VOLUME 5 | ISSUE 4

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

MODUS OPERANDI IN FINANCIAL CYBERCRIME

- Jyoti & Himanshu Ranjan[1]

ABSTRACT

This research paper deals with the modus operandi in financial cybercrime in which the main statement of problem is the identification of modus operandi presents significant challenges for investigators even in conventional crimes, but these difficulties are substantially magnified in cybercrime investigations. The digital nature of cybercrimes creates a fundamentally different landscape compared to traditional criminal activities, making pattern recognition and methodology analysis considerably more complex. While conventional crimes leave physical evidence and spatial patterns, cybercrimes often cross jurisdictional boundaries, utilize sophisticated technical approaches, and can be executed through layers of anonymization—all factors that complicate the investigator's ability to establish clear operational signatures of perpetrators.

This paper deals with the analysis of modus operandi in different types of financial cybercrime through various case studies. Also, it contains how the judiciary dealt with this modern problem and what laws are available in the Indian legal system to curb this problem. Some measures are provided through which people can save themselves from financial cybercrime.

In conclusion, the paper affirms that digital forensics is indispensable in contemporary law enforcement and cybersecurity, and calls for further advancements in forensic tools and, legal frameworks to effectively combat digital crimes in the future.

INTRODUCTION

The NCRB maintained information regarding certain categories of fraud for cybercrime such as credit/debit cards, ATMs, online banking frauds, OTP frauds and others. As per the

[1] Students at Chanakya National Law University

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

https://www.ijalr.in/

data published by the NCRB, details of cases registered under fraud for cybercrimes (involving communication devices as medium/target) for the period of 2022 is as under[2]: -

Cases Registered under Fraud for Cyber Crimes: -

Credit/Debit cards	1665
ATMs	1690
Online Banking frauds	6491
OTP frauds	2910
Others	4714
Total	17470

The use of the internet in India is growing rapidly. According to a recent Telecom Regulatory Authority of India (TRAI) survey, currently we have 971.50 million internet subscribers.[3] The rapid expansion of internet access, while offering cyber citizens diverse opportunities across entertainment, education, and other domains, has simultaneously led to an increase in cybercrime, with technologically adept criminals creating novel security challenges. According to the findings of survey on Economic Crime in India in Global Economic Crime Survey 2024, about 59 per cent of Indian organisations faced financial or economic fraud over the past 24 months, an 18 per cent higher than the global average of 41 per cent and marks a 7 per cent increase compared to India's 2022 survey results.[4]

Recent cyberattacks on multinational companies and financial institutions highlight the growing threat of cybercrime to organizations, with more businesses falling victim to these attacks. This surge can be attributed to the increasing adoption of e-business, internet usage, and e-commerce.[5] Financial cybercrimes, which include cheating, credit card fraud, money laundering, forgery, and online investment scams, are subject to penalties under both the Bhartiya Nyaya Sanhita (BNS) and Information Technology (IT) Act.

[2]Cyber Fraud And Digital Harassment, Ministry of Home Affairs, https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2080186#:~:text=The%20'National%20Cyber%20Crime%20Reporting%20Portal'%20(https://cybercrime.gov.in),on%20cyber%20crimes%20against%20women%20and%20children , (Accessed 13 Feb. 2025).
[3]https://www.trai.gov.in/, Telecom Regulatory Authority of India, (Accessed on 10th February, 2025).
[4]PwC's Global Economic Crime Survey 2024 — India outlook, PwC, PwC's Global Economic Crime Survey 2024 – India outlook, (Accessed 13 Feb. 2025).
[5] Prof. R.K. Chaubey, "An Introduction to Cyber Crime and Cyber law", Kamal Law House, 2012.

The Price Waterhouse Coopers organization, which deals with the economic crime survey, has defined economic crime in cyber world as *"an economic crime committed using computers and the internet. It includes distributing viruses, illegally downloading files, phishing and pharming, and stealing personal information like bank account details. It's only a cybercrime if a computer, or computers, and the internet play a central role in the crime, and not an incidental one."*[6]

Modus operandi, or the method of committing a crime, is influenced by multiple factors including the technological capabilities of both the criminal and target, the perpetrator's and victim's knowledge and habits, as well as the various rules, regulations, and processes that govern both technology use and human behavior.

