A Quarterly insight to Cyber Law!

Cyber Niyam means rules of the Cyberspace. This quarterly newsletter aims to create awareness about the rules and regulations of cyberspace, cyber security and data protection. This is also an effort to create awareness about digital safety, trending cybercrimes and effective reporting mechanisms.

CYBER NIYAM

By Adv. Vaishali Bhagwat *www.vaishalibhagwat.com*

Issue 3 of 2026 – July, 2026

In this Issue

Supreme Court Guidelines on Digital Arrest Scams

Introduction

India has witnessed a significant rise in cyber-enabled financial frauds in recent years, with "Digital Arrest" scams emerging as one of the most serious cyber frauds affecting individuals today. Fraudsters exploit technology to impersonate law enforcement agencies and government authorities, creating fear and panic among unsuspecting victims.By falsely claiming that a person is involved in criminal activities such as money laundering, drug trafficking or tax evasion, they coerce victims into transferring large sums of money under the guise of investigation or verification.

The alarming increase in such incidents, coupled with substantial financial losses suffered by citizens across the country, prompted the Supreme Court of India to take suo motu cognisance of the issue. Recognising that digital arrest scams involve multiple stakeholders—including banks, telecom service providers, intermediaries, regulators and law enforcement agencies—the Court initiated proceedings to strengthen coordination among these entities and develop an effective framework for preventing such frauds.

Through a series of interim directions and regular monitoring, the Supreme Court has taken steps to improve cyber fraud detection, strengthen investigations, protect victims and encourage the use of technology to prevent such crimes. These efforts highlight the need for a coordinated national response to tackle organised cybercrime and protect public confidence in India's digital ecosystem.

......Continued on page 2

What is Digital Arrest?

The term **"Digital Arrest"** does not have any legal recognition under Indian law. It is a deceptive tactic used by cybercriminals who falsely claim to be officials from agencies such as the Central Bureau of Investigation (CBI), the Enforcement Directorate (ED), the Narcotics Control Bureau (NCB), Customs, or the local police. Victims are contacted through phone calls or video calls and are informed that they are allegedly involved in serious criminal offences such as money laundering, parcel fraud, tax evasion or other illegal activities.
To make their claims appear authentic, fraudsters use forged identity cards, fake arrest warrants, fabricated court orders and even video backgrounds resembling police stations or government offices. Victims are often instructed not to disconnect the call and are threatened with immediate arrest, freezing of bank accounts or criminal prosecution if they fail to cooperate. Under immense psychological pressure, victims are persuaded to transfer money into so-called "safe" or "verification" accounts, which are in fact controlled by the fraudsters.

It is important to understand that no law enforcement agency in India can arrest a person through a phone call, video call or online communication. Every arrest must be carried out strictly in accordance with the procedure established by law. Therefore, any demand for money to avoid arrest or facilitate an investigation is a clear indication of fraud.

Why are digital arrest scams increasing?

Digital arrest scams are becoming more common due to a combination of technological advancements and psychological manipulation. Fraudsters often impersonate police officers, CBI officials or other government authorities and create a sense of fear and urgency by falsely claiming that the victim is involved in a criminal case or is about to be arrested.

Many people, particularly senior citizens and individuals who are less familiar with digital technology, are more vulnerable to these scams. Criminals use sophisticated techniques such as phishing links, fake UPI payment requests, caller ID spoofing and forged identity documents to make their communications appear genuine and convince victims to act without verification.

The rise in digital transactions, coupled with organised cybercrime networks operating across multiple jurisdictions, has made these offences more difficult to detect and investigate. Another significant challenge is the misuse of **mule accounts**—bank accounts opened or used to transfer and withdraw fraudulently obtained funds—allowing criminals to move money quickly and evade detection.

Although regulatory authorities, banks and law enforcement agencies have introduced several preventive measures, public awareness, safe digital practices and prompt reporting of suspicious activities remain the most effective safeguards against digital arrest scams.

GOOD TO KNOW!

1.There is no legal concept of "Digital Arrest Scam" under Indian Law. Neither the Bhartiya Nyaya Sanhita, 2023 (BNS) nor the former Indian Penal Code, 1860(IPC) recognises "digital arrest" as a legal procedure. No police officer or government agency can arrest a person through a phone or video call.

2.Recent Action: In June 2026, the CBI carried out raids across **16 States** to crack down on digital arrest scam networks, showing that authorities are actively taking action against these frauds.

