Advanced International Journal for Research (AIJFR)

E-ISSN: 3048-7641 ● Website: www.aijfr.com ● Email: editor@aijfr.com

Cyber Financial Fraud: A Major Threat to the Indian Society

Ruth Lalrinliani[1], Dr. Mridula Devi[2]

[1]Research Scholar, University School of Law and Research,
University of Science and Technology, Meghalaya
[2]Associate Professor, University School of Law and Research,
University of Science and Technology, Meghalaya

Abstract

Technological advancement results various growth in the society. Development brings improvements but it also has a negative impact in the society. India also witnessed different progress including technological evolution however, this progression multiply different types of crimes especially cyber crimes. Easy accessibility of computer and internet improves many areas of our life but crime rates become increasing as cyber criminals discovered new ways to commit different crimes by using new technology which we never known before. Among various cyber crimes, cyber financial fraud becomes one of the common crimes in the 21st Century. It is a multi-trillion dollar business for criminal organizations all around the world. India could not easily escape from this type of crime as the main activity of the criminal is financial gain which greatly attempted the cyber criminals. Financial crimes and cyber crimes are invariably linked as a significant amount of financial fraud takes place through digital technologies and the main goal of cyber criminals is illegal gains from the victims. By committing cyber financial fraud, the criminal whether being an individual or group of individuals by using computer or computer technology can easily taking money or property of the victims without their permission. If positive steps could not be taken, this type of crime will become a major threat to the development of Indian society.

Keywords: Cyber crime, Computer, Criminals.

1. Introduction

Development in 21st Century brings different benefits to human and the society at large. Improvement in new technology becomes one of the key features of computer world. Since the onset of new millennium various technological innovations have happened which improved our lives in different ways. As we know that development brings positive as well as negative impact to the society. In todays world, cyber crime became one of the common crime in various developed countries. Many great inventions also led to negative remark in the society. As computers and internet are now an integral part of our day to day life cyber crime becomes an emerging serious threat.

Statement of the problem

The nature and characteristics of cyber-crimes are different as compared to the traditional crimes. Even though it is one of the most common crimes worldwide, the criminals applied new tactics and new technology to commit the crime and this makes it difficult to have reliable preventive measures. Even the victims are not much aware of the incident during the time of the crime and this makes it difficult to arrest the criminals red handed. Many people in the society are not aware of this crime and so a large number of cases are unsettled and this makes it difficult to have the exact number of cyber crime incident records by the authority.

Objective of the Study

The objective of the study is to find out common types of cyber crimes especially cyber financial fraud which largely affect the Indian society, the current cyber financial fraud problems faced by the general people and different preventive measures taken by the authority.

Meaning of Cyber Crime

Cyber crime in its simplest term refers to all criminal activities done by using the medium of communication devices. Such common devices includes computers, mobile phones, tablets etc. Internet is one of the most important elements in committing cyber crime because by using internet connection different kinds of crime are committed through various devices. By the term cyber crime we mean illegal use of computer and internet to commit various criminal acts. Cyber crime is a kind of crime that happens in 'cyberspace'. The word Cyber Space is coined by author William Gibson in his sci-fi novel 'Neuromancer' written in 1984 which means something happened in the world of computer and the Internet. The term 'Cyberspace' therefore refers to the virtual world created by mankind using computers and networking through which they interact and exchange information using multiple languages or communication protocols that are created by humans so that one computer can talk to another computer[1].

Definitions of Cyber Crimes

No Indian laws gave the specific definition of cyber crime. However different writers and jurists gave their own definitions. In cyber crime, computer or computer network is one of the most essential elements to commit a crime. Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks.[2]

According to the Organization for Economic Cooperation and Development (OECD) which was the first international organization that initiated guidelines for computer crime[3] "Computer related crime is considered as an illegal, unethical, or unauthorized behaviour relating to the automatic processing and transmission of data".

[1] S.R. Myneni, Information Technology Law (Cyber Laws) 467 (Asian Law House 2013)
[2] Manish Kumar Chaubey, Cyber Crimes & Legal Measures 6 (Regal Publications 2017).
[3] OECD https://www.cybercrimelaw.net/OECD.html (last visited Jan 9, 2026).

Black's Law defined cyber crime as "An evolving area or law that is applies to computers and the various activities over the internet and networks."

Encyclopedia Britannica: The Encyclopedia Britannica defines 'cyber crime' as any crime that is committed by means of special knowledge or expert use of computer technology.

