

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 3

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Cybercrime and Victim Restitution: Reconciling Account Freezing, Due Process, and Financial Recovery

PRABHASH DALEI* AND PROF. (DR.) MANOJ KUMAR SADUAL**

ABSTRACT

Digital financial fraud has transformed cybercrime enforcement from a question of criminalisation into one of preservation, adjudication, and restitution. The central concern is whether India's legal and institutional framework can secure fraud proceeds rapidly while protecting due process and enabling financial recovery for victims. Through doctrinal examination of statutory provisions, official materials, judicial decisions, and academic literature, this study distinguishes complaint-based holds, police seizure, judicial attachment, interim custody, and final restoration of funds. These measures perform different legal functions and should not be treated as interchangeable. The national reporting and financial-fraud management framework has improved early intervention and reduced the risk of dissipation, yet uncertainty persists regarding the statutory basis, duration, scope, and review of account restraints. Recent judicial developments also reveal tension between victim protection and the disproportionate hardship imposed on innocent account holders, merchants, and downstream recipients. The emerging restitution framework provides procedures for holds, seizure, grievance redressal, interim custody, and restoration, but gaps remain in statutory coherence, judicial consistency, uniform implementation, and outcome reporting. A balanced framework therefore requires amount-specific restraint, prompt judicial supervision, transparent claim verification, periodic review, and disclosure of restoration outcomes. Effective cybercrime restitution depends on speed, legality, proportionality, and enforceable recovery operating together.

Keywords: Cybercrime; Victim Restitution; Account Freezing; Due Process; Financial Recovery

I. INTRODUCTION

India's response to digital financial fraud must be evaluated not merely by asking whether deceptive online conduct is punishable, but by examining whether criminal procedure can preserve and restore the victim's money. The National Crime Records Bureau recorded 1,01,928

* Author is a Research Scholar and Assistant Professor, Utkal University, Bhubaneswar, Odisha, India.

** Author is a Professor, School of Law, KIIT University, Bhubaneswar, Odisha, India.

cybercrime cases in 2024, compared with 86,420 in 2023, an increase of 17.9 per cent. Fraud was identified as the motive in 73,987 cases, constituting 72.6 per cent of registered cybercrime.¹ These figures establish the predominance of fraud within registered cybercrime, but they do not independently prove either the total incidence of victimisation or the failure of existing law. Increased registration may also reflect greater awareness, more accessible reporting, or changes in recording practices.

The National Cybercrime Reporting Portal permits citizens to report cybercrime, while the Citizen Financial Cyber Fraud Reporting and Management System connects law-enforcement agencies, banks, payment intermediaries, and other stakeholders to facilitate action against financial fraud.² Helpline 1930 operates across the States and Union Territories for reporting such complaints. As of 31 January 2026, the Government stated that more than ₹8,690 crore had been “saved” in over 24.65 lakh complaints through the CFCFRMS.³ That figure demonstrates the preventive potential of rapid coordination, but “saved” cannot automatically be equated with money finally restored. Funds placed on hold may still require verification, investigation, judicial determination, and resolution of competing claims.

This distinction creates a conflict between urgency and legality. Delay may allow suspected proceeds to move through successive accounts, yet blanket or prolonged restrictions may burden merchants, intermediaries, and downstream recipients whose participation in the fraud has not been established. Existing scholarship on the NCRP–CFCFRMS has therefore identified a tension between crime-control objectives and due-process safeguards, particularly where technological intervention is not matched by transparent rules concerning account restraint, review, and victim recovery.⁴ Freezing may preserve an amount, but it neither identifies the offender nor conclusively determines entitlement.

The Bharatiya Nagarik Suraksha Sanhita, 2023 contains distinct provisions governing police seizure under section 106 and court-supervised attachment, forfeiture, and restoration under section 107.⁵ Section 106 requires seizure to be reported forthwith to the jurisdictional Magistrate, while section 107 provides a judicial procedure for attaching property believed to be the proceeds of crime and, after such determination, distributing it among affected persons.

¹ National Crime Records Bureau, Ministry of Home Affairs, Government of India, CRIME IN INDIA 2024, Vol. I, “Cyber Crimes” (2026), <https://www.ncrb.gov.in/uploads/files/CrimeinIndia2024-VolumeI.pdf>.

² Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, NATIONAL CYBERCRIME REPORTING PORTAL (NCRP), <https://i4c.mha.gov.in/ncrp.aspx> (last updated Mar. 11, 2026).

³ Ministry of Home Affairs, Government of India, Lok Sabha Unstarred Question No. 3913, Answer at 2 (Mar. 17, 2026), <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/3913.pdf>.

⁴ Dakshina Chandra, *Examining the Contours and Challenges of the National Cybercrime Reporting Portal in Countering Digital Financial Frauds*, 8 J. Victimology & Victim Just. 65, 74–81 (2025).

⁵ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023, §§ 106–107.

