UPSC & STATE PCS CURRENT AFFAIRS · UJIYARI.COM

DAILY CURRENT AFFAIRS

Gujarat's Cyber Financial Fraud e-Zero FIR: Registering a Case Without Entering a Police Station

27 July 2026 · SECURITY & DEFENCE POLITY · GS3 GS2

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

Gujarat's Cyber Financial Fraud e-Zero FIR: Registering a Case Without Entering a Police Station

27 July 2026 · 15 min read ·

✓ **Every fact web-verified against primary sources**

> *Gujarat launched a Cyber Financial Fraud e-Zero FIR service in Gandhinagar on 27 July 2026, under which a complaint to the national cybercrime helpline 1930 automatically generates a Zero FIR that is routed electronically to the jurisdictional police station. The victim no longer needs to visit a police station to start the criminal process.*

WHAT GUJARAT HAS ROLLED OUT

Deputy Chief Minister and Home Minister Harsh Sanghavi launched the service at Gandhinagar. Principal Chief Secretary (Home) Sanjeev Kumar and Director General of Police Gyanendra Singh Malik were present, while Rajesh Kumar, Chief Executive Officer of the Indian Cyber Crime Coordination Centre (I4C), joined virtually. Inspector General of Police Bipin Ahire, who heads the state's Cyber Centre of Excellence, is among the officers steering implementation.

The service was rolled out statewide over the Gujarat State Wide Area Network (GSWAN) to all Police Commissioners, Range Inspectors General, Superintendents of Police and Cyber Crime Police Inspectors, which matters because a reform of this kind fails at the last mile if the receiving station does not know what to do with an electronically generated Zero FIR.

A complaint made on the helpline 1930 or on the National Cybercrime Reporting Portal at cybercrime.gov.in now triggers automatic generation of an e-Zero FIR, which is transmitted electronically to the police station having territorial jurisdiction. The investigating officer then contacts the complainant, records the remaining particulars and converts the Zero FIR into a regular FIR before proceeding with investigation. In the first case processed under the system, an Ahmedabad resident was prevented from losing more than Rs 15.76 lakh in a digital arrest scam.

The initiative also sits alongside Gujarat's wider enforcement push against the financial plumbing of cyber fraud, including operations against mule-account networks and a bank-police coordination drive to speed up account freezing.

UNDERSTANDING ZERO FIR, E-FIR AND E-ZERO FIR

FEATURE	REGULAR FIR	ZERO FIR	E-ZERO FIR
Where registered	Police station with territorial jurisdiction over the offence	Any police station, irrespective of where the offence occurred	Auto-generated from a helpline or portal complaint, no station involved at intake
Serial number	Regular running number of that station	Numbered “0”, renumbered on transfer	Numbered “0”, renumbered on transfer
Victim’s physical presence	Required in practice	Required at the receiving station	Not required at any stage of registration
Transfer	Not applicable	Sent to the competent station for investigation	Electronically routed to the competent station
Time to registration	Depends on station workload and the victim’s travel	Depends on travel to the nearest station	Near-immediate, machine-triggered
Statutory anchor	Section 173, BNSS, 2023	Section 173(1), BNSS, 2023, “irrespective of the area”	Section 173(1) read with the electronic communication clause

Section 173(1) of the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 gives Zero FIR its first explicit statutory footing. The provision allows information about a cognizable offence to be given orally, in writing or by electronic communication, at any police station, irrespective of the area where the offence is committed. Where information is given electronically, it is taken on record only after the informant signs it within three days, a safeguard against anonymous or fabricated complaints. If a station refuses, the complainant may approach the Superintendent of Police under Section 175 of the BNSS.

Under the earlier Code of Criminal Procedure, 1973, Zero FIR rested on judicial interpretation and executive advisories rather than statutory text, which is why refusal on jurisdictional grounds was so hard to challenge. The concept entered mainstream policy through a recommendation of the Justice J.S. Verma Committee constituted in 2013 after the December 2012 Delhi gang rape, which found that jurisdictional refusal was routinely costing victims the critical first hours. Gujarat’s reform applies a safeguard designed for sexual offence victims to financial fraud victims, where the clock runs even faster.

THE I4C ARCHITECTURE BEHIND IT

The Indian Cyber Crime Coordination Centre was established as a scheme of the Ministry of Home Affairs in 2018, inaugurated in New Delhi in January 2020, and made an attached office of the Ministry with effect from 1 July 2024. It has seven components: the National Cyber Crime Threat Analytics Unit, the National Cyber

Crime Reporting Portal, the National Cyber Crime Training Centre, the Cyber Crime Ecosystem Management Unit, the National Cyber Crime Research and Innovation Centre, the National Cyber Crime Forensic Laboratory Ecosystem, and the Platform for Joint Cyber Crime Investigation Team.