While technology historically played a minor role in criminal activities, the rise of information and computer technology across all aspects of life has transformed crime significantly. When comparing traditional and cybercrime methods, it's evident that technology's capabilities and vulnerabilities have become central to criminal activities in the digital age, with cyberspace essentially serving as a new medium for committing conventional crimes through different means, making cybercrime distinct in its modus operandi from traditional criminal behavior.

MODUS OPERANDI IN CONVENTIONAL CRIME AND FINANCIAL CYBERCRIME: A COMPARATIVE ANALYSIS

Traditional crimes, often referred to as blue-collar crimes, are crimes that are more easily recognisable and involve physical acts of violence or property destruction. These crimes are typically associated with individuals from lower socio-economic backgrounds, although this is not always the case. *Whereas* Dr. Debarati Halder and Dr. K. Jaishankar define cybercrimes as: *"Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)"*[7] There are distinct methodological patterns

[6]Cybercrime: protecting against the growing threat, Global Economic Crime Survey, https://www.pwc.pt/pt/deals/images/2011_global_economic_crime_survey.pdf, (Accessed on 10th February, 2025).

[7]Rashmi Saroha, Profiling a Cyber Criminal,http://www.ripublication.com/irph/ijict_spl/ijictv4n3spl_06.pdf , (Accessed on 14th March, 2025).

between conventional criminal activities and digital financial offenses, highlighting how perpetrator behaviors, technical approaches, and investigative challenges fundamentally differ across these evolving criminal landscapes.

1. **Physical vs. Digital Footprints**

In conventional financial crimes, culprits deposit physical traces such as fingerprints, DNA, surveillance footage, or eyewitness testimony. Physical entry points, tool markings, and personal contact with victims can be investigated. However, financial cybercrimes produce cyber footprints which are purposefully hidden through virtual private networks addresses, and encrypted transmissions. While traditional criminals need to physically travel areas, cybercrime perpetrators may access from any place in the world without the necessity of being there physically, which renders conventional methods of analyzing a crime scene redundant.

2. **Jurisdictional Complexity**

Conventional financial crimes usually have geographical constraints, and investigators can use domestic laws and operate under established jurisdictional boundaries. The modus operandi in such cases is limited by physical restraints and insider information. Financial cybercrimes, on the other hand, regularly traverse multiple international jurisdictions, with criminals, victims, servers, and financial transactions potentially touching dozens of countries. Such jurisdictional complexity presents extreme difficulties in establishing patterns because attackers intentionally leverage these boundaries to make it difficult to investigate and prosecute.

3. **Risk and Reward**

The cybercrime offers low risks and high rewards as compared to traditional crimes. For example, in an externally perpetrated cybercrime, a fraudster infiltrates a banking system, remotely, to steal money or personal information. The fraudster is at a lesser risk when compared to someone who physically steals assets from an organization. There are fewer risks when committing cybercrime. The fraudster is not present at the location; hence the chances of getting caught are less. It is difficult for law enforcement agencies to follow traditional investigative steps to prosecute the perpetrator owing to the different location

and jurisdiction of the perpetrator. The perpetrators can return to the scene of the crime with relatively minimal fear of detection.[8]

4. Scale and Automation

Conventional financial crimes are bound by physical limitations—a bank robber can only rob one location at a time, and new planning must be done for the next crime. The modus operandi is modified for each target depending on individualized security measures and physical configurations. Cybercrimes of a financial nature can be automated and scaled exponentially, and the same attacks can be run simultaneously against thousands of victims using methods such as phishing campaigns, credential stuffing, or distribution of ransomware. Mass-scale automation radically alters how investigators need to study patterns, going beyond individual incidents and examining larger campaign signatures.

5. Technical Sophistication and Evolution

Conventional financial crime methods evolve relatively slowly, with techniques like check fraud, confidence schemes, or physical theft maintaining consistent core elements across decades. The modus operandi changes tend to be incremental, allowing investigators to build expertise and predictive models based on historical patterns. Financial cybercrimes evolve at remarkable speed, with attack methodologies constantly incorporating new vulnerabilities, evasion techniques, and technological developments. This fast-paced technological development implies that cyberattack signatures can shift significantly within weeks, and investigators need to keep revising their analytical models and technical expertise.

