

# ONLINE INVESTMENT FRAUD: AN EMPIRICAL STUDY OF VICTIM PERCEPTION IN CHENNAI.

R. John Wesley<sup>1</sup>, Dr. S. Latha<sup>2</sup>

<sup>1</sup> MSC (Criminology and Forensic Science), DR. M.G.R Educational and Research Institute, Chennai.

<sup>2</sup> Assistant Professor in Department of Criminology, University of Madras Chennai, Tamil Nadu, India.

\*\*\*

**Abstract** - Now a day, various types of online investment fraud has increased, while the number of victim became outraged and also there had so many unreported case on online investment fraud. This study based on how a people get into the online investment frauds on the perspective of victim and the role of social media platform and other online application in the online investment frauds based on the victim concern. Through the combination of survey and interview method to examine the factor that individual gets into the investment fraud and role of the online application in the online investment fraud. This study contains 51 victims of online investment fraud in Chennai and that focused on the quantitative analysis of the victim profile, various types of online investment fraud and comparative analysis of rate of victimization based on the gender and crime, indicating factor of individual in online investment and role of the online application in the online investment frauds, criminal activity by scammer and response of report behavior.

**Keyword:** online investment fraud, victim profile, indicating factor, role of online application, report behavior.

## 1.INTRODUCTION

In 21<sup>st</sup> century, the society will be more modernize and there had develop technologies like smart phone, internet, cloud server that use in companies for storing the employee data and companies' data etc. . In this century, there will be more digitize in every category of data that use in every format like companies, study material, educational institute, etc. . and crime also modernized and evolve in every development of technology like cybercrime, cyber frauds and other crime relate to computer. This study based on one of the cybercrime, tilted as "Online investment frauds: An Empirical study on victim perception in Chennai", in this study focus on

online investment fraud based on the victim perceptive. Now a day, many people are involved in the investment to gain the extra money for maintain their comfortable life, investment platform are available in online platform to invest the money but they happen many fraud incident in online, the raider are target the people those are invest the money on online. Its will be easier for raider to commit the crime in online for money and also easy to escape from the investor. In this study based on victim perceptive, major finding will be demographical factor of victim like age of the victim- their education qualification- marital status- employment status of victim- their investment knowledge to invest the money, types of investment and platform their choose by victim, observed any criminal activity by raider through the online and report behavior like reporting the fraud – reporting platform – response from reporting platform – money recovery from raider. This finding will be analyzed with data that given by the victim of online investment frauds.

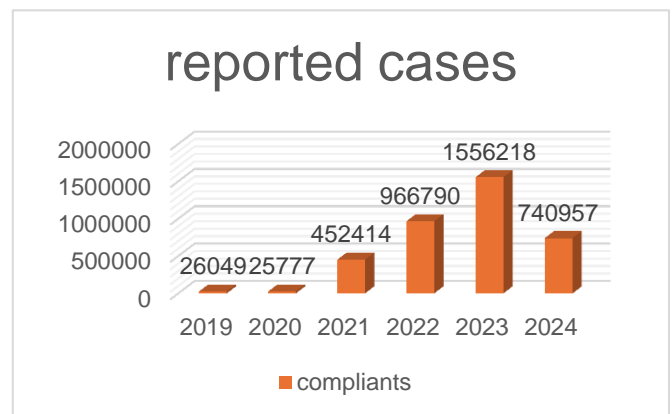
First of all , online investment is process of investing the money or buying in the online market , gold, land, mutual fund, crypto currency, etc. through the online platform. Now a day , there are so many online platform available for investment and also many startup companies are available to be a brokage for online investment to the common people. In online investment, Investors it including those new to the field, can access a variety of educational resources on numerous internet platforms. These resources encompass instructional videos, online seminars, and analytical tools, enabling individuals to make well-informed investment choices. It had some risk and may had chance to lose the money in the online investing because the financial product could be changing every time , it could high value and its could be low and also there had many fraud investing site in online platform before investing , there should verified the site or clarified the site with the expert.

And there is various type of online investment like stock, Bonde, Fixed Deposits, cryptocurrency, Trading etc.... After the industrial revolution the online investment made a huge revolution to mankind with the help of rapid technology development. Nowadays the power of technology makes a common man to investing in mutual funds, Trading, Stocks etc.. using the Investing App. The Internet plays a vital role in online investment because it teaches about the How invest, what to invest, when to invest those details help a common people to enter in online investing world. The Invention of Apps elevated the usage of online investment and makes the transition easier without any brokage support. These apps easily attract the beginners to the world of finance by providing platform as user-friendly, easy entry, easily access, various investing options etc... These apps help in reducing the cost of transactions and also we can easily monitory the real time status of the investment. The Flexibility of online interest help get notify the drop and rises of the price of investment in the market at any time and any place using the phone or desktop with the help of internet. The analysis tool help to predict the near match price of the investment in future. Transparency of online platforms give clear picture of fees, brokage fees, other charges, taxes etc.. which help trades to calculate the charge which involved in investment. The online platform provides the customer support for technical support and also individual assistance which motivate the beginners to invest in online. The online investment is very cheaper, convivence and faster method than the traditional method. Online investment fraud is a one of the cybercrimes , its define that as a deceptive scheme that occur online, where fraudsters use various tactics to convince individuals to invest in non-existent or worthless assets. These scams often exploit technology and the internet to reach potential victims, promising high returns with little to no risk. In recent days, online investment fraud should be a recent trend crime in cybercrime in India. Frauds will be update, evolve and innovative, its will be changing in a every year. They're had various type of online investment fraud like Ponzi scam, pyramid fraud, pump and dump scam, affinity fraud etc..,

### 1.1 Crime rate of online investment frauds

I4C stated that first four months of the 2024 overall 740000 complaints would register in India. Overall, 1750 crores are losses by Indian citizen through the cyber frauds.

