INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 3 | Issue 6 [2025] | Page 435 – 443

UNDERSTANDING THE LEGAL PATHWAY OF A CYBER FRAUD INVESTIGATION

-Shagun Ranjan Kumar[1]

ABSTRACT

The increasing use of digital platforms for investment and financial transactions has led to a parallel rise in cyber investment fraud in India. This article examines the legal framework governing such frauds, with reference to the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. It analyses the legal responsibilities of intermediaries and the conditional nature of safe harbour protection under Section 79 of the IT Act. The study highlights how due diligence obligations under Rules 3 and 4 play a critical role in identifying, preventing, and responding to fraudulent online activity. By mapping the procedural and substantive legal pathways available to victims and enforcement agencies, this study underscores the importance of intermediary accountability in combating organized cyber fraud. The article argues that effective enforcement of due diligence norms is essential to ensure user protection, preserve digital trust, and strengthen India's cyber governance framework.

Keywords

Cyber Investment Fraud; Intermediary Liability; IT Act, 2000; Bharatiya Nyaya Sanhita, 2023; Safe Harbour; Due Diligence; Digital Platforms

[1] 2nd Year B.A. LL.B., Manikchand Pahade Law College, Chhatrapati Sambhajinagar.

INTRODUCTION

Picture this: a regular person scrolling through their phone, dreaming of a better future. A friendly message pops up from someone who seems to know all about smart money moves. They share tips, show flashy charts with skyrocketing profits, and soon guide the person to a sleek app or website that promises easy riches through stocks, crypto, or forex trading. Deposits go in smoothly; bank transfers, UPI, even crypto wallets, but when it's time to cash out? Excuses pile up: extra fees, account freezes, or the platform simply vanishes.

This is the dark side of online investing today. Scammers build trust slowly, sometimes over weeks, acting like mentors or even romantic interests. They use fake apps that look real, complete with live dashboards showing fake gains. Victims keep pouring in money, chasing the illusion of wealth, only to lose everything. Billions are wiped out every year as these traps spread through social media, various platforms groups, and shady websites.

Take one real story: a hardworking professional was convinced by an online "expert" to invest in a stock. Over months, the app showed steady 10 – 15% monthly returns. Excited, the person added more funds by savings, loans, even sold property. Then came the shock: withdrawal requests were denied, support went silent, and the website disappeared overnight. Over lakhs of rupees gone.

To fight back, rules like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, often just called the IT Rules, step in as a frontline defence. Trying right into that fight against cyber investment cons and trading tricks, these rules push for user verification, like linking accounts to real phone numbers, so scammers can't hide behind fake profiles. It's all about building trust; if a platform slacks off, it loses its legal shield and could face the music under broader laws. In following article we will deal with a what legal provision will apply on cyber investment fraud case and related judgements and about what due diligence does Intermediaries have under IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

KEY LEGAL PROVISIONS FOR CYBER INVESTMENT FRAUD

In India multiple laws that empower victims of online fraud Provisions under Information Technology Act, 2000[234]:

The IT Act, 2000 is India's primary cyber law. It directly addresses various forms of online fraud.

1. Section 43 – Under Section 43 of Chapter IX of the Act, whoever, without the permission of the person in charge of the computer system, accesses, Penalty for unauthorized access or damage to computer systems.
2. Section 65 – Under section 65 of Chapter XI of the Act, Whoever knowingly or intentionally conceals, destroys, or alters any computer source code shall be punished.
3. Section 66 – Under section 66 of Chapter XI of the Act, If any act under Section 43 is done dishonestly or fraudulently, it becomes punishable under Section 66. Can charge up to 3 years of Imprisonment and 5 lakh rupees fine.
4. Section 66C – Under section 66C of Chapter XI of the Act, Whoever fraudulently or dishonestly makes use of electronic signature, password, or any other unique identification feature of any person. Can attract up to 3 years imprisonment and fine up to 1 lakh.
5. Section 66D – Under section 66D of Chapter XI of the Act, Whoever, by means of any computer resource, cheats by personating another person. Can attract Up to 3 years imprisonment and fine up to1 lakh. This section covers App calls, fake app, and advisor deception etc.
6. Section 72 – Under section 72 of Chapter XI of the Act, Whoever disclose personal information without consent; can attract up to 2 years of Imprisonment and 2 lakh rupees fine.
7. Section 79 – Under section 79 of Chapter XII of the Act and read with IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Liability arises for intermediary as it failed to remove advertisement despite high-return fraud Flags. And if they have actual knowledge about this advertisement and did not take any action they will lose safe harbour under section 79 of this act. Must remove fraud content within 36 hours.

[2] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[3] https://lawcrust.com/online-fraud-law/

[4] https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india

These provisions form the cornerstone of legal action in most cybercrime complaints.