6. Identity Concealment and Attribution

In conventional financial crimes, criminals have to appear physically, even if under disguise or fake identities. Their modus operandi involves how they handle their physical appearance and interactions—issues that can result in identification based on witness accounts or behavioral patterns. Financial cybercriminals hide behind multiple layers of technical disguise, utilizing compromised infrastructure, false identities, and cryptocurrency-based transactions to mask their activities. Attribution becomes

[8] Economic Crime in India: an ever increasing phenomenon, Global Economic Crime Survey 2011, India, Price Waterhouse Coopers, 2011. also available at https://www.pwc.in/assets/pdfs/publications-2011/economic-crime-survey-2011-india-report.pdf (Retrieved on 17th March, 2025).

exceptionally difficult when multiple criminal groups use the same infrastructure, or advanced actors intentionally impersonate others' techniques to construct false flags.

MODUS OPERANDI IN FINANCIAL CYBER FRAUD

With the advancement of technology, the cyberfraud cases are increasing and the criminals are well equipped with the technology and use it against the poor people and the person having low or no knowledge about the technology. Many time we came across such incident that a link came in the message while clicking on it all the details and transactions are looted and which is further used for extortion, blackmailing and many more. Some of the techniques used to do cyber fraud by the criminals are as follows along with their modus operandi: -

1. **SPOOFING**

Website spoofing is a deceptive practice that takes several forms based on the perpetrator's intentions. Financial fraud is the most common motivation, with attackers creating convincing replicas of banking and payment websites to steal credentials and financial information from unsuspecting victims. These sophisticated imitations often include identical logos, layout, and domain names with slight variations that are difficult to notice.[9]

Beyond financial targets, website spoofing extends to impersonating other legitimate sites for various purposes: personal entertainment, spreading misinformation, harvesting personal data, or causing embarrassment to specific organizations or communities. These non-financial spoofs can damage reputations, mislead users.

Case Study- Nykaa email spoofing case- Fraudsters tricked Nykaa by spoofed emails which redirected Nykaa's payment intended for one of its Italian suppliers to their own bank accounts.[10]

Modus Operandi- The criminals imitated a valid supplier's email address. Emails from such an address would've appeared as authentic, as the sender's address clearly showed a

[9]Deb Shinder, Understanding E-mail Spoofing, www.windowsecurity.com, April 6 2005 also available at http://searchsecurity.techtarget.com/definition/email-spoofing (Retrieved on 17th March, 2025).

[10]Nykaa Email Spoofing Case, https://logix.in/blog/nykaa-email-spoofing-case/#:~:text=Spoofed%20Emails%20Are%20A%20Major,was%20out%20of%20the%20bag, (Retrieved on 17th March, 2025).

real supplier's email address. The fraudsters sent a fake email to Nykaa, asking the cosmetics retailer to redirect the payment to another bank account. They gave taxation as a reason for this change of account. It was only afterwards when Nykaa asked for confirmation of the payment did it find out their grave mistake. The original Italian supplier denied all claims of such an email. The sum was of an astounding Rs 62 Lakh, which could never be recovered.

2. PHISHING

Phishing scams trick victims into revealing sensitive information by masquerading as legitimate organizations. These attacks rely on technical deception, using disguised links in emails that appear trustworthy but actually direct users to fraudulent websites. Techniques like misspelled URLs(like http://www.google.com@membcrs.abc.com/) and misleading subdomains help criminals create convincing illusions that capture financial data, passwords, and personal details from unsuspecting victims. While browsers have patched some vulnerabilities, phishers continuously develop new methods to bypass security measures and exploit user trust.[11]

Banks often try to shift phishing liability to customers, claiming negligence when users respond to fraudulent emails. However, legal precedent suggests otherwise. Under India's Information Technology Act 2000 (especially after 2008 amendments), phishing violates multiple provisions and causes wrongful loss to customers, triggering Section 43 adjudication rights. Banking law has long established that forgery cannot be held against customers regardless of sophistication. Furthermore, banks' failure to implement digital signatures for internet transaction authentication potentially makes them negligent under Sections 79 and 85, holding them liable for offenses originating from bank computers. This stance was reinforced when Bank of India accepted responsibility for a phishing fraud in Bangalore, compensating the victim with full reimbursement plus interest.[12]

Case study- A client spoke with their supplier about an upcoming payment, with the supplier promising to email an invoice. Subsequently, the client received a legitimate-looking $30,000 AUD invoice from the supplier's Xero account containing "updated" banking details. The client processed the payment as anticipated. Six months later, the

[11] Phishing, n." OED Online, March 2006, Oxford University Press. Oxford English Dictionary Online. and also at https://en.wikipedia.org/wiki/Phishing (Retrieved on 17th March, 2025).
[12] http://www.naavi.org/cl_editorial_09/edit_dec_23_09_boi_phishing.htm(Retrieved on 17th March, 2025).