Source: Business standard (2025)

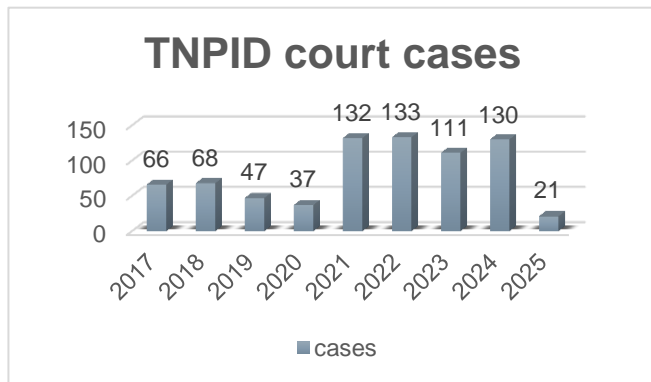


This data refers from the business standard news journal, the complaint data established by the I4C under the ministry of home affair. In this report statistics, before the covid period the cyber frauds would be less reported but after 2020, the cyber frauds should be increase more that 3to 5 times higher than the before 2020. In 2024 , these cases will be report in first four month of the 2024.

In 2023, the I4C reported over 100,000 investment fraud incidents. Trading scams accounted for 20,043 cases, leading to a loss of Rs 1,420 crore to cybercriminals during the same period. I4C stated that 222 crores are loss by people through investment scams and the report across 62687 reported cases filed in first four month in 2024.

In Tamil Nadu, the cyber cell received 2732 reported cases for cyber financial frauds and 34392 reported cases for online frauds in 2024. Overall, 771.98 crores are loss by people through the online scam and financial fraud through online and cyber cell recovered the 83.84 crores amount to the victim.

I4C established the cyber report of 2023, Tamil Nadu received 59549 cases of cyber financial frauds that include all types of financial crimes. 661.2 crores loss by people in Tamil Nadu.



Source: Indian kanoon

In this chart show that the cases data from 2017 to present date. This data clearly explains that before 2020 investment frauds will be less reported but after 2020 its will be rapidly increase in year by year. After 2020, every year reporting rate will be increase. This data only shows that cases report in TNPID court that present in Madras high court.

## 2. REVIEW OF LITERATURE

Eldad Bar Lev, Liviu-George Maha, and Stefan-Catalin Topliceanu (2022) in their article “Financial Frauds’ Victim Profiles in Developing Countries”, Social and Behaviour Influence Financial Frauds Victims in Emerging Countries and its offer an interesting review of the social-demographic and psychological factors underlying financial fraud perpetrators in developing countries. Through a review-types approach, the authors create both the theory and empirics to describe the traits and conditions that make certain populations vulnerable to swindles. The investigation indicates that, in different developing countries, victims of financial fraud belong to some common characteristics, as they are also male, employed, single to married, and different in their educational degrees. In countries like China, India and Nigeria, many are caught in the scam and opportunistic scammers are everywhere. In places like Latin America, on the other hand, victims of the violence are motivated, certainly not by a standpoint of community solidarity or commitment, but by the search for better fiscal opportunities or the absence of an emotional imagination, potentially by reckless fantasies that corrupt invisibility can be bought like private property. Another recurring motif is the importance of connections in social networks: many victims are

urged to participate in by-now classic Ponzi schemes by their friends, family members, or acquaintances who are fully persuaded of their legitimacy, thus underscoring the relevance of social capital in the spreading of financial fraud. This study examines psychological correlates of susceptibility to fraud. Impaired cognition, reduced self-control, impulsivity, and greater tolerance of risk is all cited as important factors. Typically, victims believe themselves to be shrewd and are too smart to fall for something of this nature, trust a professional and are influenced into doing so by fraudsters. Such psychological predispositions, particularly in combination with situational factors such as burden of debt and social isolation, and contextual factors such as lack of financial literacy, make them more prone to fraudulent practices. Socio demographic factors are also important. For example, in India and Nigeria, younger people are more likely to be approached, in part because they are active on digital platforms and are interested in high-return investments, such as cryptocurrencies. Older people, especially retired people who have received little financial education, are vulnerable to scams in places like Malaysia and Bolivia, but not as easily so in Ireland or Canada though these, indeed, are many other factors to consider when it comes to the older demographic in any given country 8. Gender relations are different, with men being the primary victims of these scams in India and women, who are the main providers and managers of household wealth in China, being hit more often. Educational level alone does not act as a shield; in certain event, better-educated individuals are at even greater risk, perhaps because they are overconfident” or are more exposed to sophisticated investment opportunities. The authors also highlight the importance of tailored interventions to reduce susceptibility to financial exploitation. Recommendations include improving financial literacy programs, particularly for at-risk populations, establishing strong regulatory frameworks to regulate financial transactions, and developing public awareness campaigns to educate people about common fraudulent schemes. By tackling the psychologically and socio-demographic factors found, policies and stakeholders can create holistic strategies to safeguard those in emerging markets from financial scams.