PLATFORM OR INITIATIVE	FUNCTION
National Cybercrime Reporting Portal and helpline 1930	Citizen-facing intake for all cybercrime and financial fraud complaints
Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS)	Backend that pushes a reported transaction to banks, wallets and payment intermediaries for freezing
Cyber Fraud Mitigation Centre (CFMC)	Joint centre in New Delhi with representatives of major banks, financial intermediaries, payment aggregators, telecom service providers, IT intermediaries and state law enforcement agencies
Samanvay	Web-based module for cybercrime data repository, sharing, mapping, analytics and inter-state coordination
Cyber Commandos	Specialist cyber cadre drawn from central and state forces, with 5,000 to be trained over five years
Suspect Registry	National registry of cybercrime suspects linked to the reporting portal, supporting bank and intermediary fraud risk management
Pratibimb	Module mapping the geographic locations of cybercriminals and crime hotspots on a map interface

The Cyber Fraud Mitigation Centre, Samanvay, Cyber Commandos and the Suspect Registry were launched together on 10 September 2024 at the first Foundation Day of I4C. The architectural point for an aspirant is that I4C is not an investigating agency. It owns no police powers of its own. It is a coordination and platform body, and every one of these verticals works only to the extent that State police forces feed it and act on it.

THE GOLDEN HOUR AND THE NATIONAL PRECEDENT

The operating logic is the golden hour. Money moved out of a victim's account does not sit still. It passes within minutes through a chain of mule accounts, is split across several beneficiaries, converted into cryptocurrency or gift vouchers, or withdrawn at an ATM, and becomes practically unrecoverable within hours. The Citizen Financial Cyber Fraud Reporting and Management System was built precisely so that a complaint on 1930 generates an immediate ticket to the beneficiary bank to place a lien on whatever balance is still lying in the chain. Every step that stands between the victim and that ticket, including a trip to a police station and a queue at the writer's desk, is a direct transfer of value to the fraudster.

The Mule-Account Chain

Understanding why speed matters requires understanding the chain. A victim is induced to transfer money to a “layer one” account, usually opened in the name of a person paid a few thousand rupees for the use of their identity, or duped through a fake job offer. Within minutes the sum is broken up and pushed to layer two and layer three accounts across different banks and states, then cashed out. Each hop weakens the evidentiary link and multiplies the number of jurisdictions an investigator must approach. Freezing works only at the top of the chain, which is why the first hour, not the first day, is the operative unit.

The National Precedent

The Ministry of Home Affairs launched a national e-Zero FIR initiative in May 2025, piloted in Delhi for cyber-financial frauds above Rs 10 lakh, by integrating three systems that had never spoken to each other: the I4C reporting portal, Delhi Police’s e-FIR system and the National Crime Records Bureau’s Crime and Criminal Tracking Network and Systems (CCTNS). Delhi later lowered its e-FIR threshold for cyber fraud cases. Gujarat’s rollout is the extension of that model to an entire state, without a stated loss threshold, which is the more significant design choice: most cyber fraud victims lose sums well below Rs 10 lakh and were structurally excluded from the Delhi pilot.

FEDERALISM, CAPACITY AND THE DIGITAL DIVIDE

Police and public order are State subjects under Entry 2 and Entry 1 respectively of the State List in the Seventh Schedule of the Constitution. Cybercrime, by contrast, is inherently trans-jurisdictional: the victim is in Ahmedabad, the mule account is in another state, the SIM was issued in a third, the call originated from Southeast Asia and the beneficiary sits outside India altogether.

The I4C model resolves this tension not by constitutional amendment and not by creating a central police force, but by building a shared platform on which State police forces plug in voluntarily. The Union supplies the technology stack, the data repository and the banking interface; the States supply the police powers, the investigating officers and the courts. It is one of the cleanest live examples of cooperative federalism in internal security, and its weakness is the same as its strength: outcomes vary with each State’s willingness and technical capacity to integrate. Gujarat can do this today because it already runs GSWAN and a Cyber Centre of Excellence. A state without that backbone cannot simply announce the same reform.

Three caveats deserve equal weight in any answer.

The digital divide. An online-only registration channel can exclude elderly, low-literacy, non-English-speaking and rural victims, who are precisely the demographic targeted by digital arrest and fake investment-app frauds. A victim frightened enough to be held on a video call for six hours is not necessarily a victim who can navigate a web portal afterwards. A hybrid model, in which the walk-in and telephonic route is preserved and actively staffed alongside automated registration, is essential if the reform is not to become quietly regressive.