PROVISION UNDER THE BHARATIYA NYAYA SANHITA, 2023[5]

Several traditional penal provisions still apply in online fraud situations

1. Section 314-315 – Under this section of Chapter XVII of the Act, narrate about Criminal Breach of Trust which attract up to 10 years of Imprisonment and fine also if by public servant, banker, merchant, agent, or trustee.
2. Section 316 – Under this section of Chapter XVII of the Act, deals with Cheating which can attract up to 7 years imprisonment if property valued over ₹10,000 or involves fiduciary breach.
3. Section 317 – Under this section of Chapter XVII of the Act, deals with Cheating with Knowledge that Wrongful Loss May Ensue to Person Whose Interest Offender is Bound to Protect and this can attract imprisonment up to 5 years and fine.
4. Section 318 – Under this section of Chapter XVII of the Act, deals with Cheating and Dishonestly Inducing Delivery of Property and can attract up to 10 years of imprisonment if via computer/communication device.
5. Section 319 – Under this section of Chapter XVII of the Act, deals with Fraudulent Deeds and Disposition of Property; can attract Up to 5 years and fine.
6. Section 333 to 342 - Under this section of Chapter XVIII of the Act, deals with Of Offences Relating to Documents and Property Marks which includes Making a False Document Forgery, Forgery for Purpose of Cheating, Falsification of Accounts and etc. which can attract up to 7 years of Imprisonment and fine.
7. Section 111 – Under this section of Chapter VI of the Act, which deals with the offense of organized crime (if any scam is operated as a syndicate with multiple accounts). Can attract life imprisonment or death if linked to economic sabotage.

This are relevant legal provision under cyber investment fraud of IT Act, 2000 and BNS, 2023. Other legal provisions of The Payment and Settlement Systems Act, 2007[6] and Consumer Protection Act, 2019[7] can also be applied in this online fraud.

[5] https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
[6] https://www.indiacode.nic.in/bitstream/123456789/2082/4/a2007-51.pdf
[7] https://www.indiacode.nic.in/handle/123456789/15256

DUE DILIGENCE OBLIGATIONS OF INTERMEDIARIES

The due diligence of Intermediaries is more clearly mentioned in IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021[8], than in IT Act, 2000 it is read both to together for due diligence. More clearly mentioned in Rules 3 and Rule 4 of the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose stringent "safe harbour" conditions on intermediaries (e.g., Google for ads, WhatsApp for messaging) to prevent hosting fraudulent content. Non-compliance strips Section 79 IT Act, 2000 an immunity to Intermediaries.

WHAT ARE INTERMEDIARIES?

The written definition of Intermediaries in IT Act, 2000 under section 2(1)(w) is following — "intermediary, with respect to any particular electronic records, means any person who on behalf of another person receives, stores or transmits that record or provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes." [9]

In general sense an intermediary is like a middleman who helps move, store, or manage electronic messages/data for someone else. They don't create the content, they just handle it (receive it, keep it, send it, or offer services related to it). Think of them as the post office or delivery guys for digital stuff. [10]

They include:

- Internet providers (like Airtel, Jio)
- Websites that host content (like Google Drive, YouTube)
- Search engines (Google)
- Payment apps (Paytm, Google Pay)
- Online shopping sites (Amazon, Flipkart)

---

[8] https://www.meity.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

[9] https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf

[10] https://blog.ipleaders.in/safe-harbor-provision-under-the-digital-millennium-copyright-act/
https://blog.ipleaders.in/safe-harbour-provisions-for-intermediaries-in-india-and-us/

- Cyber cafes, etc.

Imagine you send a WhatsApp message to your friend.

- You – create the message.
- WhatsApp (Intermediary) –receives it from you, stores it temporarily, and sends it to your friend.
- Jio/Airtel (intermediary) – provides the internet connection to transmit the message.
- Here, WhatsApp and Jio/ Airtel are intermediaries. They didn't write the message – they just helped deliver it.

Another example:

You upload a video on YouTube. YouTube stores it and shows it to others – acts as an intermediary. It doesn't own the video, but manages it for you.

In short, anyone who handles digital data (stores, sends, or helps use it) without creating it is an intermediary. They are the invisible helpers of the internet.

Rule 3 [11]

This rule requires all intermediaries to exercise "reasonable care" in curbing unlawful content, interpreted by algorithmic ae well as human oversight to detect fraud signals.

1. The intermediary shall publish the rules and regulations, privacy policy and user agreement in English or language in 8th schedule of Indian Constitution and consequences.
2. Users must be informed, through rules and regulations, terms and conditions, or user agreements, not to host, display, upload, modify, publish, transmit, update, or share any content that is unauthorized, illegal, harmful, or violates the rights of others
    - Belong to another person;
    - Is grossly harmful;
    - Harmful for minor;
    - Violates any patent, trademark, copyright, trade secret, or other proprietary rights.[12]
    - Deceives or misleads or communication is menacing in nature;
    - Impersonating;

[11] https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[12] https://content.edgar-online.com/ExternalLink/EDGAR/0001193125-17-127476.html?hash=64bd001f39e2c96c4a

- To interfere with, disable, destroy, or degrade the operation of any computer resources.
- Any conduct that jeopardizes India's national unity, defence, or security.