Marguerite Deliema, Doug Shadel, Karla Pak,(2020) on their article “Profiling the Victim in

**Investment Frauds: Mindsets and risk behaviour**", in its study, the researcher investigates the psychological and behavioural characteristics of individuals who are victims of investment fraud relative to those of typical investors. Given the massive financial losses and numbers of individuals victimized by investor scams, the authors focus on the psychological processes of those most at risk for fraud perpetration. Drawing on the opportunity framework of predatory victimization, an international telephone survey of 214 confirmed victims of investment fraud and 813 general investors was conducted. Participants were selected from random digit dialling and represent a diverse and representative sample. The study intently aimed to explore variations that exist in investment behaviours and psychological mindsets that can lead people to the chagrin of exposure to investment scams, as well as how potential victims may be more alluring and more open to gaining target. A number of highlighting differences of fraud victims can be identified in the results. Demographically, victims tend to be older and male. Psychologically, they are materially moralistic than the average investor. Victims behaviourally trade more frequently and are more likely to buy investments that have advertised through unsolicited means like cold calling, emailing, TV advertising or "free lunch" seminars. Otherwise, they are not more likely to invest from social network-mates, suggesting some independence from peer advice or a propensity to invest without outside validation. The results highlight the need for focused investor education campaigns to mitigate behaviours and mindsets such as those empirically shown here. By concentrating on decreasing materialistic attitudes, inculcating scepticism towards uninvited investment offers, and encouraging consultation of trustworthy social groups, such campaigns could help to rein in the ability of people to become involved in investment fraud. The researchers say that as increasing numbers of retirees take control of their retirement savings, they may be will be tempted by "unrealistic" investment returns offered by unprincipled brokers and urged that the life stage of being retired is a key time for teaching people about the danger involved in some investment. DeLiema, Shadel, and Pak's article (DeLiema et al., 2017) offers useful information about the people who are victimized by investment fraud and the research h is instructive e in a number of ways, particularly the contributions to understanding the role that

psychological and behavioural factors play in determining a person's risk for victimization. Their results support targeted education programs to promote safer investment behaviours and greater consumer protection.

**Obasanjo S. Balogun, Tomisin A. Akangbe, Olumide D. Fagbamila and Felix O. Aigbovbioisa (2024)** on this article "**Internet Users' Perception of the Prevalence of Online Investment Fraud and Victimisation in Nigeria**" by examines the prevalence of online investment fraud among Nigerian internet users, perceiving and experiencing it and the impact of some socio-demographic factors. The researchers adopted a cross-sectional survey research design to elicit data from 164 participants in Ilorin, Kwara State through Google forms on the basis of convenience sampling. The study is theoretically informed by the Routine Activities Theory (RAT) whereby crime takes place when a motivated offender has contact with a suitable target in the absence of capable guardian. Results show that 76.3% of respondents are young people aged 18-24 who have tertiary education and, who, for the most part, are students, highlighting their fragility in terms of financial experience and their desire for rapid financial returns. Significantly, more than 50% of those surveyed have invested online, in decisions influenced to a large extent by personal recommendations from family and friends and their search for financial independence. Alarmingly, 77.3% of investors suffered from online investment scam which consists of most case of Ponzi/pyramid schemes (42.6%), cryptocurrency fraud (26.5%) and forex trading fraud (19.1%). Monetary loss varied from less than ₦50,000 among 50% to more than ₦1,000,000 among others. The research highlights critical vulnerability factors, such as weak regulation, poverty, unemployment, and low levels of training on fraud prevention. There was a strong relationship between investment experience and high returns as a cause of fraud victimisation and the importance of financial education was underscored. Also, 87.8% of respondents reported that the unregulated environment leaves Nigerians vulnerable to online investment fraud with 75.6% believing that poverty and unemployment serve as a risk factor for victimisation. In conclusion, the study calls for immediate regulation of the online platform, public awareness and educational campaigns to reduce the potential hazards of online investment

fraud in Nigeria. Recommendations have been provided with the view to implementing tougher laws on offenders, and greater consumer education to help mitigate due diligence requirements and focused initiatives on dealing with socio-economic issue which cause vulnerability to fraud. The findings of the study are important for policymakers, financial regulators, as well as other stakeholders to safeguard the internet consumers from the emerging challenge of online investment fraud.

These study are related to this study, most of the study would be based on the various types of financial frauds and investment through online.

### 3. Methodology

This research based on the quantitative analysis research and sample will be victim of online investment fraud in Chennai. The data will be a primary data and collect by using the questionnaire with interview method. In this study, overall, 51 sample will collect by snowball technique, and analysis with SPSS software.

#### 3.1 Objective Of Study

- To explore the types of investment fraud among the victim.
- To analyse the role of the online application in the online investment frauds.
- To analyse the victim profile in online investment fraud .
- To observe report behaviour from the law enforcement and official site of application.

### 4. Results and Discussion

In this study, the data will analyse with 59 samples by using SPSS software for valid value.

Table 1: Gender

S.no	Gender	Percent
1	Male	58.8
2	Female	41.2
	Total	100.0

In this table 1 show that male will be 58.8% responded and women will be 41.2% responded.

Most of the responder will be male and also male will be victim more than women. In this study, most response that received from male so, we could not conclude that male are more vulnerable in online investment frauds. But male is more involve in investment field more than female because in our country female would be depend on family or life partner if she is a working person , her salary could be control by other so, that female could not more involve in investment field.

Table 2: Age of Respondents

S.no	Age	Percent
1	18-23	7.8
2	24-29	21.6
3	30-40	41.2
4	41-50	23.5
5	51-60	2.0
6	60 above	3.9
	Total	100.0

In this table 2 shows that 30-40 age category had high percentage (41.2%) and 41-50 age category had second higher percentage(23.5%) among the respondents and above 51 age category people had low percentage (5.9%). In this analysis, worker age people had more committed in online investment and also become more victim. More respondents mention that investment is a one of the part time income, so that they invest the money on online platform based on other opinion for another income.