Registration is not conviction. The National Crime Records Bureau's Crime in India 2023 recorded 86,420 cybercrime cases, a rise of 31.2 per cent over 65,893 in 2022, with the cybercrime rate rising from 4.8 to 6.2 per lakh population. Conviction in these cases remains very low. Faster FIR registration without matching investment in digital forensics laboratories, trained cyber prosecutors, judicial familiarity with electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023, and mutual legal assistance for offshore servers simply shifts the bottleneck downstream from the writer's desk to the courtroom.

The money trail is a banking problem. Cyber fraud losses stood at Rs 22,845 crore in 2024 and Rs 22,495 crore in 2025. Enforcement in 2025 involved freezing 1.33 million mule accounts and deactivating 1.2 million SIM cards, with about Rs 5,489 crore recovered. Digital arrest cases specifically declined sharply in 2025 after a steep surge the previous year, which suggests that publicity, freezing and takedown do work when applied together. The Reserve Bank of India's MuleHunter.AI, developed by the Reserve Bank Innovation Hub and introduced in December 2024, and the Digital Payments Intelligence Platform built with the National Payments Corporation of India, are the financial-sector half of the same enforcement problem. Registration reform and account-level detection have to advance together, because a police station cannot freeze an account and a bank cannot file a chargesheet.

LEGAL FRAMEWORK AND WAY FORWARD

Cyber financial fraud is prosecuted under a combination of statutes rather than a single code. Section 66C of the Information Technology Act, 2000 covers identity theft and Section 66D covers cheating by personation by using a computer resource, punishable with imprisonment up to three years and fine up to Rs one lakh. Section 43A and Section 72A of the same Act deal with failure to protect sensitive personal data and wrongful disclosure of information. Under the Bharatiya Nyaya Sanhita, 2023, cheating is punishable under Section 318, criminal breach of trust under Section 316, forgery under Sections 336 to 340, and organised crime, which expressly includes organised cyber-crime, under Section 111. Proceeds of large frauds attract the Prevention of Money Laundering Act, 2002.

The way forward has five elements:

- **Nationwide rollout with a low uniform threshold.** Extend e-Zero FIR to every State and Union Territory without a high monetary cut-off, so that small-value victims, who are the overwhelming majority, are not excluded by design.
- **Real-time bank-police integration.** An FIR number and a freeze instruction should travel together rather than sequentially, with a defined service-level obligation on the beneficiary bank.
- **Break the mule chain at source.** Mandate periodic Know Your Customer re-verification, behavioural monitoring of dormant and suddenly active accounts, and a faster, legally clear route for banks to act on suspected mule accounts.
- **Build the back end.** Expand digital forensic laboratory capacity, train prosecutors and investigating officers, and pursue mutual legal assistance treaties and 24x7 points of contact for offshore evidence.

- **Protect the victim.** Create a statutory victim-compensation fund financed from recovered and confiscated proceeds, so that restitution does not depend entirely on the speed of the first hour, alongside sustained public awareness that no law enforcement agency in India conducts an arrest over video call.

UPSC RELEVANCE

GS Paper 3: Challenges to internal security through communication networks; Basics of cyber security; Money laundering and its prevention; Role of external state and non-state actors in creating challenges to internal security; Various security forces and agencies and their mandate.

GS Paper 2: Functions and responsibilities of the Union and the States, issues and challenges pertaining to the federal structure; Government policies and interventions for development in various sectors and issues arising out of their design and implementation; Mechanisms, laws, institutions and bodies constituted for the protection and betterment of vulnerable sections; Statutory, regulatory and various quasi-judicial bodies.

Prelims pointers:

- The Cyber Financial Fraud e-Zero FIR service was launched in Gandhinagar on 27 July 2026 by Deputy Chief Minister and Home Minister Harsh Sanghavi.
- The Indian Cyber Crime Coordination Centre was set up as a scheme of the Ministry of Home Affairs in 2018 and became an attached office of the Ministry from 1 July 2024.
- I4C has seven components, including the National Cyber Crime Threat Analytics Unit and the National Cyber Crime Forensic Laboratory Ecosystem.
- Section 173(1) of the BNSS, 2023 gives Zero FIR statutory recognition through the words "irrespective of the area where the offence is committed".
- Electronic information under Section 173(1) is taken on record only after the informant signs it within three days.
- The national cybercrime helpline number is 1930 and the reporting portal is cybercrime.gov.in.
- The Cyber Fraud Mitigation Centre, Samanvay, Cyber Commandos and Suspect Registry were launched on 10 September 2024 at I4C's first Foundation Day.
- The Ministry of Home Affairs launched e-Zero FIR in May 2025, piloted in Delhi for cyber-financial frauds above Rs 10 lakh.
- NCRB's Crime in India 2023 recorded 86,420 cybercrime cases, a 31.2 per cent rise over 65,893 in 2022.
- Police and public order fall under Entries 2 and 1 respectively of the State List, Seventh Schedule.
- Section 66D of the Information Technology Act, 2000 punishes cheating by personation using a computer resource with up to three years imprisonment and fine up to Rs one lakh.