situation unraveled when the supplier called about an unpaid invoice. Realizing something was amiss, the client immediately reached out to Smile IT to investigate the discrepancy, suggesting they had fallen victim to a sophisticated payment diversion scam.[13]

Modus Operandi-

1. The supplier sent the invoice using their legitimate Xero account.
2. The email was intercepted by the hacker during transit via SMTP Injection Attack.
3. The hackers bypassed authentication, gaining unauthorised access to the email and decrypted the email and created a replica invoice with the fraudulent bank details.
4. The hackers altered the return path – making it look like it was sent from the legitimate supplier.
5. The fraudulent invoice was sent to the client user.
6. Client users had MFA enforced on their email accounts.

3. ONLINE FRAUD

Identity theft follows successful phishing or spoofing attacks when criminals acquire victims' credentials. Armed with stolen usernames, passwords, account numbers, and personal details, perpetrators quickly monetize this information through unauthorized transactions. They may drain bank accounts via electronic transfers, make fraudulent credit card and debit card purchases, open new financial accounts, apply for loans, or engage in online shopping sprees—all while posing as the legitimate user. The damage often extends beyond immediate financial losses, as victims face damaged credit scores, account lockouts, and the lengthy process of reclaiming their digital identity, sometimes discovering the breach only after significant harm has occurred.

Case Study- In January 2021, Bangalore police registered a strange case where fraudsters used a blocked debit card and withdrew a huge sum. The complainant told police that he had only Rs 19 balance and yet criminals could run away with more than seven lakh rupees.[14]

[13]Smile it, Phishing Attack case study, https://www.linkedin.com/pulse/phishing-attack-case-study-smile-it, (Retrieved on 17th March, 2025).
[14]Emerging Cyber Crimes In India: A Concise Compilation, Bureau Of Police Research And Development, National Cyber Crime Research & Innovation Centre, (August, 2021)Ministry of Home Affairs, Government of India , https://bprd.nic.in/uploads/pdf/20220405035311525361 2EmergingCyberCrimesinIndia.pdf, (Retrieved on 17th March, 2025).

Modus Operandi-

1. Criminals used a blocked debit card of a customer who had only Rs 19 in account balance.
2. Somehow, they succeeded in duping the bank itself by withdrawing more than seven lakh rupees by using the blocked debit card.
3. It is suspected by Police that there must be some bug in the backend of the Banking software which let this fraudulent transaction take place.

4. CYBER EXTORTION

In the digital realm, cyber extortion functions as a virtual form of blackmail. Rather than physical abductions or hostage-taking, online criminals deploy sophisticated digital strategies to intimidate targets through internet-based channels. Frequently, these malicious actors claim possession of sensitive personal information and demand payment to prevent its public disclosure, creating a psychological rather than physical threat to extract funds from victims.

According to a research paper "Cyber extortion can take many forms. It can be very lucrative, netting attackers millions of dollars annually. A typical cyber-attack may result in a demand for thousands of U.S. dollars. Furthermore, payment does not guarantee that further attacks will not occur, whether the attacks continue from the same cyber extortionists or a different group attacks". [15]

Case Study- According to a recent report published in Indian Express, India is among the top 10 sextortion mail source countries. Sextortion is a type of phishing crime where the criminals send emails to the victims demanding money by claiming to have private photos or videos of an individual.[16]

Modus Operandi-

1. Criminals send emails to vulnerable persons. They claim that they have accessed the compromised photographs or videos of the victims.
2. Victims get afraid and try to negotiate with the criminals without informing anyone.

[15]Emerging Cyber Crimes In India: A Concise Compilation, Bureau Of Police Research And Development, National Cyber Crime Research & Innovation Centre,(August, 2021)Ministry of Home Affairs, Government of India , https://bprd.nic.in/uploads/pdf/20220405035311525361 2EmergingCyberCrimesinIndia.pdf, (Retrieved on 17th March, 2025).

[16]Indian Express, https://indianexpress.com/article/technology/tech-news-technology/india-top-10-sextortion-country-how-to-protectfrom-cyber-attack-6380192/, (Retrieved on 17th March, 2025).

3. Criminals demand ransom and continue to exploit.

5. DIGITAL ARREST

A digital arrest is a fraudulent tactic used by cybercriminals to falsely accuse individuals of breaking the law, often claiming the existence of a digital arrest warrant. These scammers pose as officials from organizations such as customs, income tax department or even central investigative agencies. Their goal is to intimidate you into paying money or providing sensitive personal details.