Table 3: Educational qualification

S.no	Educational qualification	Percent
1	10 below	2.0
2	10th	2.0
3	12th	3.9
4	Under graduate	52.9

5	Post Graduate	39.2
	Total	100.0

In this analysis, the most of the respondent will be under age of 30-40 (41.2%) and also most of victim well educated and also most of responder finish the graduated, Under Graduated (52.9%) and Post graduated(39.2%). Most of the respondents will be educated person and also most of victim has hesitate to give sample, they had shame to talk about their delude because Others claimed that "someone tricked or deluded educated people."

Table 4: Profession

S.no	Profession	Percent
1	Private job	68.6
2	Government job	23.5
3	Unemployed	5.9
4	Daily wages	2.0
	Total	100.0

In this table 4 shows that profession among the respondents, 68.6% of respondent working in the private sector and 23.5% of respondent work at Government sector. Very less percentage of Daily wages employee among the respondents. Most of IT employee are investing the online platform.

Table 5: Amount of loss

S.no	Amount range	Percent
1	1000-10000	25.5
2	10000-50000	27.5
3	50000-1 lakhs	3.9
4	1 lakhs-10 lakhs	21.6
5	more than 10 lakhs	21.6
	Total	100.0

In this table 5 show that most of respondent loss the amount under the 1000-50000(52.9%) and 1 lakhs to more than 10 lakhs(43.2%). Some people get scammed in beginning stage and other get scammed after they extend the amount of investment.

Table 6: First time succeed in online investment

S.no	First time succeed	Percent
1	Yes	41.2
2	No	58.8
	Total	100.0

In this table 6 shows that more than 40% of respondents succeed in their investment, nearly 60% respondents get scammed in their first investment. In this analysis, most of respondents said that they gain the money in online investment when the invest the minimum amount, but when the upgrade the investment amount, and when people invest the large amount of money in online, they get scam in first time.

Table 7: Investment knowledge

S.no	Respondents	Percent
1	Yes	15.7
2	No	84.3
	Total	100.0

In this table 7 show that more than 80% of respondents doesn't investment knowledge. Most of victim doesn't have investment knowledge when they invest the money, they invest the money based on the other indicating factor like advertisement, friends etc..

Table 8: Idea

S.no	Indicating factor of online investment	Percent
1	Social media	29.4
2	Friend	52.9
3	Advertisement	13.7

4	Other	3.9
	Total	100.0

In this table 8 shows that 52.9% of respondents invest the money in online based on friend's idea, and 43.1% of respondents invest the money based on social media and advertisement. Mostly of respondents doesn't have investment knowledge that show in table 7, they invest the money on online platform based on the social media's advertisement and other people opinion. They believe that when they invest the money in online platform to gain the amount that show in advertisement like jackpot, instant profit etc.. and also, they invest the money in online that refer by their friend or relative without any hesitation and also they didn't verify the site or stock value in the market when they invested.

Table 9: Type of online investment

S.no	Types of investment	Percent
1	scheme	41.2
2	stocks	43.1
3	other	15.7
	Total	100.0

In this table 9 shows that 43.1% of respondents invest the money on stock market and 41.2% of respondents invest the money on scheme. In this analysis, the stock value will be depended on the company and product value in the market, sometimes its will be increase the value or decease the value but the seller or third app or company promote the low value stock to buyer to sell it in higher price, most of the respondents get scam like that. In cryptocurrency investment , the currency will be same value for all region, but the currency value maybe up and down in sometime, that why cryptocurrency fraud had low rate among the sample.

Table 10: Specific type of online investment

S.no	Specific type	Percent
1	business development	2.0
2	cash and carry	2.0
3	chit	2.0
4	company stocks	5.9
5	fund	3.9
6	income stock	2.0
7	job offer	7.8
8	online gaming	7.8
9	phone stocks	2.0
10	provident fund	29.4
11	share market	2.0
12	trading	27.5
13	value stocks	2.0
14	work from home	3.9
	Total	100.0

In this table 10 shows that 29.4% of respondents will be delude in provident fund and 27.5% of respondents will be scam in trading. In this data, respondents get scam by various type of trading and stocks, more than 15% of various type of stocks fraud that got by respondents like income stocks, phone stocks, value stocks etc., and also some respondents get scam by various job scheme(14%).

Table 11: Realize of fraud

S.no	Realization	Valid Percent
1	link disable	7.8
2	no response	72.5
3	tell by someone	3.9
4	Online message	5.9
5	other	9.8
	Total	100.0

In this table 11 show that 72.5% of respondents realize the fraud due to the no response, 7.8% respondents realize the fraud when the link disables after they deposit the money. In online platform, they easily rid off their contact from the people, when the respondent deposit the large-scale amount in the online investment, they lost the contact from the receiver and also when they invest the money through the third-party link, it will disable after receiving the large amount.

Table 12: Family Known About Victimization

S.NO	Addressing the victimization to their family	Percent
1	Yes	60.8
2	No	39.2
	Total	100

The table 12 shows that 60.8% of victims' families were aware of the online investment fraud victimization, while 39.2% were not informed. This indicates that a significant number of victims were open about their experience, although a considerable portion still preferred to keep it private, likely due to shame, guilt, or fear of judgment. Among those who did share their experience, reactions varied. The most common responses was scolding, followed by feeling bad, expressions of sadness, and anger. A notable of families had no reaction, which may reflect emotional detachment or a lack of understanding of the issue. Others responded with advice, raised family issues, or simply acknowledged the situation without strong emotional responses. This range of reactions

highlights the emotional and psychological toll on victims, who may face additional stress from family dynamics. Negative family responses such as scolding or anger can deepen the victim's sense of shame and discourage reporting, while supportive reactions can help in coping and recovery. This underscores the importance of awareness and sensitization programs for families to foster empathy and constructive support when such incidents occur.