Cyber Crime & Traditional Crime

As truly said, crime have "…always depended on the force, vigour and movement of public opinion from time to time and country to country and even in the same country, from decade to decade".[4] The fact of crime was closely related with the culture and society of the people. Even though crime could be committed anywhere by anyone, there are various elements which largely effect the mode or types of crimes committed in the particular area. In India, criminal jurisprudence can be traced back to the days of Manu where Manu had recognized assault, theft, robbery, false evidence, slander, criminal breach of trust, cheating and rape as offences.[5] Development especially technological development brings changes the modes of crimes committed in the society. As compared to the traditional crime, cyber crime is easily committed as physical contact of the victim is not needed by the criminals and it could easily be completed from any places by using technological devices.

Various technological inundations like evolution of computers and technical excellence of the masses results in the advancement of the society. The first generation of computer which took place between 1940s to 1950s mainly performs arithmetic calculations by exploiting vacuum tubes. The second generation of computers falls between the 1950s to 1960s, the third generation in the 1060s to 1970s, the fourth generation from the 1970s and now we are in the fifth generation which began from 1980s till date. Since the first generation the characteristics of computer technology changes continuously for the betterment. It continuously improved the speed, accuracy, size and price to urge the form of the fashionable day computer.[6]

The technology behind the fifth generation of computers is Artificial Intelligence simply known as Artificial Intelligence (AI). It allows computers to behave like humans and in some cases the works of computers are much reliable than the human being. It is often seen in programs like voice recognition, area of medicine and entertainment and it is difficult to differentiate between the works of computers and humans. Within the field of game playing also it has also shown remarkable performance where computers are capable of beating human competitors.[7] This enormous development in technology on the other hand results negative impact in the society. Different new crimes which never known in the primitive society took place in different levels. As compared to the traditional common crime the effects of cyber crime also known as computer crime is immeasurable.

[4] R.C. Nigam, Principles Of Criminal Law 3 (Asia Publishing House 1965).

[5] Talat Fatima, Cyber Crimes 62 (Eastern Book Company 2021).

[6] Generations of Computers, https://www.geeksforgeeks.org/generations-of-computers-computer-fundamentals/ (last visited Jan 10, 2026).

[7] Id.

Cyber Financial Fraud

Cybercrime in finance is the act of obtaining financial gain through profit-driven criminal activity, including identity fraud, ransomware attacks, email and internet fraud, and attempts to steal financial account, credit card, or other payment card information. In other words cyber financial fraud includes activities such as stealing payment card information, gaining access to financial accounts in order to initiate unauthorized transactions, extortion, identity fraud in order to apply for financial products, and so on. The financial services industry is a very lucrative target and is, therefore, heavily impacted by the rise of cyber criminality.[8] Everyone may fall victim to cyber financial crime as one of the main aim of cyber criminals is to gain illegal monetary gain from others.

In general words, Cyber Financial Fraud or Cyber Financial Crime is a situation where the victim easily loses his or her money dishonestly through any kind of electronic devices. Different online payment systems like UPI, Internet banking, mobile banking and online banking systems have got a huge rise all over the world. Even though it makes life easier it in turn effects the security protection of user's financial accounts. In recent years, online payment system and online fraud have gained much attention in the business market. It is easier for the people to practice cashless system in the business activities but on the other hand this results in the increasing rate of cyber financial fraud.

The cyber criminals applied different tactics to defraud the victims and there are different schemes which are performed in online services to cheat others. Some common examples are:

1) Credit card online fraud – It is very common way of defrauding the cyber crime victims. Using of another's credit card or debit card information without their permission is illegal and it is called as credit card or debit card fraud. Due to carelessness and sharing debit/credit card number and secret pin many people loss huge amount and the culprits are very difficult to trace as it involved several criminals to commit the crime.

2) ATM skimming - It is also universal global financial cyber crime. A criminal affixes a skimmer to the outside or inside of an ATM to collect card numbers and personal identification number codes. The criminal then either sells the stolen data over the internet or makes fake cards to withdraw money from the compromised accounts.[9]

3) E-mail online fraud – This is another common method to defraud others. E-mail is very inexpensive and anyone can create email with or without showing their real identity and a person can have multiple e-mails. By distributing fraudulent emails, the victims without having second thought responded the cyber criminals by providing their personal details like account number, ATM card number and secret pin. The most common tactic used by cyber criminals is sending those e-mails as banker and police so they can easily deceived the victims.

