CAUTION DIGITAL FORENSIC EVIDENCE DIGITAL FORENSIC EVIDE

The Digital Arrest Dossier

Deconstructing India’s Cyber-Extortion Epidemic and the Framework for Defense

A comprehensive intelligence brief on transnational coercion scams, legal realities under Indian Law, and the RBI's systemic response.

A Transnational Extortion Epidemic

₹1.5 Crore

Extorted from a single senior citizen couple in Ambala.

₹58.13 Crore

Laundered through thousands of fake accounts in a single Mumbai network.

₹120.3 Crore

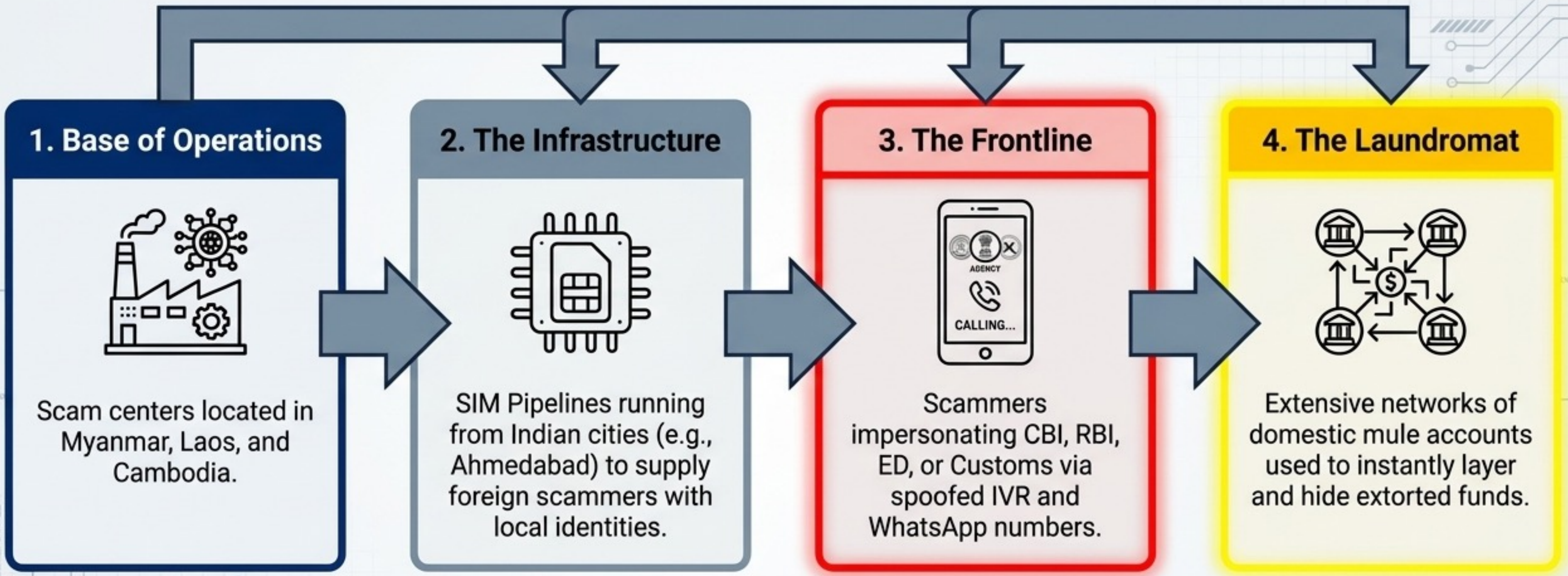
Total financial loss to Indian citizens reported by the Ministry of Home Affairs.

Lethal Impact

The psychological toll led to the tragic suicide of an elderly couple after losing ₹50 lakh.