Table 13: online investment after victimization

S.no	Respondents	Valid Percent
1	Yes	13.7
2	No	86.3
	Total	100.0

In this table 13 shows that 86.3% of respondents does not invest again in online platform, 13.7% of respondents invest the money again in online platform. More than 85% of respondents don't investment money in online platforms because most of respondents had some psychological problems due to the victimization, and their family reaction leads to a burden on them. Most of the respondent had stress, when they loss the money in the online investment, and others had hypertension and pressure.

Table 14: Advertisement platform

S.no	Platform	Percent
1	Add in video game	23.5
2	Social media	56.9
3	Telegram bot	17.6
4	Other	2.0
	Total	100.0

In this table 14 shows that social media had high level of advertisement related to the online investment among respondents 56.9%, and 23.5% respondents frequently watch the advertisement of online investment in video games and also they received the advertisement and promotion in telegram bot 17.6%. some respondents mention that

, they received message from social media like telegram, WhatsApp, Instagram for promoting the investment company and also brainwash the respondents to invest their company or product. Few respondents received call from investor to promote their company and product.

Table 15: Frequency level of advertisement

S.no	frequency	Valid Percent
1	low	21.6
2	medium	49.0
3	high	29.4
	Total	100.0

In this table 15 shows that 49% respondents had moderate level of advertisement and promotion receive in their social media feed and other application but 29.4% respondents had high level of advertisement and promotion in their social media feed and other application. Now a day, the investment related advertisements telecast in the television and there promote the private and also third-party companies for investment with disclaimer, but it will be indicating factor to individual for online investment and also increase the greediness of individual to gain more money. It built the trust without hesitation while their watching the advertisement in television and social media, but it led to misuse the trust or using their trust for committing the fraud.

Table 16 : Investment based on promotion video

S.no	Investment based on promotion video	Percent
1	Yes	13.7
2	No	86.3
	Total	100.0

Table 16 shows that only 13.7% of respondents made investment decisions based on promotional videos, while a significant 86.3% did not. This

suggests that although promotional videos have some influence, the majority of individuals are either cautious or rely on other sources for making investment decisions. It reflects a degree of scepticism among investors toward promotional content and may indicate growing awareness of potential online scams. However, the 19.6% who were influenced by such videos still represents a notable vulnerability, highlighting the need for stricter regulation and awareness campaigns targeting misleading promotional material in digital platforms

Table 17: Third party app or company

S.no	Investment in Third party app or company	Percent
1	yes	56.9
2	No	43.1
	Total	100.0

In this table 17 shows that 56.9% of respondent invest the money on third party app or link and 43.1% of respondent didn't invest their money on third party app or link. Many respondent mention the third-party links and companies but most of the respondents doesn't remember the link and few respondents mention the whatsapp and telegram for received the message related online investment by unknown contact. Many well know banks are involve in online investment fraud, these banks are well famous in overall India. These types of third party app , few are available in officail site or app and other link and app suggest by social media through the unknown link in their site.These data based on the sample perceptive

Table 18: Report

S.no	Report	Percent
1	Yes	68.6
2	No	31.4
	Total	100.0

In this table 18 shows reporting the fraud, most of the responders report the fraud 68.6% and other of doesn't report the fraud 31.4%. In this analysis, most of the respondents doesn't know the helpline number of cybercell

Table 19: Reason for non-report behavior

S.no	Reason	Percent
1	Reported	70.6
2	don't know to report	17.6
3	many days passed	7.8
4	no proof	3.9
	Total	100.0

Most of the victim doesn't know about how to report the fraud in cyber cell. In this table 19 that reason for respondents doesn't report the fraud.17.6% of respondents doesn't know how to report the fraud in cyber cell and the particular site,7.8% of respondents mention that they realize the fraud after many day so they didn't report the fraud. 3.9% of respondent mention that they had no proof against the raiders. This table shows the many reasons for not cooperating in the report system, the reason for not reporting whether it may be personal, it shows that most of the people about 50percent of the people reported the incident and still many people are not aware how to report the incident to police or cyber cell, they are unaware of the incident to report and some have responded about the days passed by ,which shows the people of Chennai in a small percentage are least bothered about reporting, while many of them do not have a proof to report ,and they think without proof their report won't last long, so people are hesitant to report if they don't have a proper proof or proper reason, they cannot simply go behind each door to door for reporting so the government should provide a system for reporting and other complaint cell which is friendly to people of Chennai for the online investment fraud.

Table 20: Reported platform

S.no	Reported platform	Percent
1	Cybercell	71.4
2	particular app	20.0
3	both	8.6
	Total	100.0

Table 20 provides crucial insights on the response habits of victims of online investment scam by highlighting their reporting activity. The fact that a sizable majority of respondents—roughly 71.4%—reported the occurrence to the cyber cell suggests that formal cybercrime reporting procedures are becoming more widely recognized and trusted. This pattern is a reflection of the growing public awareness that cybercrime is a significant problem that needs government action. However, 20% of victims decided to report the scam exclusively through the specific website or platform wRemarkably, 8.6% of respondents reported the fraud to both the cyber unit and the particular website, indicating a two-pronged response mechanism meant to guarantee maximum accountability and traceability. This conduct implies that a small percentage of victims have a proactive mindset, which may be impacted by prior experiences or increased digital literacy. Overall, the data highlights the need for more comprehensive awareness campaigns and efficient, user-friendly reporting mechanisms that encourage more victims to use multiple channels for faster and more effective redressal of online fraud, even though the high percentage of cyber cell reporting is encouraging.here it happened, perhaps because it was convenient, available right away, or they were unaware of official reporting channels like the Cyber cell..

