Mains Analysis: Digital arrest scams – can making banks pay stop a crime that runs on fear?

Internal Security · 31 October 2026 · https://www.shanmugamiasacademy.in/upsc-mains-analysis



Context

On **29 October 2026**, a Supreme Court bench of **Chief Justice Surya Kant, Justice Joymalya Bagchi and Justice V. Mohana**, hearing its **suo motu case on "digital arrest" scams**, said it was **proposing to direct that banks compensate victims** – at least the amount lost – where the fraud succeeded because the bank failed in due diligence. The bench said the victim's account should see "zero debit", that unusual transactions should be **held and verified before release**, and that it would examine the RBI's draft **Know Your Customer (KYC) Amendment Directions, 2026** before passing final orders. The Attorney General, R. Venkataramani, opposed court-imposed penalties and said the RBI's new measures would be operational by **December 2026**. About **Rs 800 crore** has been lost to digital arrest scams so far this year, the Court was told. The policy question: when a crime runs on fear and the victim himself presses "pay", who should carry the loss – the citizen, the bank, the platform or the State?

> **GS mapping:** GS-III – Challenges to internal security through communication networks; basics of cyber security; money laundering and its prevention; role of media and social-networking sites. GS-II – Government policies and interventions; statutory and regulatory bodies (RBI, I4C); judicial

activism (suo motu, continuing directions); Centre–State cooperation in policing; vulnerable sections (senior citizens). Also useful for Essay on technology and trust.



Background: what a "digital arrest" is

- **Modus operandi:** a caller poses as police, CBI, ED, customs, TRAI or even a court; claims the victim's Aadhaar, SIM or parcel is linked to drugs or money laundering; keeps the victim on a **video call for hours or days** ("you are under digital arrest, do not tell anyone"); shows fake uniforms, police-station backdrops and forged court orders; and makes the victim transfer savings to "verify" them. The money is moved at once through layers of **mule accounts**.
- **No such thing in law:** Indian criminal law has no "digital arrest". The PM said in *Mann Ki Baat* (115th episode, 27 October 2024) that no investigating agency ever questions anyone by phone or video call, and gave three steps – **"Ruko – Socho – Action lo" (Stop – Think – Take Action)**.
- **Scale:** the MHA told the Rajya Sabha (12 March 2025) that the National Cyber Crime Reporting Portal (NCRP) recorded **39,925** digital arrest and related cases with Rs 91.14 crore lost in 2022, and **1,23,672**

cases with **Rs 1,935.51 crore** lost in 2024. The Centre later told the Supreme Court that over **Rs 3,000 crore** had been extorted, mostly from elderly people.

- **The wider fraud wave:** NCRP data cited in an RBI discussion paper (April 2026) show cyber-fraud reports rising from about 2.6 lakh (2021) to about **28 lakh (2025)**, and the amount from Rs 551 crore to **Rs 22,931 crore**. I4C data reported in 2026 placed **Tamil Nadu third** in cyber-fraud losses, after Maharashtra and Karnataka.
- **Existing machinery:** NCRP (cybercrime.gov.in) and helpline **1930**; the Citizen Financial Cyber Fraud Reporting and Management System (2021) to freeze money quickly – over Rs 4,386 crore saved by February 2025 (PIB); **I4C**, an attached office of the MHA; over 7.81 lakh SIM cards and 83,668 WhatsApp accounts blocked by February 2025; DoT's **Sanchar Saathi / Chakshu** for reporting suspected fraud calls; and the RBI Innovation Hub's **MuleHunter.AI** (announced December 2024) to detect mule accounts.

The Supreme Court's suo motu case – a timeline

Date	Step	Significance
17 Oct 2025	Suo motu cognisance on the complaint of a senior-citizen couple from Ambala who lost Rs 1.05 crore to callers posing as CBI, ED and court officials (forged court orders shown on video)	Court treats it as an attack on public faith in courts and agencies
1 Dec 2025	CBI given a pan-India probe, with a free hand to examine the role of bankers; RBI asked why AI/ML is not used to catch mule accounts; States asked to give consent; Interpol help sought	Shift from scattered State FIRs to a national, follow-the-money investigation
9 Feb 2026	Court calls the siphoning of over Rs 54,000 crore through digital frauds "robbery and dacoity"; Centre asked to frame an SOP with RBI, banks and DoT; joint meeting on victim compensation	Compensation enters the agenda
28 Jul 2026	Court suggests defining "digital arrest" as a standalone offence with harsher punishment; Solicitor General says a draft law on digital arrests and deepfakes is being prepared	Legislative gap recognised

