circumstances. In such a way, the legal challenge does not solely involve the determination whether the particular platform contained fraudulent material, but rather the determination of its responsibilities when receiving knowledge about unlawful content, and reasonable procedures for reporting, removing, preserving and cooperation with relevant authorities.

All in all, the Indian legal regime offers a number of legal avenues to deal with investment fraud via social media. Securities law regulates market-based offences and financial activities; criminal law regulates fraudulent actions; information technology law regulates technology issues; and evidence law regulates use of digital evidence in court proceedings. However, it is

critical to apply these provisions in coordination since fast-changing dynamics of online fraud, including usage of anonymous accounts, artificial intelligence and cross-platform communication, requires an integrated approach to investigation and prosecution.

4. Investigation, Enforcement Challenges and Legal Gap

The mere presence of several legal measures is not automatically indicative of the successful enforcement of the social media investment scams. The first problem is that the fraudulent behaviour will be spread over several digital identities, communication tools, financial transactions and jurisdictions. Hence, investigators should trace a link between the identity used to contact the victim, the owner of this identity and the financial beneficiary of the scam. It becomes extremely problematic when offenders employ fake identities, temporary phone numbers, several social media accounts and stolen personal data for account registration.

There is an additional issue related to the collection and preservation of digital evidence. Social media messages, user profile, advertisements and groups could be changed or deleted in a relatively short time. The first step victims make is saving only screenshots which might not provide enough information about the origin of the message. Encrypted messages and messages that disappear will make it even more challenging. Investigation of fraud cases needs timely collection of evidence before they are deleted. Attribution is another challenge associated with investigation of online frauds. The fact that one manages to find out the account that sent a fraudulent message does not mean that it will be possible to detect the offender. An account might be controlled using someone else's device or a hijacked account; additionally, an intermediary might send a fraudulent message on behalf of other people. It is important to understand the structure of fraud networks: fraudsters will try to separate the persons who are contacting the victims from the persons who control bank accounts.

Identification and recovery of the money is yet another challenge. Money that is obtained fraudulently might be quickly routed through different bank accounts or payment channels. Mule accounts may be employed to make the perpetrator less traceable from the victim. When it comes to reporting the crime, the money may already have been transferred to new accounts or withdrawn. Prompt reporting and speedy coordination among the victim, banks and cybercrime agencies as well as other necessary parties can increase the probability of freezing or recovering the funds.

The cross-border character of online fraud poses further problems concerning jurisdiction. The victim may live in India, the website where the fraud occurred operates on infrastructure outside India, and the perpetrator lives in a different country. The necessary information in electronic form or financial data might be possessed by an entity in a different jurisdiction. Gaining such information legally might be a lengthy process, whereas the communication and financial transactions related to fraud can happen immediately.

Yet another gap relates to the issue of many unregistered individuals who appear as experts in investments by virtue of their presence on social media sites. It is comparatively easier for regulation agencies to use traditional means of regulation in case where the individual is a market intermediary that is known to them. Those who conduct frauds through anonymity or from a position outside the regulated financial system find it harder to be detected until they do some damage to the investors.

AI is another problem that regulators will encounter while trying to detect and curb the practice of investment fraud. Deepfake videos, synthetic voice and fake endorsements can make it hard for one to determine whether a public figure or financial expert has really made certain statements. Since the use of AI materials is quick and easy to duplicate on various platforms, traditional investigation techniques may prove inadequate.

Another challenge is that of fragmented enforcement institutions. Misconduct in the securities market may involve SEBI, while criminal investigation might come under the purview of the police or the cybercrime investigators. Information from banks and payment providers is needed to trace the money flows, while the accounts and communications records will be controlled by the social media platforms themselves. Absence of prompt information exchange means slower and more inefficient investigations. Moreover, the victims themselves could have trouble figuring out what body should handle the matter and take immediate measures.

Such issues reflect another flaw of the current scheme. It is not just about the lack of legislation, but about the gap between the legal authority and its implementation. Fraud using social media for investments involves dealing simultaneously with digital identity, securities legislation, financial transactions, and electronic evidence. A fragmented approach may lead to exploiting loopholes between the different institutions involved. Thus, better institutional cooperation, prompt evidence preservation, financial tracing, and social media involvement are crucial to ensure that the legal protections are efficient beyond just prosecuting the crime afterwards.

