The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

Digital Arrest Scams and Existing Legal Remedies

Mannat Gothwal

In 2024, a prominent industrialist reportedly lost ₹7 crore after cybercriminals posing as CBI officers convinced him that he was under investigation for money laundering. For nearly two days, he remained under constant video surveillance, believing he was in the custody of law enforcement officials. In reality, he was the victim of a "digital arrest" scam. Similar incidents have affected retired professionals, senior citizens, and even highly educated individuals across India. The scam succeeds not because victims are careless, but because fraudsters exploit fear, authority, and unfamiliarity with legal procedures.[1]

One of the fastest-growing cyber frauds in India today is the so-called *digital arrest scam*. The phrase sounds official, which is precisely why it is effective. Fraudsters impersonate officers from agencies such as the CBI, ED, NCB, customs authorities, or even the judiciary and falsely inform victims that they are involved in a serious criminal investigation.

Victims are told that their Aadhaar number, bank account, mobile number, or a parcel sent in their name has been linked to offences such as money laundering, narcotics trafficking, or financial fraud. They are then placed under what scammers describe as "digital custody" through video calls and threatened with arrest unless they cooperate.

The scam has caused significant financial losses. According to data cited by the Indian Cyber Crime Coordination Centre (I4C), Indians lost more than ₹120 crore to digital arrest frauds between January and April 2024 alone.[2] Prime Minister Narendra Modi also warned citizens

---

[1] *81-Year-Old Man Loses Rs 7 Crore in Digital Arrest Scam After Fraudsters Pose as Mumbai Police*, YouTube (Economic Times, Jan. 5, 2025), https://www.youtube.com/watch?v=EXBAlghEphQ

[2] Amitabh Sinha, *Indians Lost ₹120 Crore in Digital Arrest Frauds in January-April 2024*, Indian Express (Oct. 28, 2024), https://indianexpress.com/article/india/indians-lost-rs-120-crore-in-digital-arrest-frauds-in-january-april-2024-9641952/

about the menace during his *Mann Ki Baat* address, emphasising that no government agency conducts investigations or arrests through video calls.

How Does a Digital Arrest Scam Work?

Most digital arrest scams follow a carefully scripted pattern:

1. **The Initial Call -** The victim receives a call, often through WhatsApp or an international number. The caller claims to be from a law enforcement or regulatory agency.
2. **A Serious Allegation -** The victim is informed that a parcel containing drugs or forged documents has been intercepted. Alternatively, they are told that their Aadhaar number or bank account has been linked to money laundering.
3. **Escalation Through Video Calls -** The victim is transferred to a video conference with individuals posing as senior officers. Fake police stations, uniforms, forged notices, and fabricated court orders are displayed to create legitimacy.[3]
4. **Isolation and Intimidation -** Victims are instructed not to contact family members, lawyers, or friends. They are threatened with immediate arrest if they disconnect the call.
5. **Transfer of Money -** Funds are demanded under labels such as “security verification”, “bail amount”, “clearance fee”, or “temporary deposit”. Once the money is transferred, it is rapidly moved through multiple accounts, making recovery difficult.

What makes this scam particularly dangerous is its psychological intensity. Victims may remain on continuous video calls for several hours or even days, creating the illusion that they are genuinely under official surveillance.

Recent Incidents

Digital arrest scams are no longer isolated incidents.

- In Kolkata, a retired bank employee lost approximately ₹4.4 crore after fraudsters

[3] Yasmin Hussain, *Digital Arrest: How India's Fastest-Growing Scam Uses Fake Investigations and Video Calls to Siphon Of Crores*, Econ. Times (June 8, 2026, 11:13 AM IST), https://economictimes.indiatimes.com/wealth/save/digital-arrest-how-indias-fastest-growing-scam-uses-fake-investigations-and-video-calls-to-siphon-off-crores/articleshow/131538736.cms

posing as government officials convinced him that he was implicated in an international money laundering investigation. He remained under constant video monitoring before transferring the money.[4]

- In another widely reported case, scammers allegedly impersonated senior law enforcement officials and convinced a businessman that he was under investigation, resulting in a loss of nearly ₹7 crore.
- The issue became so serious that the Supreme Court reportedly took suo motu cognisance after fraudsters used forged court documents to extort more than ₹1 crore from a woman.

The victims are not merely the elderly or technologically inexperienced. Anyone can become vulnerable when confronted with fear, urgency, and apparent official authority.

Existing Legal Remedies

Although "digital arrest" is not recognised under Indian law, the acts committed by fraudsters attract several criminal offences.

Bharatiya Nyaya Sanhita, 2023

Relevant provisions include:

- **Section 318** – Cheating and dishonestly inducing delivery of property.
- **Section 319(2)** – Personation of a public servant.
- **Section 351** – Criminal intimidation.
- **Section 61** – Criminal conspiracy where multiple offenders operate together.[5]

Information Technology Act, 2000

- **Section 66D** penalises cheating by personation through computer resources or communication devices.
- **Section 66C** criminalises identity theft and misuse of electronic identities.

[4] Dwaipayan Ghosh, *Sr Citizen Loses ₹4.4 Crore in Digi-Arrest Scam*, Times of India (June 8, 2026, 12:17 AM IST),https://timesofindia.indiatimes.com/city/kolkata/sr-citizen-loses-4-4-crore-in-digi-arrest-scam/articleshow/131573177.cms

[5] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 61, 318, 319(2), 351 (India).

- **Section 46** enables compensation through the adjudicatory mechanism established under the Act.[6]

Prevention of Money Laundering Act, 2002

The **Prevention of Money Laundering Act, 2002 (PMLA)** may also become relevant where the proceeds of a digital arrest scam are transferred through multiple accounts or organised criminal networks. Money obtained through such fraudulent activities may constitute "proceeds of crime" under the Act, enabling enforcement agencies to trace, investigate, and attach assets linked to the offence.[7]

What Should Victims Do?

If a person suspects that they are being targeted:

1. Immediately disconnect the call.
2. Do not transfer money or share personal information.
3. Contact the National Cyber Helpline **1930**.[8]
4. Report the incident through the National Cyber Crime Reporting Portal. 5. File an FIR under the relevant provisions of the BNS and the Information Technology Act.
6. Preserve screenshots, call recordings, bank transaction details, and communication records as evidence.

Rapid reporting is critical because authorities may be able to freeze recipient accounts before funds are dispersed through multiple banking channels.

Conclusion

The success of digital arrest scams lies in a simple but powerful deception: criminals borrow the credibility of the state to commit fraud. By impersonating police officers, investigators, and judicial authorities, they create a climate of fear that overrides rational decision-making.

[6] Information Technology Act, No. 21 of 2000, §§ 46, 66C, 66D (India).
[7] Prevention of Money Laundering Act, No. 15 of 2003, §§ 2(u), 5 (India).
[8] National Cyber Crime Reporting Portal, Ministry of Home Affairs, Government of India, https://cybercrime.gov.in/

Indian law already contains sufficient provisions to prosecute these offences. The greater challenge lies in prevention, rapid reporting, and public awareness. Citizens must remember one fundamental fact repeatedly emphasised by government authorities and the Prime Minister: **there is no such thing as a "digital arrest" under Indian law. No legitimate agency will conduct an investigation, demand money, or place an individual under custody through a WhatsApp or video call.**

That single piece of knowledge may be the most effective legal protection against this rapidly evolving form of cybercrime.