4 Aug 2026	RBI to adopt an SOP on temporary debit holds within four weeks, with grievance redressal and money-restoration modules; States to notify State Cyber Crime Coordination Centres and adopt e-Zero FIR	Victim-side remedies built; 36,290 cases, Rs 18.05 crore restored so far
Sep 2026	RBI issues draft KYC Amendment Directions, 2026: SOP for suspected mule accounts (transactions of Rs 1,000 or more flagged, debit hold up to 60 days, effective 1 April 2027)	Prevention moves into banking regulation
29 Oct 2026	Bench proposes bank compensation for due-diligence failure, "zero debit" for victims, hold-and-verify for unusual transactions; States to report FIRs	From "awareness" to "liability"

Core analysis: why bank measures are necessary but not enough

Layer	What exists / is proposed	Gap
Customer liability	RBI 2017 circular: zero liability for unauthorised electronic transactions caused by bank negligence or third-party breach reported promptly	Digital arrest victims "authorise" the payment under fear, so most fall outside it
Payment friction	RBI discussion paper (Apr 2026): one-hour delay on authorised push payments of Rs 10,000 or more, cancellable; trusted-person check for elderly; customer "kill switch"	Victims under coercion may still confirm; delays affect genuine payments
Mule accounts	MuleHunter.AI; draft KYC Amendment Directions 2026 – flag, hold up to 60 days, STRs where required under AML rules	Mule accounts are rented or bought; KYC is done but the account is sold later
Telecom and platforms	SIM and IMEI blocking, Chakshu, spoofed-call blocking; WhatsApp banned about 9,400 scam-linked accounts from January 2026 (I4C status report to SC)	Calls come over internet apps and from compounds abroad; blocking is after the event

Policing	1930/NCRP, I4C, CBI probe, e-Zero FIR, State coordination centres	Inter-State and cross-border trails; low recovery; few convictions of the masterminds
Law	BNS: cheating by personation, extortion, personating a public servant, organised crime; IT Act s.66C/66D	No defined offence of "digital arrest"; draft law still awaited

Dimensions

- **Internal security:** the scams are run by organised networks, often from scam compounds abroad that use trafficked workers. Proceeds fund other crime – a classic convergence of cyber crime, money laundering and human trafficking.
- **Economic and financial:** fear of fraud slows digital payments and hurts trust in UPI and online banking – the backbone of India's Digital Public Infrastructure.
- **Social:** senior citizens, retired officials and doctors are prime targets because they have savings and respect authority; shame stops many from reporting.
- **Governance and federal:** police and public order are State subjects, but the crime crosses States and borders – hence the CBI, I4C and Court-driven coordination.
- **Rights:** holding transactions and auto-reporting to police protect victims but can hurt genuine customers and raise privacy questions under the DPDP Act.

Challenges

- **The "authorised" payment trap:** the victim himself presses "pay", so banks argue they followed instructions – the core reason the Court is moving towards strict liability.
- **Speed of money:** funds pass through several layers of accounts and wallets within minutes; the "golden hour" after the fraud is usually lost.
- **Cross-border havens:** callers sit outside Indian jurisdiction; extradition and mutual legal assistance are slow.
- **Insider complicity:** the CBI has been asked to probe bank staff who open or ignore mule accounts.
- **Moral hazard vs fairness:** full bank liability may make customers careless and raise costs; no liability leaves the most vulnerable to bear it all.
- **False positives:** holds of up to 60 days can freeze genuine accounts, small traders and gig workers, with no compensation for wrongful holds.

Way forward

1. **Shared-liability framework:** a clear rule on who pays what – bank, receiving bank (which hosted the mule account), platform and telecom – with time-bound refunds, as the Court's August 2026 order asked the committee to examine.
2. **Risk-based friction:** cooling-off periods and trusted-person checks for unusual, high-value transfers from accounts of senior citizens, not blanket delays for everyone.
3. **Hit the receiving end:** stronger checks when an account suddenly receives large credits; liability on the bank that opened the mule account.
4. **Define the offence:** a specific offence of impersonating law enforcement to extort, with asset freezing on prima facie evidence.
5. **Platform duty:** verified "government agency" labels, rapid takedown of impersonating accounts and data-sharing with I4C under law.
6. **International action:** Interpol notices, joint operations with neighbouring countries hosting scam compounds, and rescue of trafficked workers.
7. **Awareness that sticks:** repeat the simple rule – no agency arrests on video, no agency asks for money to "verify" – through banks, post offices, pension offices and local bodies; report at once on 1930.

> **Conclusion:** Digital arrest is not a technology failure; it is a trust failure that technology makes faster. Banks can slow the money, platforms can block the caller and police can trace the trail – but only if each carries a clear share of the loss. A system in which the frightened citizen alone pays will never fix itself. Shared liability, smart friction and fast policing together can.