FACTS CORNER, KNOWLEDGEPEDIA

GUJARAT E-ZERO FIR:

Launched at Gandhinagar on 27 July 2026 by Deputy Chief Minister and Home Minister Harsh Sanghavi

Officials present: Principal Chief Secretary (Home) Sanjeev Kumar and Director General of Police Gyanendra Singh Malik

I4C Chief Executive Officer Rajesh Kumar joined virtually

Statewide rollout network: Gujarat State Wide Area Network (GSWAN)

Trigger channels: helpline 1930 and cybercrime.gov.in

First case: an Ahmedabad resident saved from losing over Rs 15.76 lakh in a digital arrest scam

I4C AND THE LEGAL BASE:

Establishment: scheme of the Ministry of Home Affairs, 2018; inaugurated in New Delhi in January 2020

Status: attached office of the MHA with effect from 1 July 2024

Components: seven, including the National Cyber Crime Threat Analytics Unit, the National Cyber Crime Training Centre and the National Cyber Crime Forensic Laboratory Ecosystem

Zero FIR statutory basis: Section 173(1), Bharatiya Nagarik Suraksha Sanhita, 2023

Refusal remedy: approach the Superintendent of Police under Section 175, BNSS, 2023

Policy origin: Justice J.S. Verma Committee, constituted 2013

IT Act, 2000: Section 66C identity theft, Section 66D cheating by personation using a computer resource

Bharatiya Nyaya Sanhita, 2023: Section 318 cheating, Section 316 criminal breach of trust, Section 111 organised crime

DATA POINTS:

Cyber fraud losses: Rs 22,845 crore in 2024 and Rs 22,495 crore in 2025

Enforcement in 2025: 1.33 million mule accounts frozen, 1.2 million SIM cards deactivated

NCRB Crime in India 2023: 86,420 cybercrime cases, rate up from 4.8 to 6.2

Cyber Commandos target: 5,000 trained over five years

KEY CONCEPTS:

Zero FIR: an FIR registered at any police station irrespective of territorial jurisdiction, numbered “0” and transferred to the competent station

> e-FIR: an FIR registered through electronic communication, valid once signed by the informant within three days
>
> Digital arrest: a fraud in which callers impersonating police, CBI or customs officers keep a victim on continuous video call under threat of arrest until money is transferred
>
> Mule account: a bank account, often opened by a paid or duped third party, used to receive and layer fraudulently obtained funds
>
> Golden hour: the short window immediately after a fraudulent transfer within which reporting can still freeze the money
>
> CFCFRMS: Citizen Financial Cyber Fraud Reporting and Management System, the backend that relays a complaint to banks for freezing
>
> MuleHunter.AI: a Reserve Bank Innovation Hub tool using machine learning to detect mule accounts
>
> CCTNS: Crime and Criminal Tracking Network and Systems, the NCRB-run national police case database

Sources: PIB, Ministry of Home Affairs, The Hindu

Source: Gujarat's Cyber Financial Fraud e-Zero FIR: Registering a Case Without Entering a Police Station — Ujiyari.com | Free UPSC & State PCS Current Affairs

RELATED EDITORIALS

BUSINESS STANDARD

A Fresh Slate: Why Exam Integrity Needs Institutions, Not Resignations

27 Jul

MINT

The Democracy Quotient: Why India's Middle Power Moment Begins at Home

27 Jul

THE HINDU

Code as Contraband: When the State Takes Down an Architecture, Not a Post

27 Jul

THE HINDU

Law That Cannot Be Found: The Case for Open Legal Publishing

27 Jul

RELATED KEY TERMS

KEY TERM

16th Finance Commission

The constitutional body chaired by Arvind Panagariya that recommends...

KEY TERM

42nd Amendment Freeze on Delimitation

The constitutional freeze that locked Lok Sabha seat allocation to the...

KEY TERM

Advance Directive (Living Will)

A legal document in which a competent adult specifies their medical...

KEY TERM

Advanced Technology Vessel (ATV) Programme

India's classified, decades-long programme to indigenously design and...

CURATED & WRITTEN BY

Bharat Choudhary

UPSC Educator & Content Creator

linkedin.com/in/epicbharat

📖 Read Full Article on Ujiyari →

https://ujiyari.com/daily/2026/07/27/gujarat-e-zero-fir-cyber-financial-fraud-i4c-2026/