Table 21: Response

S.no	Responded platform	Percent
1	Cybercell	76.7
2	Particular site	16.7
3	Both	6.7
	Total	100.0

In this both table 20 and 21 show that 71% of victim report the fraud in cybercell and they get 76% response from cybercell, and other report the fraud in particular site(20%) and they get response from 16.7% in particular site. More than 75% of respondent state that there had no report option in third party app and site or link.

Table 22: Money recovery

S.no	Money recovery	Valid Percent
1	yes	37.3
2	no	62.7
	Total	100.0

This table shows whether the people recovered their lost money, but from the response it is seen that lost money was recovered by people in only a small number this shows that when there is a financial loss it is very difficult to recover the money lost, and overall it is seen that this leads to huge pressure about 63 percent of the people didn't get money which means that a large number of respondents didn't get their financial loss and it leads to huge problem and those got money have correct proof and reported to the cyber cell , as of all the online investment case study shows that people involved online investment fraud when they are investing in an online investment it is hard to get back their money ,even after reporting .a small portion of 37 percent got their money back which is only a small percentage of money, and this online investment scams if not reported correctly and if used with protection can lead to money loss and financial loss

leading to problems in getting back the money or recovery the money mainly in the field of online investment fraud.

### Major Finding

- ❖ Among the respondent, Male will be 58.8% responded and women will be 41.2% responded. Most of the responder will be male and also male will be victim more than women.
- ❖ The most of the respondent will be under age of 30-40 (41.2%) and also most of respondents well educated and also most of responder finish the graduated, Under Graduated (52.9%) and Post graduated(39.2%).
- ❖ More than 40% of people succeed in their investment, nearly 60% people get scammed in their first investment.
- ❖ More than 80% of respondents doesn't investment knowledge. Most of respondents doesn't have investment knowledge when they invest the money, they invest the money based on the other indicating factor like advertisement, friends etc. 52.9% of respondents invest the money in online based on friend's idea, and 43.1% of respondents invest the money based on social media and advertisement.
- ❖ 43.1% of respondents invest the money on stock market and 41.2% of respondents invest the money on scheme. 29.4% of respondents will be delude in provident fund and 27.5% of respondents will be scam in trading. various types of trading and stocks, more than 15% of various types of stocks fraud that got by respondents like income stocks, phone stocks, value stocks etc., and also some respondents get scam by various job scheme(14%).
- ❖ 72.5% of respondents realize the fraud due to the no response, 7.8% respondents realize the fraud when the link disables after they deposit the money.
- ❖ 49% respondents had moderate level of advertisement and promotion receive in their social media feed and other application but 29.4% respondents had high level of advertisement and promotion in their social media feed and other application. social

media had high level of advertisement related to the online investment among respondents 56.9%, and 23.5% respondents frequently watch the advertisement of online investment in video games and also, they received the advertisement and promotion in telegram bot 17.6%.

- ❖ 56.9% of respondent invest the money on third party app or link and 43.1% of respondent didn't invest their money on third party app or link. Many respondents mention the well know bank(29.4%) and most of respondents doesn't remember the site or link (9.8%). 5.9% of respondent mention the whatsapp.
- ❖ most of the responders report the fraud 68.6% and other of doesn't report the fraud 31.4%. In this analysis, most of the respondents doesn't know the helpline number of cybercell. Most of the victim doesn't know about how to report the fraud in cyber cell.
- ❖ 71% of victim report the fraud in cybercell and they get 76% response from cybercell, and other report the fraud in particular site(20%) and they get response from 16.7% in particular site. More than 75% of respondent state that there had no report option in third party app and site or link. most of respondent 62.7% doesn't get their money back but who are complaint in cybercell about the fraud their get money back.

## DISCUSSION

Online investment fraud has become a serious menace in India targeting people from all walks of life. New data shows that 58.8% of victims are male and 41.2% are female. Most of these accesses are in the age of 30 to 40 and have higher education degrees, such as under graduation and postgraduation. Many of them have no idea what investing is, and some are victims of a series of fraud."

Many victims claimed they had been lured into an investment by social media ads and recommendations by friends or family. About 52.9% were influenced to invest following recommendations from friends, while 43.1% were swayed by online promotions. Notably, 56.9 percent

of surveyed victims invested through third-party applications or through spear-phishing links without confirming if the platforms were authentic or not. Investment modalities comprised stock marketing (43.1%), diverse schemes (41.2%), provident fund pyramids (29.4%), and trading (27.5%). Shockingly, more than 15% fell victim to scams involving other types of stocks, like income, phone and value stocks, and 14% were duped by questionable job promises.

The realisation that that money was gone came late for many – 72.5% realised that something was wrong when they didn't hear back from the platform, while 7.8% only realised when links to trades vanished after they paid their money. In spite of the wide spread of these scams, a total of 68.6% reported the incidents; However, 31.4% didn't and unawareness of reporting mechanism is the most reason behind. Of those who reported, 71 per cent reported to the cyber cell with a response rate of 76 per cent while 20 and a quarter per cent reported at the specific sites with of 16.7 per cent. More than 75% reported that there was no way to report such scams on third-party apps or websites, and 62.7% were unable to get their money back. But those who reached the cyber cell's door, the odds of getting the money back were much better.

The emotional and psychological damage caused by these scams is real. Many victims were well-educated, but felt too embarrassed, or worried they would not be believed to report their experiences. Their vulnerability was additionally aggravated by the misplaced trust in familiar sources, whether friends, or known platforms, without due diligence. High-frequency commercials touting looking easy money also led many to believe that they could easily earn big from these scams.