Mains practice question

Q. "Digital arrest" scams exploit fear of the State rather than flaws in technology. Discuss the measures taken to curb them and examine whether making banks liable to compensate victims is the right approach. *(15 marks, 250 words)*

Answer framework: Introduction – what digital arrest is; 2024 NCRP data (1.23 lakh cases, Rs 1,935 crore) · Body – (a) modus operandi and why victims "authorise" payments; (b) measures: NCRP/1930, I4C, blocking of SIMs and accounts, Chakshu, MuleHunter.AI, RBI drafts, CBI probe, e-Zero FIR; (c) Supreme Court suo motu case and the bank-liability proposal – arguments for (due diligence, deep pockets, incentive to prevent) and against (moral hazard, cost, false holds); (d) remaining gaps – cross-border havens, no defined offence · Way forward – shared liability, risk-based friction, receiving-bank checks, international action · Conclusion – faculty-view line.

Prelims pointers

- National Cyber Crime Helpline: **1930**; portal: cybercrime.gov.in (NCRP).
- I4C (Indian Cyber Crime Coordination Centre) – an attached office of the Ministry of Home Affairs.

- Chakshu – facility on DoT's Sanchar Saathi portal to report suspected fraud calls and messages.
- MuleHunter.AI – AI model for detecting mule accounts, developed by the Reserve Bank Innovation Hub (announced December 2024).
- Supreme Court suo motu case: *In Re: Victims of Digital Arrest Related to Forged Documents*, SMW (Crl.) 3/2025.

Asked before in UPSC Mains (PYQ)

Official question-paper wording, with how this analysis helps you answer it.

GS-III 2020 10 marks

"Discuss different types of cybercrimes and measures required to be taken to fight the menace."
How this helps: Digital arrest is the sharpest current example of social-engineering cyber fraud; use the NCRP–1930–I4C chain, mule-account controls and the Supreme Court directions as "measures".

GS-III 2021 10 marks

"Discuss how emerging technologies and globalisation contribute to money laundering. Elaborate measures to tackle the problem of money laundering both at national and international levels."
How this helps: Scam money moves in seconds through layers of mule accounts, wallets and crypto to compounds abroad – use mule accounts, MuleHunter.AI, the RBI draft debit-hold SOP and Interpol help as examples.

GS-III 2024 15 marks

"Social media and encrypting messaging services pose a serious security challenge. What measures have been adopted at various levels to address the security implications of social media? Also suggest any other remedies to address the problem."
How this helps: Digital arrest calls run on WhatsApp and Skype video; cite account blocking by I4C with platforms, Chakshu reporting and the Court's questions on platform responsibility.

Faculty view – looking ahead (Shanmugam IAS Academy)

The real story of this case is a shift in who carries the risk. For years the message was "be aware" – the loss stayed with the victim. The Court is now moving towards **"authorised push payment (APP) fraud"** being treated as a shared risk: if the victim pressed "pay" under coercion, but the bank ignored obvious red flags, the bank must pay. The UK took this route in 2024 with mandatory reimbursement. Expect India to build a middle path – liability linked to due diligence, plus friction aimed only at risky transfers.

- **A shift to note:** from "awareness and blocking" to "liability and prevention by design". Write: "make the system, not the scared citizen, carry the risk".
- **What to watch next:** (1) the Court's final directions on compensation and hold-and-verify, (2) the RBI's KYC Amendment Directions, 2026 and measures promised by December 2026, (3) the

mule-account SOP from 1 April 2027 (as drafted), (4) a Bill defining digital arrest and deepfake impersonation, (5) how auto-reporting to police is squared with the DPDP Act.

- **Ready-made conclusion line:** "Fear travels faster than money – India must make money travel slower than fear, and make those who could have stopped it share the loss."

Sources: PIB (MHA), "Steps taken to address the issue of digital arrest scams", 12 March 2025; Rajya Sabha reply reported by PTI; Reserve Bank of India – draft KYC Amendment Directions, 2026 and the April 2026 discussion paper on digital payment safeguards (as reported by All India Radio and MediaNama); reports on the Supreme Court hearings of 27 October 2025, 1 December 2025, 9 February, 28 July, 4 August and 29 October 2026 (LiveLaw, Bar and Bench, The Leaflet, ETV Bharat, Verdictum, DT Next, Deccan Chronicle, ThePrint, Outlook Money, The Week, NewsGram, MediaNama); I4C data reported by IANS (January 2026) and Outlook Money (July 2026); Mann Ki Baat, 27 October 2024. Original analysis by Shanmugam IAS Academy.

Shanmugam IAS Academy – your next step

- **Courses:** TNPSC Group 1, 2 / 2A (Prelims + Mains), Group 4, UPSC / IAS – Coimbatore · Madurai · Online – https://www.shanmugamiasacademy.in/fees
- **Books (PDF):** TNPSC PYQ books, UPSC books – https://www.shanmugamiasacademy.in/study-materials
- **Free quiz + daily PDFs:** https://www.shanmugamiasacademy.in/free-pdf-download · All news of this day: https://www.shanmugamiasacademy.in/upsc-mains-analysis

Admissions – call / WhatsApp: 99941 46662 · 99944 27714 · www.shanmugamiasacademy.in