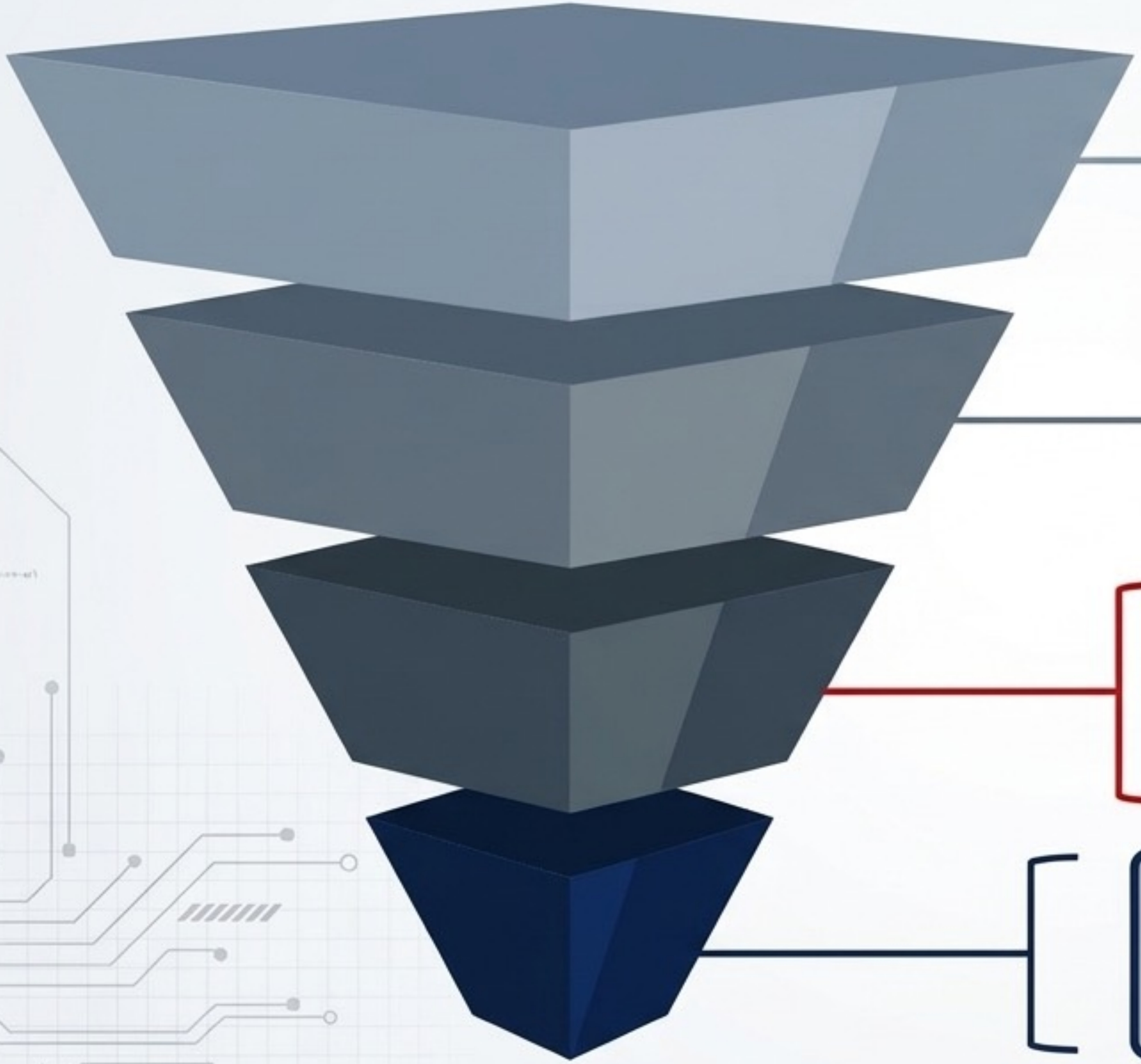
This is not **petty theft; it is highly organized economic terrorism** targeting India's digitally active citizens.

The Cross-Border Fraud Ecosystem



KEY INSIGHT: The operation relies on industrialized deception, prompting the Supreme Court of India to order coordinated CBI probes and AI-driven banking countermeasures.

The Coercion Funnel



Stage 1: The Bait (IVR Spoofing)
Automated calls impersonating FedEx, Telecom Dept, or Police.

Stage 2: The Hook (Intimidation)
False allegations of contraband in parcels, Aadhaar linked to money laundering, or SIMs used in terror activities.