Background of the Supreme Court's Suo Motu Proceedings

The Supreme Court initiated suo motu proceedings after a shocking case involving a senior citizen couple who were allegedly cheated of approximately ₹1.05 crore through a digital arrest scam. The fraudsters impersonated officials of the CBI and Enforcement Directorate and contacted the victims through phone and video calls. To reinforce the deception, they produced forged documents purportedly issued by the Supreme Court and threatened the victims with arrest, criminal prosecution and attachment of their property.

Believing the calls to be genuine, the victims transferred large sums of money over several days. The incident exposed the organised nature of digital arrest scams and showed that even educated individuals can fall victim to such frauds.

Taking note of the increasing number of similar cases, the Supreme Court took *suo motu* cognisance and directed various authorities to strengthen fraud prevention, investigation and victim protection.

KEY DIRECTIONS ISSUED BY THE SUPREME COURT :-

During the course of the proceedings, the Supreme Court issued several significant directions aimed at strengthening India's response to digital arrest scams.

1. **Investigation by the Central Bureau of Investigation (CBI) :-**

- The Court directed the CBI to investigate identified digital arrest scam cases involving organised cybercrime
- State Governments were directed to extend necessary cooperation and grant sanctions wherever required to facilitate effective investigation.

2. **AI-Based Detection of Mule Accounts :-**

- Reserve Bank of India (RBI) was directed to examine the use of Artificial Intelligence (AI) and Machine Learning (ML) for identifying mule accounts used to transfer fraudulent funds.
- Banks were encouraged to adopt advanced fraud detection systems to identify suspicious transactions at an early stage.

3. **Strengthening Coordination among Stakeholders**

- Banks, intermediaries,telecom service providers and investigating agencies were directed to work in close coordination for preventing and investigating digital arrest scams.
- Authorities were also encouraged to establish effective mechanisms for timely information sharing.

4. **Preservation of Electronic Evidence :-**

- Online intermediaries were directed to preserve electronic records relating to cyber frauds and cooperate with investigating agencies during investigations.

5. **SIM Verification and Telecom Measures :-**

- The Department of Telecommunications (DoT) and telecom service providers were directed to strengthen compliance with SIM card verification norms.
- Measures were also proposed to prevent the misuse of multiple SIM cards and spoofed calls.

6. **Freezing of Fraudulent Transactions**

- The Court permitted prompt freezing of suspicious bank accounts linked to digital arrest scams, in accordance with law, to minimise financial losses suffered by victims.

7. **Compliance By Digital Intermediaries:-**

- The Court directed digital intermediaries to comply with the provisions of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
- They were also directed to preserve and provide relevant electronic data and information to investigating agencies to facilitate timely and effective investigation of cyber fraud cases.

8. **Strengthening Cybercrime Infrastructure :-**

- The Court directed the States and Union Territories to operationalize Regional Cybercrime Coordination Centres and integrate them with the Indian Cyber Crime Coordination Centre (I4C)
- This will help agencies work together better, share information faster and respond more effectively to cybercrime across the country.

RBI's role in preventing Digital Arrest

The Reserve Bank of India (RBI) has taken several steps to help prevent digital arrest scams and other online financial frauds. It has encouraged banks to use Artificial Intelligence (AI) and Machine Learning to identify suspicious transactions and detect mule accounts used by fraudsters.

The RBI has also prepared a Standard Operating Procedure (SOP) to help banks quickly place a temporary hold on suspicious accounts and coordinate with law enforcement agencies during investigations. In addition, it is exploring stronger safeguards, including better fraud detection systems and a possible compensation framework for victims of cyber fraud.

Bank's Responsibilities :

- The Supreme Court has observed that banks are not just financial institutions but also custodians of public trust. They should take steps to prevent fraud instead of acting only after customers suffer losses.
- Banks should use AI-based monitoring systems to detect unusual transaction patterns and generate alerts for suspicious or high-value transactions.
- Wherever necessary, banks should carry out additional verification before processing suspicious transactions.
- They should regularly educate customers about emerging cyber frauds and strengthen their internal fraud detection systems.
- The Court has emphasised that early detection, quick action and strong security measures are essential to protect customers and maintain confidence in the digital banking system.