In the digital arrest there is 4 common element: -

1. Authority- The cybercriminals shows their authority to victims that they belongs to the particular organisations like income tax department, enforcement officer, etc. and told them that now you are under arrest.
2. Trust- By showing fake Id cards, papers they create trust with the victims and now they easily fall into the trap.
3. Fear- In this the cybercriminals shows the evidence that you are committing some wrong to develop fear in the minds of the victims. Now, the ordinary prudence mind will stop functioning and will easily oblige and be manipulated.
4. Urgency- once you fall into their trap then they will show the urgency and demand money to get out of this offence.

Case study- Hyderabad police arrested 31-year-old Mohammed Zubair Ahmed at RGI Airport upon his return from Dubai for his involvement in a digital arrest scam. Operating multiple bank accounts for fraudulent transactions, Zubair and associates impersonated officials to extort money from victims, including one who transferred Rs 55 lakh after being deceived by supposed FedEx executives and fake police.[17]

Modus Operandi: -

1. Initial contact through impersonation of FedEx courier company representatives
2. False claims about packages containing illegal items (drugs) seized by customs
3. Escalation to fake police communication via Skype for increased credibility
4. Presentation of forged documents related to money laundering to intimidate victims

[17]Indian Express, https://www.newindianexpress.com/cities/hyderabad/2025/mar/16/hyderabad-, (Retrieved on 17th March, 2025).

5. Creation of a false sense of urgency and legal jeopardy through "digital arrest" threats
6. Demands for payments into specific bank accounts for supposed police clearance
7. Use of international base of operations (Dubai) to evade immediate detection
8. Operation of multiple bank accounts to receive and disperse fraudulently obtained funds

9. ONLINE RECRUITMENT FRAUD

Job scammers prey on desperate job seekers by advertising fraudulent employment opportunities, then demanding upfront fees or sensitive personal information that enables identity theft. These schemes, while less prevalent than other cybercrimes, are becoming increasingly common as scammers create convincing fake company profiles to extract financial gain or harvest valuable personal data from unsuspecting applicants eager to secure employment.

Case study- A 40-year-old teacher from Nanjundapuram, Coimbatore fell victim to an elaborate online scam, losing Rs 28.55 lakh after responding to a part-time job offer shared through social media. Initially lured by a modest Rs 1,500 payment for part-time work, she was gradually manipulated into making investments, ultimately transferring funds through 17 separate transactions. Upon realizing she had been defrauded, she filed a report with the cybercrime police. [18]

Modus Operandi-

1. The thieves initially gained credibility by making a small, honest payment for uncomplicated work, and followed up with investment demands after gaining trust.
2. Compartmentalizing the scam into several small payments instead of one large one.
3. This allowed the criminals to capitalize on psychological breakpoints that make incremental loss less threatening than a single large extraction.
4. The use of social media for initial contact provided both anonymity for the perpetrators and a veneer of legitimacy through the platform's perceived social validation.

[18]TOI Tech Desk, Online Scam: How a woman lost Rs 28.55 lakh in 'part-time job scam' in 17 transactions | - Times of India, (Retrieved on 17th March, 2025).

10. PONZI SCHEMES

Ponzi schemes are particularly insidious, enticing victims with promises of high returns on investments. Once enough funds are collected, the scammers vanish, often through seemingly legitimate websites and apps that attract those seeking easy income.

Case Study- The Odisha Crime Branch has arrested a female cybercriminal in Delhi for an Rs 87 lakh investment fraud. The victim, a Bhubaneswar-based private company employee, was added to a fake WhatsApp group called "101 Stock Discussion Group" led by someone posing as a professor. The fraudsters convinced the victim to invest in stocks through counterfeit applications, resulting in approximately Rs 87 lakh being deposited into various bank accounts. Authorities seized a mobile phone, SIM cards, and identification documents as evidence.[19]

Modus Operandi-

1. They created a seemingly legitimate investment community through WhatsApp, establishing credibility with a fake professor persona.
2. They gradually build trust before directing the victim to fraudulent stock trading applications.
3. The criminals used multiple bank accounts across different institutions to distribute and obscure the money trail, making the scheme harder to trace while creating a false sense of legitimacy through organized group discussions about investments.