Stage 3: The Trap (Digital Confinement)
Victim is forced onto Skype/WhatsApp video calls. Scammers use fake police station setups and forbid disconnecting.

Stage 4: The Extortion (Demand for Money)
Demands for security deposits or transfers to safe accounts to supposedly clear the victim's name.

The Intimidation Engine: Deconstructing the Forgery

Forged Signatures

Use of high-profile names, such as fake signatures of Supreme Court Justices or senior police officials.

Fabricated Seals (Convndential)

Counterfeit Enforcement Directorate (ED) or Supreme Court stamps layered onto PDFs.

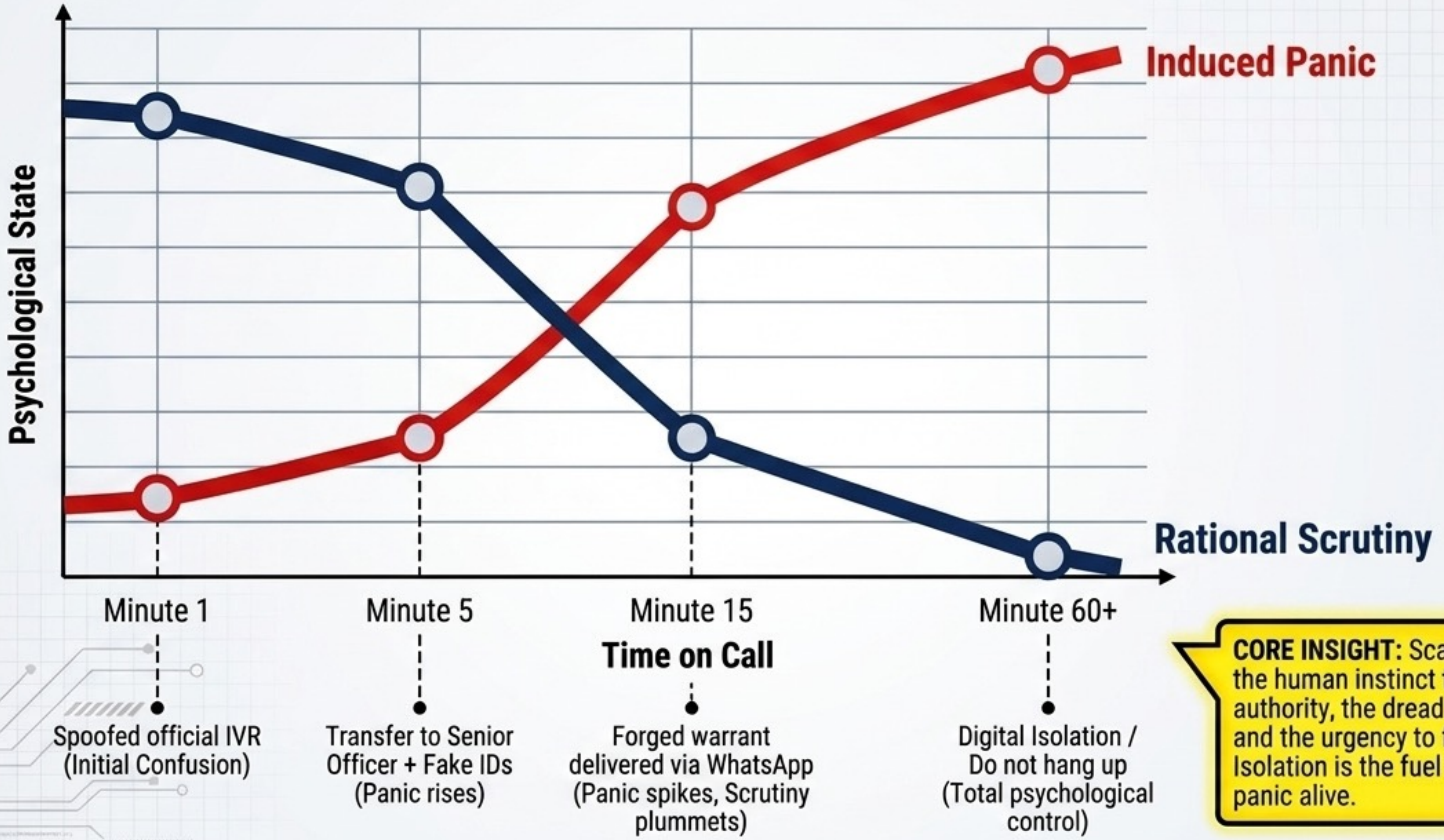
Fake Arrest Warrants

Documents citing the Prevention of Money Laundering Act (PMLA) to freeze assets.