5. Responsibility of social-media platforms and financial intermediaries

There is an emerging trend of social-media usage in investment communications that places not only the investor and regulator but also the social-media platform and the financial intermediaries responsible for fraud to bear certain responsibilities. Social media companies make possible the delivery of advertisements, profile pictures, videos, groups and even private messages to the potential victims of fraud. Banks, payment intermediaries and other legitimate market actors who handle financial transactions play significant roles in the process as well.

Effective measures should be adopted to detect and prevent any fraudulent investment promotion campaigns through the social media sites. The platform must ensure particular caution in case the account represents itself as being registered as an intermediary of SEBI or represents an identity of an institution and makes claims of unreasonable profits. The platforms may consider automated detection and manual review system to detect any suspicious pattern, repeated advertising or coordinated accounts. Financial advertisers can also adopt any verification measures for distinguishing real investment professionals from anonymous advertisers. These measures, however, must be designed in such a way that does not affect lawful expressions or financial education.

Another measure that must be considered for the protection of investors is making available any easy method for reporting any suspected fraud cases to the platform. The investors need not undergo lengthy processes for reporting any suspected case of investment fraud. Appropriate priority should be given to such complaints as fraudulent content may reach thousands of people in short span of time. In case of any unlawful content that is found in accordance with any valid legal process, the platform needs to act in accordance with the law.

Prevention is also a critical task for the financial intermediaries. It is common for banks and payment service providers to be among the earliest financial organizations that receive the proceeds of the fraudulent transaction. Transaction monitoring systems can aid in detecting unusual behaviour, speedy transactions, and suspicious accounts. Prompt coordination when a fraud victim reports the crime might increase chances of preventing further movement of funds. It is crucial for financial institutions to raise customers' awareness concerning fraudulent investment schemes especially those asking the customer to make payments to unknown applications, personal bank accounts, or non-official channels.

It is essential for legitimate brokers, investment advisers, and other regulated institutions to be proactive in protecting investors against fraudsters posing as them. Impersonators use the reputation and names of legitimate financial organizations to make the scam more convincing. Hence, the legitimate entities need to ensure that the contact information on their accounts is up to date and warn investors immediately upon discovery of fraudulent websites or accounts operating under their name.

The roles of these actors should not be seen as placing all of the responsibility of fraud prevention from the State to other organizations. Criminal investigation is still the task of the authorities, and regulatory organizations have to define the standards for regulated participants. Roles of platforms and intermediaries have to be performed within a legal framework taking into account investor protection, privacy, freedom of speech, and technological possibilities.

It would thus be more effective to act through coordination than through isolated actions of institutions. Social media platforms will help with verification and content management, financial intermediaries will be able to help with transaction monitoring and rapid response, regulated entities will be able to safeguard themselves and their clients, and authorities will be able to regulate and investigate. It will limit possibilities for fraudsters and increase the possibilities of investors to differentiate real financial services from online scams.

6. Reforms and Recommendations

As social media investment fraud becomes more sophisticated, an integrated regulatory framework, encompassing both preventive and enforcement mechanisms, is needed. This must not merely focus on punishing the offender after any financial damage has been incurred but also create a legal environment in which the fraud itself does not occur in the first place.

First, it would be useful to establish an effective verification system for individuals and firms offering investment-related services via the social media platform. Digital verification, in conjunction with SEBI registration, could make it possible for investors to identify legitimate firms from imposter firms. Additionally, social media platforms need to develop an effective verification process for advertisements involving securities and investments.

Increased institutional cooperation is just as necessary. SEBI, cybercrime enforcement, banks, financial payment intermediaries and social media platforms need ways of exchanging

information as per the laws in place. A cooperative reporting system would help complaints to be evaluated and channelled to the right authorities. Communication at an early stage by cybercrime authorities and financial institutions becomes very critical when prompt action can help stop further movement of fraudulently moved money.

Technological solutions must be a part of any regulatory measures. Artificial intelligence can help detect fraudulent investment advertisements, repetitive fraudulent accounts and other similar financial information manipulation. However, the artificial intelligence must be operated under proper human supervision in order to minimize false positives. Deep fake investment marketing campaigns and fake financial professional endorsements must get particular attention.

Digital evidence retention can be improved with the implementation of effective procedures for the storage of pertinent social media content, account data, and transaction history following receipt of credible complaints. Finally, investor awareness can be used as a preventive measure. Investor awareness campaigns must focus on highlighting certain red flags such as guaranteed profits, urgency to make investments, unauthorized trading platforms, and the need to make payments to personal accounts. Also, investors must be encouraged to verify the registration of advisers or intermediaries before making any financial decisions.