11. CRYPTOJACKING

Cryptojacking covertly utilizes victims' computers for cryptocurrency mining without their consent, while ransomware attacks encrypt files and demand cryptocurrency for decryption keys. In severe cases, if ransoms are unpaid, attackers might deploy cryptojacking malware using the victim's resources.

Case Study- In the US it has been reported that digital frauds involving cryptocurrencies are on a rise. Criminals have started deceiving people in the name of investments in

[19]Indian Cybercrime Coordination Centre (14C), https://i4c.mha.gov.in/cyber-digest.aspx, (Retrieved on 17th March, 2025).

cryptocurrencies. Many are running crypto currency Ponzi schemes and promises people of incredibly high returns. [20]

Modus Operandi-

1. When someone sees the value of crypto currency go up and decides to invest for high returns, he approaches an online trader.
2. The trader asks the investor to buy some amount of cryptocurrency using cash and he also takes a commission for doing that.
3. After some time the investor wants to encash the profits and asks the trader to do so. The trader asks for more out-of-pocket commission and even goes out of contact.

LAW DEALING WITH FINANCIAL CYBERCRIME

India's legal framework for combating financial cybercrimes has evolved significantly in response to the digital transformation of its economy. As traditional financial crimes increasingly migrate to digital platforms, India has developed a multi-faceted legal approach combining specialized cyber legislation with amended traditional criminal statutes. Some of them are as follows: -

The Bharatiya Nyaya Sanhita of 2023[21] establishes comprehensive legal provisions addressing various fraudulent activities: -

Section 316 (Criminal breach of trust)[22] criminalizes situations where a person entrusted with property dishonestly misappropriates or converts it for unauthorized purposes, betraying the confidence placed in them by the property owner. This covers embezzlement by employees, agents, or fiduciaries who abuse their positions of trust.

Section 318 (Cheating and dishonestly inducing delivery of property)[23]penalizes deceptive practices where individuals use fraudulent representations to convince victims to surrender their property. This addresses schemes where perpetrators intentionally mislead others through false statements or promises, causing financial harm to the victims.

[20]Emerging Cyber Crimes In India: A Concise Compilation, Bureau Of Police Research And Development, National Cyber Crime Research & Innovation Centre,(August, 2021)Ministry of Home Affairs, Government of India , https://bprd.nic.in/uploads/pdf/20220405035311525361 2EmergingCyberCrimesinIndia.pdf, (Retrieved on 17th March, 2025).
[21]The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, (India).
[22]The Bharatiya Nyaya Sanhita, 2023, sec. 316, No. 45, Acts of Parliament, 2023, (India).
[23]The Bharatiya Nyaya Sanhita, 2023, sec. 318, No. 45, Acts of Parliament, 2023, (India).

Section 336 (Forgery for the purpose of cheating)[24] targets individuals who create false documents with the specific intention of defrauding others. This provision covers activities like fabricating identification documents, contracts, or certificates to facilitate financial scams or identity theft.

Section 344 (Falsification of accounts)[25] addresses the deliberate manipulation of financial records, ledgers, or accounting documents to conceal fraud or misrepresentation. This provision is particularly relevant to corporate fraud, tax evasion, and schemes involving the deliberate misreporting of financial information.

The word Fraud is clearly defined under **The Indian Contract Act, 1872**. **Section 7**[26] - "Fraud" means and includes any of the following acts committed by a party to a contract or with his connivance or by his agent, with intent to deceive another party thereto or his agent, or to induce him to enter into the contract.

The **Prevention of Money Laundering Act (PMLA) of 2002**[27] serves as comprehensive legislation designed to combat money laundering and associated financial offenses in India. The Act places mandatory reporting requirements on financial institutions to flag suspicious transactions and grants significant powers to authorities for confiscating assets linked to money laundering operations, particularly those derived from criminal proceeds. This legislation creates a robust framework for tracking illicit financial flows and disrupting attempts to legitimize funds obtained through unlawful activities.