The Secrecy Clause

Explicit written threats that speaking to family or lawyers will result in immediate jailing for interfering with an investigation.

The Psychological Escalation Curve



CORE INSIGHT: Scammers exploit the human instinct to obey authority, the dread of social ruin, and the urgency to fix the problem. Isolation is the fuel that keeps the panic alive.

Illusion vs. Law

The Digital Arrest Scam	Lawful Arrest under BNSS
WhatsApp video call / Skype.	Formal written notice or physical summons (Section 35 BNSS).
Digital confinement; forced isolation on camera.	Conducted at a designated station with the right to meet an advocate.
Tell no one or face immediate jail.	Statutory right to inform a relative or friend about the arrest.
Demands transfer to a safe account or security bond.	Police never demand immediate digital fund transfers to clear your name.

THERE IS NO CONCEPT OF DIGITAL ARREST UNDER ANY INDIAN LAW.

The True Legal Arsenal

Bharatiya Nyaya Sanhita, 2023 (BNS)

- **Sec 318 & 319:** Cheating by deception and personation.
- **Sec 308:** Extortion (threats to obtain money).
- **Sec 351:** Criminal intimidation.

Information Technology Act, 2000

- **Sec 66C:** Identity theft using digital identifiers.
- **Sec 66D:** Cheating by personation using a computer resource.

TAKEAWAY: If a caller threatens you with a digital arrest, they are the ones committing the crimes listed above.

The Systemic Counter-Attack

Supreme Court of India

Took suo motu cognisance of the Ambala case, recognizing that fake judicial orders strike at the foundation of public trust. Directed widespread CBI probes.

Technological Mandates

The Supreme Court demanded that telecom providers and banks utilize AI and Machine Learning to proactively detect suspicious transactions and freeze mule accounts.

MHA & I4C

Establishment of the Cyber Fraud Mitigation Centre, enabling swift cooperation between telcos, payment aggregators, and local police.

The RBI Safety Net (Effective Jan 2027)