The above measures must work hand in hand and not separately. While verification will help minimize the risk of being associated with criminals, technology can be used to track suspicious activities, while collaboration will ensure rapid action is taken against the perpetrators. An effective approach of combining the above measures will make India better at dealing with online investment fraud while allowing legitimate digital finance communication.

7. Conclusion

The emergence of investment and trading fraud via social media websites is a case in point where technological progress opens up avenues for conducting crimes. While the technology has made it easier to access financial data and has increased participation in financial markets, it also presents an opportunity for the perpetrators of financial crimes because social media websites possess certain characteristics which are not only useful in facilitating financial transactions, but also useful to fraudsters. Fake identities, impersonation, fraudulent trading apps, fake investment groups, manipulated recommendations, and artificially created content

via artificial intelligence can be employed to establish financial credibility.

In India, there are various legal remedies available against such conduct. There are laws on securities that can be used against fraudulent and unauthorized activities relating to securities market and laws on criminality that can be invoked against deception and dishonest inducement. Further, there are provisions in IT Act and evidence laws that can be considered as possible mechanisms. However, all such legal remedies are hindered by certain practical difficulties related to anonymity, changing digital content, attribution, electronic evidence, cross-border issues and recovery of funds.

This analysis further highlights that investor protection should not only be a result of investigations and prosecution after any fraud takes place. The social media platforms and financial institutions must be responsible for prevention as well. Financial promoters can be verified, suspicious advertisements can be tracked, appropriate means of reporting can be created, and cooperation with law enforcement agencies can be initiated. Thus, a more effective measure would be to create a cyber-financial regulatory system in which SEBI, cybercrime agencies, financial institutions, and digital platforms can cooperate within the framework of information exchange, evidence preservation, and prompt actions. At the same time, technology should be used cautiously and with regard to such values as privacy and freedom of expression. In this case, the fight against social media investment fraud will have to include both prevention and detection of fraud, investigation, financial tracing, and investor protection.

References

1. Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, 2023 (India).
2. Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, Acts of Parliament, 2023 (India).
3. Digital Personal Data Protection Act, 2023, No. 22 of 2023, Acts of Parliament, 2023 (India).
4. Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India).
5. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E), Gazette of India (2021).
6. Securities and Exchange Board of India. (1992). *Securities and Exchange Board of India Act, 1992*.
7. Securities and Exchange Board of India. (2003). *Securities and Exchange Board of India (Prohibition of Fraudulent and Unfair Trade Practices relating to Securities Market) Regulations, 2003*.
8. Securities and Exchange Board of India. (2013). *Securities and Exchange Board of India (Investment Advisers) Regulations, 2013*. Securities and Exchange Board of India
9. Securities and Exchange Board of India. (2014). *Securities and Exchange Board of India (Research Analysts) Regulations, 2014*. Securities and Exchange Board of India
10. Securities and Exchange Board of India. (2025a, April 11). *Caution to public against fraudulent/manipulative activities on social media platforms (SMPs) related to securities market*. Securities and Exchange Board of India
11. Securities and Exchange Board of India. (2025b, May 21). *Caution to investors on stock market scams through social media platforms*. Securities and Exchange Board of India
12. Securities and Exchange Board of India. (2025c, May). *Advisory to SEBI registered intermediaries—Uploading advertisements on social media platforms (SMPs)*. Securities and Exchange Board of India

13. Securities and Exchange Board of India. (2025d, August 22). *Advisory against investment in fraudulent trading schemes claiming to be offered to Indian residents by FPIs*. Securities and Exchange Board of India

14. Securities and Exchange Board of India. (2025e, November 6). *SEBI intensifies efforts to combat online investment scams, calls for greater collaboration from social media platforms*. Securities and Exchange Board of India

15. Securities and Exchange Board of India. (n.d.). *Staying away from investment frauds and get rich quick schemes*. SEBI Investor. Sebi Investor

16. Securities and Exchange Board of India. (n.d.). *Social media frauds: Modus operandi*. SEBI Investor. Sebi Investor

17. Ministry of Home Affairs, Government of India. (n.d.). *National Cyber Crime Reporting Portal*. National Cyber Crime Reporting Portal