India's **Information Technology Act 2000**[28] addresses internet fraud through several key provisions. **Section 43(d)**[29] penalizes those who damage data, with "damage" defined as destroying, altering, adding, modifying, or rearranging computer resources. This covers fraudulent activities like false stock issuance and market manipulation schemes. **Section 65**[30] criminalizes tampering with computer source code, which includes program listings, commands, designs, and analysis. Additionally, **Section 66**[31] addresses wrongful loss

[24]The Bharatiya Nyaya Sanhita, 2023, sec. 336, No. 45, Acts of Parliament, 2023, (India).
[25]The Bharatiya Nyaya Sanhita, 2023, sec. 344, No. 45, Acts of Parliament, 2023, (India).
[26]The Indian Contract Act, 1872, sec. 7, No. 9, Acts of Parliament, 1872, (India).
[27]The Prevention of Money-Laundering Act, 2002, No. 15, Acts of Parliament, 2003, (India).
[28]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000,(India).
[29]The Information Technology Act, 2000,sec. 43(d), No. 21, Acts of Parliament, 2000,(India).
[30]The Information Technology Act, 2000, sec. 65, No. 21, Acts of Parliament, 2000,(India).
[31]The Information Technology Act, 2000, sec. 66, No. 21, Acts of Parliament, 2000,(India).

caused by destroying or altering data, diminishing its value, or otherwise injuriously affecting computer resources.

Section 447 of the Companies Act, 2013[32] addresses corporate fraud with severe penalties. It prescribes imprisonment and financial penalties for individuals found guilty of manipulating company accounts or defrauding shareholders. This provision is designed to deter fraudulent activities in corporate governance and protect stakeholder interests.

The Securities and Exchange Board of India (SEBI) Act, 1992[33] establishes SEBI as the regulatory authority for India's securities markets. The Act implements stringent rules to combat fraudulent practices including insider trading, market manipulation, price rigging, and other securities frauds. Through these comprehensive regulations, SEBI aims to ensure market integrity and protect investor interests in India's financial markets.

The Reserve Bank of India Act, 1934[34] **and Banking Regulation Act, 1949**[35] empower the RBI with comprehensive authority to regulate and supervise banks throughout India. These acts specifically enable the RBI to monitor and address fraudulent banking practices, including money laundering, unauthorized transactions, and misuse of banking services. Through these legislative frameworks, the RBI maintains oversight of banking activities to ensure financial system integrity.

JUDICIAL APPROACH

Since the advancement of technology, the cybercrime is increasing so it became the duty of our judiciary system to give the judgment which relief the people and punish the cyber criminals so that in future such people develop fear before committing such cybercrimes. Our judiciary has given many important judgments recently which is shaping our judiciary in dealing with such cases of cybercrime. The guidelines and decisions given by our courts are important in dealing with such evolving issue. Some of the recent judgments are as follows: -

Vineet Jhavar v. State of NCT of Delhi[36], Justice Swarana Kanta Sharma said that "These online frauds contribute to eroding the trust of people in the online financial transactions

[32]The Companies Act, 2013,sec. 447, No. 18, Acts of Parliament, 2013, (India).
[33]The Securities And Exchange Board Of India Act, 1992, No. 15, Acts of Parliament, 1992, (India).
[34]The Reserve Bank Of India Act, 1934, No. 2, Acts of Parliament, 1934, (India).
[35]The Banking Regulation Act, 1949, No. 10, Acts of Parliament, 1949, (India).
[36]Vineet Jhavar v. State of NCT of Delhi, 2023 LiveLaw (Del) 1248.

and thus, discourage the newcomers into entering the digital realm, which negatively impacts the overall economy of the country," The Delhi High Court, denying bail to a man accused of online fraud, observed that cybercrimes erode public trust in digital financial platforms, which contradicts India's "Digital Bharat" aspirations. Justice Sharma noted that cyber criminals' tactics constantly evolve and emphasized courts' responsibility to address grievances of technology users defrauded of their money. The judge highlighted how app developers exploit cyber-illiterate individuals by misusing accessed personal data for extortion and fraud, pointing out that this particular scheme—involving transactions of approximately ₹140 crores—targeted vulnerable citizens during the COVID-19 pandemic who had invested small amounts hoping for survival loans.

Atanu Choudhary v. State of Punjab,[37]the Court held that to thoroughly investigate the modus operandi adopted by the accused and his other co-accused, his custodial interrogation was necessary.

Pune Citibank Mphasis Call Center Fraud (2005)[38] The 2005 Citibank-Mphasis incident involved call center employees who exploited customer trust to obtain PINs, subsequently transferring funds from legitimate US accounts to fraudulent ones. Rather than employing sophisticated hacking techniques, perpetrators exploited procedural vulnerabilities, memorizing customer information to circumvent security protocols during entry and exit searches. The court classified this as cybercrime since it involved unauthorized electronic account access. Defendants faced charges under Section 43(a) and 66 of the Information Technology Act, 2000, along with Sections 420, 465, and 467 of the Indian Penal Code. The ruling established that the IT Act's scope extends to crimes involving electronic documents, treating them equivalently to offenses using traditional materials.