In order to fight this rising threat, it is important to increase financial literacy. The introduction of financial literacy programs that concentrate on basic investment and risk assessment may help people to have a greater control over their lives. One should ensure that whatever platform you are putting your money into is for real especially if it is from a recommendation of a friend or from some random ads from online. In the events of fraudulent transaction, timely reporting to the cyber cell helpline 1930 or on the National Cyber Crime Reporting Portal could lead to fund recovery. When it comes to advertisements, specifically ones with guaranteed returns, it is imperative to be careful and

not invest in unsolicited third-party apps or links before doing proper due diligence.

The sudden spike in online investment scams highlight the importance of joint vigilance and the obligation to take precocious action to protect a person from potential financial scams.

Self-victimization define that the person exaggeratedly expresses the feeling as a victim or their victim hood to seek other attention or play victim role for some benefits or manipulating other. Cyber victim also will be under the self-victimization because there are voluntarily went to the trap of scammer, there gave all data and money for their individual benefit, but they are willingly giving all the personal detail and money to stranger without any verification. In this study, few people became self-victimization like received some message from social media about investment related their business, without any verification they contact to stranger and investment some amount after that strange made up the fake success investment report to the investor, and put some words to investor to invested more money. Investor invested the money several time to the strange , that amount came around 1.4 crores, after that the strange didn't response to the investor after the amount received. In this incident, the investor gave all their savings to the scammer voluntarily but they blame the scammer, they didn't accept their mistake. In this research, most of the respondent become the victim like this. Most of the scammer used the pig butcher scam method to the people for gain their trust to invest more money in their fake product or stocks.

## CONCLUSION

In this research of ONLINE INVESTMENT FRAUD: AN EMPIRICAL STUDY OF VICTIM PERCEPTION IN CHENNAI, we can see that most of the victim will be educated and also working person but there had no knowledge about online investment while investing because there are investing their money based on the social media advertisement and their friend. And also, there had no criminal activity in online investment fraud but some sample say that online loan app involves in crime activity like threatening, video morphing threat etc.

In report behaviour, most of the victim doesn't know about the complaint process and helpline number and also golden hour in cyber cell, who all report the

fraud in cyber cell, they get money recovered from the raiders. In India , our government took many precautions measure and create the awareness through advertisement and caller tones etc., but our people successful ignored the cyber awareness from Government and fell into the fraud traps in online. People should aware before investing the money in online and gain the investment knowledge and verify the company or site or product before investing.

## Reference

- Ansar, S. A., Yadav, J., Dwivedi, S. K., Pandey, A., Srivastava, S. P., Ishrat, M., ... & Khan, R. A. (2021). A critical analysis of fraud cases on the Internet. *Turkish Journal of Computer and Mathematics Education*, 12(12), 2164-2186.
- Aqib, M. S., & Sukiati. (2024). Crime of Fraud (Pig Butchering Scam) Through Social Media in the Perspective of Islamic Criminal Law. *Journal Equity of Law and Governance*, 4(2), 231-237. <https://doi.org/10.55637/elg.4.2.10013.231-237>
- Baker, H.K. and Puttonen, V. (2017), "Trap 2: Being Deceived by Other Investment Frauds", *Investment Traps Exposed*, Emerald Publishing Limited, Leeds, pp. 183-226. <https://doi.org/10.1108/978-1-78714-252-720171006>
- Baker, H.K. and Puttonen, V. (2019), "Trap 2: Becoming a Victim of Investment Frauds and Scams", *Navigating the Investment Minefield*, Emerald Publishing Limited, Leeds, pp. 79-103. <https://doi.org/10.1108/978-1-78769-053-020191005>
- Balachandar, A. (2022). Financial Frauds in India: An Analysis. *Jus Corpus LJ*, 3, 213.
- Balakrishnan, V., Ahhmed, U., & Basheer, F. (2025). Personal, environmental and behavioural predictors associated with online fraud victimization among adults. *PLOS ONE*, 20(1), e0317232. <https://doi.org/10.1371/journal.pone.0317232>
- Balogun, O. S., Akangbe, T. A., Fagbamila, O. D., & Aigbovbioisa, F. O. (2024). Internet users' perception of the prevalence of online investment fraud and victimisation in Nigeria. *Gusau Journal of Sociology*, 4(2), 169-181. <https://doi.org/10.57233/gujos.v4i2.13>