4) Setting up fake website – This is another common financial fraud practiced by cyber criminals. Fake companies and fake business enterprises displayed false information to defraud the target person.

[8] What Is Financial Cybercrime, And How Can We Prevent It? (Jan 10, 2026, 1:00 PM) https://www.visma.com/blog/what-is-financial-cybercrime-and-how-to-prevent-it/

[9] Manish Kumar Chaubey, Cyber Crimes & Legal Measures 21 (Regal Publications 2017)

Without careful examination customers spent huge amount of money without getting the products. As the fake website it is difficult to trace the creators of those fake websites. In some cases, the cyber criminals establishes fake investment schemes, fake online offer or fake advertisements and by baiting and enticing offer of huge amount of returns the cyber criminals easily attract the target's attention.

5) Scam lotteries - Scam lotteries are another game plan designed by the cyber criminals to defraud the victims. The scammers usually informed the victims as they won a huge amount of money and for claiming that amount they make them to share their personal and banking details. In that way the victims easily lose huge amount of money and results even bankruptcy to some victims.

Cyber Financial Fraud and Indian Society

Even though the world got introduced to the computer technology in late forties, India bought its first computer in 1956 and it was nothing more than a number crunching machine and was huge in size. When time comes various developments took place in the Indian society. As compared to other countries, India has enormous contribution in the area of Information Technology and due to this advancement the conventional law was not adequate enough for dealing with cyber crimes. So the cyber law i.e., the Information Technology Act, 2000 was passed by the Indian Parliament to control the arena of the cyber world and introduce digital safety measures; the cyber laws are concentrated upon the internet and cyberspace. However, even though various measures were taken the Indian society still in a dark place due to cyber crimes.

On 17th December, 2025 the Hon'ble Minister of State for Home, Shri Bandi Sanjay Kumar informed the Rajya Sabha that more than seven thousand crore rupees have been saved in more than 23 lakh complaints so far through the Citizen Financial Cyber Fraud Reporting and Management System.[10]

In India one of the most alarming tactics played by the cyber criminals is the "digital arrest" scam. The criminals contact random person often by using phone or video calls and informed them as they are under investigation for fabricated offense like making dirty money through drug trafficking, drug dealing, tax evasion, using fake Aadhar card or bank account and other illegal activities. They threatened the victim to arrest or defaming them and pressure them to transfer large amounts to exonerate them from the false accusations. The panic victims believing the false imputation transfer large sums to them to "clear their name." even though digital arrest is not included in the Information Technology Act, 2000 or any other Indian laws, this is one of the rapidly growing forms of cyber crimes in the present Indian society.

The Hindu in an Article titled "Elderly woman loses ₹20 crore to 'digital arrest' fraud; 3 held" published in March 20, 2025 reported that an 86-year-old woman from south Mumbai lost more than ₹20 crore of her savings over two months to a 'digital arrest' fraud. As per the complaint filed by the woman, she had received a call from a man, who claimed to be a CBI officer, and told her that based on her Aadhaar card, a bank account was opened which was used for money laundering. The man then told her that the

[10] Akashvani News, https://www.newsonair.gov.in/over-rs-7000-crore-saved-through-citizen-financial-cyber-fraud-reporting-and-management-system/ (last visited on Jan 9, 2026).

case was being investigated by the Central Bureau of Investigation (CBI) and she should stay in her room, while threatening her with "digital arrest". He also threatened to arrest her children.[11]

NDTV News in the article titled "Gold Sold, Deposits Broken: Gujarat Doctor Loses 19 Crores to Digital Arrest" published in July 31, 2025 again reported that in that month, a senior woman doctor in Gujarat's Gandhinagar was kept under 'digital arrest'. The scammers used a multi-way approach to target the doctor and convince her that she was in trouble. A woman caller introduced herself as she was from the Telecommunications Department, another caller said he was Sub-Inspector; three other callers introduced themselves as public prosecutors and notary official. For over three months, they forced her to break fixed deposits, take loans, and blackmailed into paying more than Rs 19 crore.[12]

Apart from these, various types of cyber crimes took place the Indian society every day. According to Live Mint Report, "In the past six years, Indians lost over ₹52,976 crore to various cyber frauds and cheating cases". The report reveals rise in financial crimes including investment traps, digital arrest, online scams, banking frauds, and cyber phishing, across the country.[13]