In Re: In matter of tackling the issue of 'Digital Arrest Scams'[39], The Rajasthan High Court has taken suo-moto cognizance of increasing "Digital Arrest Scams," noting that new criminal laws lack provisions addressing this issue. Justice Dhand emphasized the urgent need for public awareness campaigns, as these scams involve fraudsters posing as

[37]Atanu Choudhary v. State of Punjab, 2025 SCC OnLine 824.
[38]Hiya Chowdhary, Pune Citibank Mphasis Call Centre Fraud Case, Lawfullegal, https://lawfullegal.in/pune citibank-mphasis-call-centre-fraud-case/, (Retrieved on 17th March, 2025).
[39]Nupur Agrawal, No Provision For Law Enforcement To Conduct Arrests Via Video Calls: Rajasthan HC Takes Suo Motu Cognizance Of 'Digital Arrest Scams', https://www.livelaw.in/high-court/rajasthan-high court/rajasthan-high-court-suo-motu-cognizance-digital-arrest-scams-281745, Accessed on 10th March,2025.

law enforcement, using fear tactics and AI to extort money from victims through fake "digital arrests."

MEASURES TAKEN TO CURB FINANCIAL CYBER FRAUD

As we know the law is currently evolving on the matter of cybercrime and since this area is wide and evolving continuously it became mandatory for the citizens to became aware about such frauds and what is the remedy and where we can file complaints, etc. generally, in such cases the reaction and action time is very less and that's why many times the police or investigators also doesn't able to help the victims. So it became important for the people to take safety precautions which helps us from such online frauds, extortion and financial crimes.

Essential Internet Safety Precautions for Internet Users: -

1. **Comprehensive Internet Security Suite-** Deploy robust anti-malware software from reputable vendors to create a protective shield around your digital presence. These comprehensive solutions provide real-time scanning, threat detection, and automatic quarantine capabilities, safeguarding your sensitive information from sophisticated malware variants and emerging threats.
2. **Robust Password Management-** Implement complex passwords combining uppercase and lowercase letters, numbers, and special characters, changing them at regular intervals. Consider using a password manager to generate and store unique credentials for each service, and always clear browser history when using shared computers to prevent credential theft.
3. **Systematic Software Updates-** Maintain a rigorous schedule for updating operating systems and security applications to patch known vulnerabilities that cybercriminals actively exploit. Enable automatic updates wherever possible, as even brief delays in implementing security patches can create significant exposure windows for sophisticated attacks.
4. **Mobile Device Security Optimization-** Implement biometric authentication, app-level permissions management, and two-factor verification on mobile devices accessing sensitive information. Restrict app installations to official stores, enable remote wiping capabilities, and maintain current operating system versions to protect against mobile-specific vulnerabilities.

5. **Legal Compliance-** Adhering to regulatory frameworks governing data protection, privacy standards, and industry-specific security requirements ensures both legal protection and security baseline. Compliance programs should incorporate regular audits, documentation of security measures, and updated policies reflecting changing legal landscapes.

CONCLUSION

Financial cybercrime has experienced an unprecedented upper hand in today's cyber world. Unlike conventional crime, cybercrime poses different challenges to law enforcers. The modus operandi in conventional crime acts as an essential identifier of criminals and deters crimes of recurrence. Cybercriminals, on the other hand, have ever-changing modes of operation that do not demand physical presence, thus greatly making it hard for investigative agencies to identify culprits and solve cases.

This sudden growth in cybercrime is due to three main vulnerabilities: technical flaws in systems, psychological vulnerabilities in human behavior, and loopholes in legal frameworks. To effectively tackle cybercrime, a holistic approach that addresses all three aspects at the same time is necessary.

As cybercriminals evolve their attacks, it should be noted that all are under potential threat. Awareness is one of our most effective defenses against these advanced scams. By studying the working behavior of different types of scams, individuals and entities can identify telltale signs before falling into the trap.

Basic preventative steps can significantly minimize exposure. These include the use of two-factor authentication, healthy skepticism of unsolicited messages, and regular updating of security measures. Finally, being vigilant and aware is the best defense against the ever-changing environment of cyber threats. Legal reform is also another crucial aspect in effectively combating cybercrime. Creating and adopting specialized law meant to combat the specific issues of cybercrime will help seal any gaps that currently exist in legal procedures and serve to adequately penalize culprits.