3. An intermediary shall not knowingly host, publish, initiate the transmission, determine the recipient of the transmission, or alter the information contained within the transmission.
4. An intermediary must, within thirty-six hours of learning—either on its own or from an affected person—about any unlawful information, disable access to it, if neccessary in coordination with the user or owner, and preserve the related data and records for at least ninety days for investigation.
5. The intermediary shall inform users that if they fail to comply with the rules, user agreement, or privacy policy governing the use of its computer resources, the intermediary may immediately terminate their access and remove any non-compliant information.
6. The intermediary shall comply fully with the provisions of the Act and all other applicable laws in force.
7. When required by a lawful order, the intermediary shall provide information or assistance to government agencies lawfully authorised for investigative, protective, or cybersecurity activities. Such information or assistance shall be furnished for purposes including identity verification, prevention, detection, investigation, prosecution, cybersecurity incidents, or punishment of offences under any applicable law, upon a written request clearly stating the purpose of the request.
8. The intermediary shall implement all reasonable measures to protect its computer resources and the information contained therein, in accordance with the reasonable security practices and procedures prescribed under the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011[13].
9. The intermediary shall report cybersecurity incidents and share all related information with the Indian Computer Emergency Response Team (CERT-In).[14]
10. The intermediary shall not knowingly deploy, install, modify, or enable any technical configuration of a computer resource, nor participate in any activity that alters or has the potential to alter the normal operation of the computer resource, thereby circumventing any law in force. Provided that the intermediary may develop, produce, distribute, or use

[13] https://indiankanoon.org/doc/114407484/
[14] https://www.cert-in.org.in/

technological measures solely for securing the computer resource and the information contained within it.

11. The intermediary shall publish on its website the name and contact details of the Grievance Officer, along with the mechanism for users or victims to submit complaints regarding any violation of rule 3 or misuse of the intermediary's computer resources. The Grievance Officer shall resolve such complaints within one month from the date of receipt.

Rule 4 [15]

Applicable to "significant data" entities (which have >5 million users), building on Rule 3 with additional obligation.

1. They must appoint a Chief Compliance Officer who is an Indian resident and responsible for compliance.
2. They must appoint a nodal contact person (Indian resident) for 24×7 coordination with law enforcement. They must appoint a Resident Grievance Officer (Indian resident) to handle user complaints.
3. They must publish monthly compliance reports detailing on:

- Complaints received,
- Actions taken,
- Content removed.

4. For intermediaries providing messaging services, they must enable identification of the first originator of information in India. This tracing is allowed only by court order or competent authority under Section 69 of the IT Act.
5. Tracing is permitted only for serious offences like:

- National security threats,
- Child sexual abuse,
- Organized cyber fraud.

The 2023 amendment extends Rule 4 to online gaming intermediaries offering real-money games.

1. Such gaming platforms must register with a Self-Regulatory Body (SRB) approved by MeitY.[16]
2. They must verify games as permissible (not gambling) before offering.

[15] https://prsindia.org/billtrack/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021

[16] Ministry of Electronics and Information Technology (MeitY),
Notifications under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

3. They must display a verification mark on approved games.

Failure to comply strips safe harbour under Section 79 of the IT Act. SSMIs face direct liability for third-party fraud if due diligence is not observed.

The intermediary liability framework under the Information Technology Act, 2000 is premised on the distinction between passive facilitators of online services and entities that exercise active control over unlawful digital activity. Section 79 of the Act grants conditional safe harbour to intermediaries, provided they adhere to statutory due-diligence obligations. The Supreme Court has clarified that such protection applies only where the intermediary's role is limited to providing access or hosting third-party information without initiating or modifying the content.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 further reinforce this position by mandating prompt action upon actual knowledge of unlawful activity and compliance with lawful takedown or blocking directions. Failure to observe these duties results in the forfeiture of statutory immunity, exposing intermediaries to legal liability.

Conversely, entities that originate, curate, or exercise decisive control over fraudulent digital content cannot claim intermediary status, as liability under Indian law follows control and intent rather than technological form. This approach prevents misuse of safe harbour provisions and ensures accountability for deliberate wrong doing.

CONCLUSION

All the above mention framework Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 establishes a structured legal pathway for investigation, liability, and enforcement. Their combined effect enables timely removal of fraudulent content, preservation of digital evidence, cooperation of intermediaries with law-enforcement agencies, and access to remedies such as refunds, compensation, and grievance redressal mechanisms. Strengthening the enforcement of intermediary responsibilities not only enhances accountability but also empowers victims by improving recovery prospects and restoring confidence in digital platforms. An effective and responsive intermediary liability regime is therefore essential for both deterrence and victim protection in the digital economy.