To lessen cyber financial crime the Indian Government took important steps since 2019. In order to control the rising Cyber Financial Fraud, the Government of India under the guidance of the Ministry of Home Affairs introduced Indian Cyber Crime Coordination Centre which is also known as the I4C scheme. Under this scheme various centers was established for the identification and investigation of cyber-crimes such as National Cybercrime Reporting, the Platform for Joint Cybercrime Investigation Team, the National Cybercrime Threat Analytics Unit (TAU), the National Cybercrime Training Centre (NCTC), National Cybercrime Forensic Laboratory (NCFL) Ecosystem Cybercrime Ecosystem Management Unit, and National Cybercrime Research and Innovation Centre.

One of the major objectives of 14C scheme was identifying research problem relating to cyber crime all over India and to priotize research and development activities for new technologies not only within India but also outside the country. It is used to prevent the exploitation of cyberspace for furthering the reason of terrorist and extremist groups. It also recommends the changes required in the present cyber laws to balance technology and international cooperation.[14] Whenever a cyber financial fraud happens, the victim can report the incident by calling at 1930 or lodge a formal complaint on the National Cybercrime Reporting Portal at www.cybercrime.gov.in.

The procedure to lodge a complaint on National Cyber Crime Reporting Portal are as follows:

1) When a cyber financial fraud occurs, a victim can access the website www.cybercrime.gov.in and get registered as a new user.
2) After registration is success, the user needs to click "Report Cyber Crime".

[11] The Hindu, https://www.thehindu.com/news/cities/mumbai/elderly-woman-loses-20-crore-to-digital-arrest-fraud-3-held/article69353437.ece (last visited Jan 8, 2026).

[12] NDTV, https://www.ndtv.com/india-news/digital-arrest-19-crore-robbed-in-102-days-gujarat-doctors-digital-arrest-nightmare-8990774 (last visited Jan 8, 2026).

[13] Live Mint News, https://www.livemint.com/news/india (last visited Jan 9, 2026).

[14] Gurpreet Kaur Dutta, Cyber Frauds in India: Overview & Redressal, Finology Blog (Jan 9, 2026, 4:00 PM), https://blog.finology.in/Legal-news/redressal-for-cyber-financial-frauds-in-india.

3) The reporter then selects his or her State.
4) Next to the "Frauds: Classification and Reporting" and then the complaint will be marked to the cyber cell, and the FIR will be lodged at the police station where the offence is alleged to be committed.

Since no legislation specifically provides cyber financial fraud as a separate offence, RBI issued guidelines for these cases, in which the provisions of Indian Penal Code (now Bharatiya Nyaya Sanhita) will be applied. Whenever financial fraud is committed either by way of online mode or otherwise, time is considered as the utmost essence, and the RBI guidelines entail the person to report the same without making any delay. Obviously, the law favours the vigilant and does not rescue the one who does not stand for his rights. If the victim without any delay reports the commission of financial fraud to the authority, the investigation process will runs smoothly and the chances of recovering the fraudulent amount becomes higher.

When the cyber crime victim filed a complaint and no action has been taken, the victim has the right to approach the Superintendent of Police under Section 173(4) of BNSS to lodge an FIR. Even after that, if no action is taken again, the victim can report the same to the Judicial/Metropolitan Magistrate under Section 175 (3) of BNSS and seek a direction to lodge the FIR. The main reason to lodged FIR is to keeps the criminal procedure in motion and mandates the Police to conduct an investigation, for cyber crimes. When a case has been registered the investigation processes may be conducted by the Cyber Cell in the Police Department who have jurisdiction and submitted reports of findings to the Court having judicial jurisdiction.

Conclusion

In today's digital age information technology plays vital role in our day to day life. Internet makes our life easy, so we were much depending on it and our life becomes incomplete without internet connection. However, the phenomenal growth of internet has provided new computer crimes in the society which never happened before. Even though the Indian Parliament enacted the law which specifically deals with cyber crime, crime rate become increasing and also the total amount of money losses through cyber financial crime are enormous. The Central Government and State Government took various steps to prevent cyber crimes by launching different schemes, organizing different awareness programmes, strengthening cyber security and cyber police station, the results are unsatisfactory. It is necessary for every one to take some positive steps to minimize cyber crime. It is our prime duty to support different initiatives taken by the authority. We are all responsible to prevent cyber crimes as we have an obligation to protect our society.