- Bar Lev, E., Maha, L.-G., & Topliceanu, S.-C. (2022). Financial frauds' victim profiles in developing countries. *Frontiers in Psychology*, 13, 999053. <https://doi.org/10.3389/fpsyg.2022.999053>
- Bartels, K. C. (2000). "Click Here to Buy the Next Microsoft": The Penny Stock Rules, Online Microcap Fraud, and the Unwary Investor. *Indiana Law Journal*, 75(1), 353–377. Retrieved from <https://www.repository.law.indiana.edu/ilj/vol75/iss1/18/>
- Bele, J. L. (2020). Financial Scams, Frauds, and Threats in the Digital Age. *Modern Approaches to Knowledge Management Development*, 39.
- Bharne, S., & Bhaladhare, P. (2023). Comprehensive Analysis of Online Social Network Frauds. In *Advances in Data-Driven Computing and Intelligent Systems* (pp. 23–40). Springer. [https://doi.org/10.1007/978-981-99-3250-4\\_3Ebin.pub+2](https://doi.org/10.1007/978-981-99-3250-4_3Ebin.pub+2)
- Button, M., McNaughton Nicholls, C., Kerr, J., & Owen, R. (2014). Online frauds: Learning from victims why they fall for these scams. *The Australian and New Zealand Journal of Criminology*, 47(3), 391–408. <https://doi.org/10.1177/0004865814521224>
- Cross, C., Richards, K., & Smith, R. G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice [Electronic Resource]*, (518), 1–14. <https://search.informit.org/doi/10.3316/informit.300566903591621>
- Cyber, I., & Coordination, C. (2024). Recent Cybercrime Trends in Financial Frauds Cybercrime Trends. August.
- Cybercrime, N., Portal, R., Cyber, I., & Coordination, C. (2024). First four months of 2024 see 7,000 online complaints per day: Investment scams, sextortion and other frauds that Indians lost Rs 1,750 crore to - Times of India. 2023–2024.
- Dalvadi, V. M., & Sharma, M. (2015). Online Investment Fraud: Nature, Pedagogy, and Remedy for Investors. *Allana Management Journal of Research*, 5(1), 30–35.
- Deb, S. and Sengupta, S. (2020), "What makes the base of the pyramid susceptible to investment fraud", *Journal of Financial Crime*, Vol. 27 No. 1, pp. 143–154. <https://doi.org/10.1108/JFC-03-2019-0035>
- Dong, W., Liao, S., & Zhang, Z. (2018). Leveraging financial social media data for corporate fraud detection. *Journal of Management Information Systems*, 35(2), 461–487. <https://doi.org/10.1080/07421222.2018.1451954>
- Graham, W. (2014). A Quantitative Analysis of Victims of Investment Crime. Financial Conduct Authority. Retrieved from <https://doczz.net/doc/8434584/a-quantitative-analysis-of-victims-of-investment-crime>
- Graham, W. (2014). A quantitative analysis of victims of investment crime. London: Financial Conduct Authority.
- Henderson, L. (2003). *Crimes of Persuasion: Schemes, Scams, Frauds: how Con Artists Will Steal Your Savings and Inheritance Through Telemarketing Fraud, Investment Schemes and Consumer Scams*. Coyote Ridge Publishing
- Jamuna, S. (2023). A STUDY ON MITIGATING ONLINE FINANCIAL FRAUDS IN DEHGAM.
- January, B. (2024). Here is how much Indians lost to cyber frauds between Jan and Apr of 2024. 2023–2024.
- Kamalludin, I., Suhendar, H., Pratami, B. D., Yaqin, 'A., & Afifah, N. (2022). Criminal Law Treats for Online Gambling Performers: Investment Fraud Modes. *Dialogia Iuridica: Journal Hukum*, 14(1), 26–51. <https://doi.org/10.28932/di.v13i2.5252>
- Lacey, D., Goode, S., Pawada, J., & Gibson, D. (2020). The application of scam compliance models to investment fraud offending. *Journal of Criminological Research, Policy and Practice*, 6(1), 65–81. <https://doi.org/10.1108/JCRPP-12-2019-0073>
- Marguerite Deliema, Doug Shadel, Karla Pak, Profiling Victims of Investment Fraud: Mindsets and Risky Behaviours, *Journal of Consumer Research*, Volume 46, Issue 5, February 2020, Pages 904–914, <https://doi.org/10.1093/jcr/ucz020>
- Mueller, E. A., Wood, S. A., Hanoach, Y., Huang, Y., & Reed, C. L. (2020). Older and wiser: age differences in susceptibility to investment

fraud: the protective role of emotional intelligence. *Journal of elder abuse & neglect*, 32(2), 152–172. <https://doi.org/10.1080/08946566.2020.1736704>

- Nash, R., Bouchard, M., & Malm, A. (2013). Investing in people: The role of social networks in the diffusion of a large-scale fraud. *Social Networks*, 35(4), 686–698. <https://doi.org/10.1016/j.socnet.2013.06.005>
- Pressman, S. (1998). On financial frauds and their causes: Investor overconfidence. *American Journal of economics and sociology*, 57(4), 405-421.
- Rusch, J. J. (1999, June). The “social engineering” of internet fraud. In *Internet Society Annual Conference*, [http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g\\_2.htm](http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm).
- Singh, K. N., & Misra, G. (2023). Victimization of investors from fraudulent investment schemes and their protection through financial education. *Journal of Financial Crime*, 30(5), 1305–1322. <https://doi.org/10.1108/JFC-07-2022-0167>
- Subhash, K. S., Sandhya, M., Uddhav, T. A., & Kiran, T. " The Rise of Social Media-Driven Stock Market Investment Scams: Analysing Financial Fraud in The Age of Social Media
- [Cyber Frauds in India: Here is how much Indians lost to cyber frauds between Jan and Apr of 2024 | India News - Business Standard](#)
- <https://effectivelaws.com/economic-offences-wing-eow/>
- [https://en.wikipedia.org/wiki/Indian\\_Cyber\\_Crime\\_Coordination\\_Centre](https://en.wikipedia.org/wiki/Indian_Cyber_Crime_Coordination_Centre)
- [https://en.wikipedia.org/wiki/Information\\_Technology\\_Act,\\_2000](https://en.wikipedia.org/wiki/Information_Technology_Act,_2000)
- <https://i4c.mha.gov.in/about.aspx>
- <https://indiankanoon.org/search/?formInput=tnpid%20act&pagenum=18>
- <https://timesofindia.indiatimes.com/technology/tech-news/first-four-months-of-2024-see-7000-online-fraud-complaints-per-day-investment-fraud-sextortion-and-other-scams-that-indians-lost-rs-1750-crore-to/articleshow/110476085.cms>
- [Ponzi Scheme: Definition, Examples, and Origins.](#)

- [What Is a Pyramid Scheme? How Does It Work?.](#)