Warning signs of a digital arrest scam:

1. If someone claims you are under "digital arrest", it's a scam.
2. Scammers create panic by saying you'll be arrested unless you act immediately.
3. Never trust a caller just because they wear a uniform or show an ID card. These can be fake.
4. Ask for the officer's name, badge number and official office details. Verify them independently before taking any action.
5. Official notices and court documents are never sent over WhatsApp for instant payment or arrest.
6. No government agency will ask you to transfer money to a "Safe account" or to "prove innocence"
7. If you feel pressured to keep the call secret or stay on a video call, it's a red flag.
8. Be cautious of documents shared over WhatsApp or email. Fake notices often contain flashy graphics, unnecessary images or poor formatting. Always verify them with the concerned authority before taking any action.
9. If you suspect a scam, hang up immediately and report it by calling 1930 or visiting the National Cyber Crime Reporting Portal.

GLOSSARY OF TERMS

What is a Mule Account?

A bank account used by cybercriminals to receive or transfer money obtained through fraud, often without the account holder knowing it's purpose.

What is Spoofing ?

A technique used by scammers to disguise their phone number, email or identity so that it appears to come from a trusted or official source.

1930 Helpline : The national cybercrime helpline where victims can immediately report financial cyber fraud and seek assistance to help stop fraudulent transactions.

NCRP (National Cyber Crime Reporting Portal)
An online portal launched by the Government of India where citizens can report cybercrime complaints, including digital arrest scams.

NEWS CORNER

RBI Introduces a new compensation framework for Digital Fraud Victims

The Reserve Bank of India (RBI) has introduced a new compensation framework to provide relief to victims of small-value digital banking frauds. Under the new rules, eligible customers who report fraud promptly may receive compensation equal to 85% of the loss or ₹25,000**,** whichever is less, for losses up to ₹50,000. The framework aims to strengthen customer protection and encourage quick reporting of cyber frauds. The new rules will come into effect from 1st January 2027

NEWS CORNER

MHA forms a high-level panel to tackle Digital Arrest scams

The Ministry of Home Affairs has informed the Supreme Court that it has constituted a high-level committee to address the growing menace of "digital arrest" scams. The panel will examine operational challenges faced by enforcement agencies, recommend systemic reforms, and explore victim compensation in cases involving regulatory failures or negligence by service providers.

NEWS CORNER

CERT-IN tightens Cyber-security Rules

CERT-IN has asked organisations to fix critical internet-facing security flaws within 12 hours, wherever possible, as AI-powered cyber-attacks are becoming faster and more advanced. It has also reminded organisations to report cyber incidents within 6 hours of detecting them.

ABOUT THE AUTHORS

Adv Vaishali Bhagwat

Vaishali Bhagwat is a practicing lawyer with 25 years of experience in civil and cyber litigation and advisory practice in Pune and Mumbai.
Vaishali has a prior degree and work experience in the field of Computer Science, a Post graduation certification in Cyber Security and Information Assurance and is a certified Privacy Lead Assessor.

She is an advisor to several companies on Cyber law and privacy compliance and advisor to various educational institutions on Protection of children from sexual offences.

She has successfully conducted several prominent cases for corporate espionage and Data theft, Data Privacy, Digital Financial Frauds, Cyber-crimes against women and children, take down orders and IP infringement in cyberspace.

Vaishali is a *TCS Chevening Scholar on "Cyber Policy and Cyber Defense" and has earned the Post Graduate certification from Cranfield University UK. She is also a Disha Alumni which is a prestigious program of the British high Commission on Innovative Leadership chaired by UK PM David Cameron and PM Manmohan Singh*.

www.vaishalibhagwat.com

Adv Kunal Gokhale

BSC. LLB (Hons.) (Business Law) Degree

Advocate Kunal Gokhale is a legal professional with nearly fourteen years of post-qualification experience. He is a graduate from the National Law University, Jodhpur and holds a BSc LLB (Hons.) (Business Laws) degree. Advocate Kunal Gokhale has significant professional experience in handling civil litigation matters with focus on commercial matters. He also provides advisory services in relation to drafting of various types of agreements and has been associated with firms such as Vaish Associates, Advocates (Delhi), Ernst & Young, India (Mumbai) and Luthra & Luthra Law Offices (Mumbai) in the past.

Mrudula Arjunwadkar

BSc., LLB, MPM

POSH Consultant
Helping organizations in end to end POSH Compliance, External member to IC, POSH trainings