Tier 1: Losses < ₹29,412

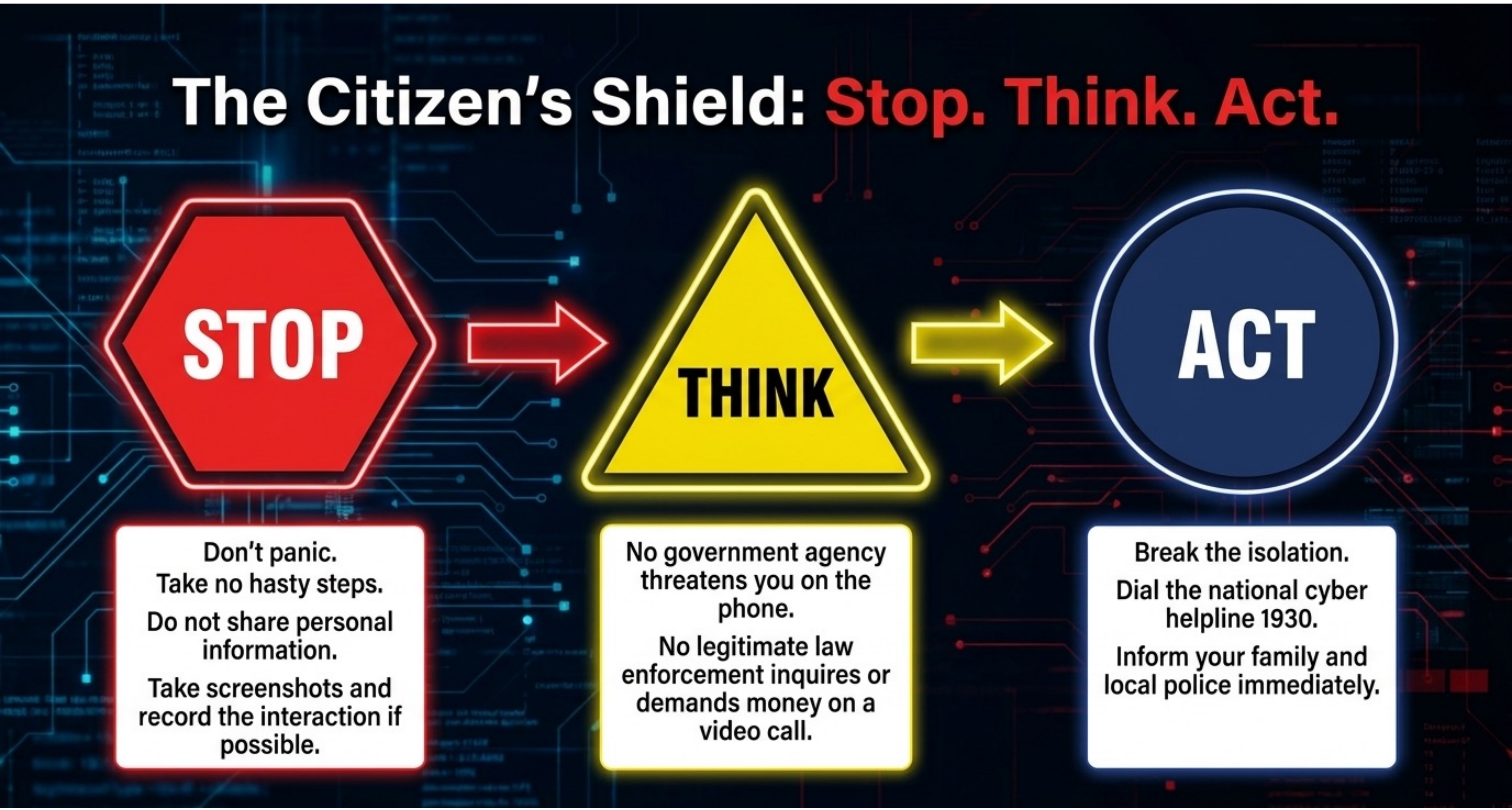
Victim is compensated 85% of the net loss.
(Cost split: 65% RBI, 10% Victim's Bank, 10% Beneficiary Bank)

Tier 2: Losses ₹29,412 to ₹50,000

Victim receives a flat maximum compensation of ₹25,000.

CRUCIAL CONDITIONS

- The victim MUST report the fraudulent Electronic Banking Transaction (EBT) **within 5 calendar days.**
- Banks must resolve the complaint within 45 days.
- Banks must fully compensate victims if the fraud resulted from the bank's negligence (e.g., failed security alerts).


The Citizen's Shield: Stop. Think. Act.
STOP
THINK
ACT
Don't panic.
Take no hasty steps.
Do not share personal information.
Take screenshots and record the interaction if possible.
No government agency threatens you on the phone.
No legitimate law enforcement inquires or demands money on a video call.
Break the isolation.
Dial the national cyber helpline 1930.
Inform your family and local police immediately.

The Golden Hour Playbook

First 5 Minutes

Hang up. Do not argue or verify. Break the isolation by telling one trusted person.

First 1 Hour

The LBW Rule

STOP	LAW ENFORCEMENT	• Call 1930 immediately and file on cybercrime.gov.in.
THINK	BANK	• Contact your bank to block cards, freeze UPI, and flag beneficiary accounts.
ACT	WIPE	• Secure devices, change passwords, and revoke suspicious app permissions.

Within 5 Days

Formalize bank complaints to qualify for RBI compensation frameworks.


Fear is Their Weapon. Knowledge is Your Defense.
A Digital Arrest relies entirely on an illusion of authority and forced isolation.
The moment you hang up the phone, the prison disappears.
EMERGENCY ANCHOR
National Cybercrime Helpline: 1930
Reporting Portal: www.cybercrime.gov.in
Suspect Communication Reporting: Chakshu (Sanchar Saathi)
Share this dossier. Break the silence. Protect your network.