Against this background, the paper undertakes a doctrinal analysis of legislation, official materials, judicial decisions, and scholarship. It addresses a gap in the literature by examining as one continuum the post-BNSS pathway from portal reporting and emergency restraint to seizure, attachment, and restitution. The 2026 Standard Operating Procedure now provides a uniform, victim-centric administrative framework for handling complaints, preservation of funds, interim custody, and restoration. Nevertheless, the statutory relationship among complaint-based holds, police seizure, judicial attachment, and final restitution, as well as the uniform implementation of these measures, remains insufficiently settled. A victim-centred framework must combine speed with proportionality, prompt judicial supervision, and an enforceable process for returning money to persons legally entitled to receive it.

II. CYBERCRIME DATA AND THE SHIFT FROM REPORTING TO RESTITUTION

Official cybercrime statistics reveal a sharp expansion in police engagement with digital offences, but they do not disclose whether victims ultimately recover their money. The NCRB recorded 52,974 cybercrime cases in 2021, 65,893 in 2022, and 86,420 in 2023.⁶ The increase establishes the growing criminal-law significance of cybercrime; it does not, without further evidence, demonstrate either the true prevalence of victimisation or the failure of existing legislation. Registered-case figures may be influenced by reporting awareness, police recording practices, and access to complaint mechanisms.

The available datasets also measure different institutional events. The NCRB records cases registered by the police, whereas the National Cybercrime Reporting Portal records complaints submitted by citizens, whose conversion into FIRs and subsequent investigation are undertaken by the concerned State or Union Territory law-enforcement agencies.⁷ CERT-In, by contrast, handled 20,41,360 cybersecurity incidents during 2024 as the national incident-response agency.⁸ These figures cannot be aggregated, because a cybersecurity incident, a portal complaint, and a registered criminal case do not represent the same legal or procedural stage. Treating them as interchangeable would exaggerate the criminal-case burden and obscure the movement of a complaint through the justice system.

CFCFRMS data illuminate a further stage: the emergency preservation of money. As of 31 January 2026, the Government reported that more than ₹8,690 crore had been “saved” in over

⁶ Ministry of Home Affairs, ASSISTANCE TO STATES TO TACKLE CYBER INCIDENTS, Press Information Bureau (Mar. 24, 2026), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504>.

⁷ Ministry of Home Affairs, Government of India, Lok Sabha Unstarred Question No. 4118, Cyber Crime Cases 2–3 (Mar. 17, 2026), <https://www.mha.gov.in/MHA1/Par2017/pdfs/par2026-pdfs/LS17032026/4118.pdf>.

⁸ Ministry of Home Affairs, ASSISTANCE TO STATES TO TACKLE CYBER INCIDENTS, *supra* note 6.

24.65 lakh complaints.⁹ The expression indicates that coordination among police, banks, and financial intermediaries may prevent further dissipation of reported funds. The aggregate amount described as “saved” does not disclose the subsequent legal status of every amount preserved. The 2026 Standard Operating Procedure separately records that, between April 2021 and November 2025, ₹7,647 crore was prevented from reaching cybercriminals, while only ₹167 crore had been restored to victims.¹⁰ The NCRB, however, does not maintain comprehensive data on the amount recovered in cybercrime cases.

This statistical gap has doctrinal consequences. A system may appear successful because complaints increase or money is intercepted, while the duration, legality, and final outcome of account restraints remain unknown. Existing scholarship similarly cautions that freezing funds does not itself identify the offender or compensate the victim.¹¹ The appropriate measure of effectiveness must therefore extend beyond access to reporting and speed of intervention. It must examine whether the law converts emergency preservation into judicially supervised, proportionate, and timely restitution. The shift from reporting to restitution is thus not merely administrative; it determines whether the cybercrime framework delivers a remedy rather than only recording or interrupting victimisation. It also requires the publication of outcomes capable of distinguishing temporary restraint from completed recovery and lawful release.

III. LEGAL CHARACTERISATION OF DIGITAL FINANCIAL FRAUD

Digital financial fraud is not constituted by a single offence under Indian law. It is a descriptive category covering transactions in which money is obtained or diverted through unauthorised access, misuse of credentials, digital personation, dishonest inducement, coercion, or false electronic records. The legal character of a transaction must therefore be determined from its proved acts and mental elements rather than from the label “cyber fraud.” A deceptive call inducing a transfer, unauthorised access to an account, the use of stolen credentials, and the fabrication of a payment record may produce the same loss, but they do not necessarily constitute the same offence.

The Information Technology Act, 2000 addresses the technological component of such conduct. Section 43 creates a compensatory framework for specified unauthorised acts involving computer resources, including access, extraction of data, and disruption. Section 66 criminalises

⁹ Ministry of Home Affairs, *supra* note 7, at 3.

¹⁰ Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, STANDARD OPERATING PROCEDURE FOR NCRP–CFCFRMS: PUTTING ON HOLD, SUSPENSION, SEIZURE, INTERIM CUSTODY, RESTORATION OF MONEY AND GRIEVANCE REDRESSAL (Jan. 2, 2026).

¹¹ Dakshina Chandra, *Examining the Contours and Challenges of the National Cybercrime Reporting Portal in Countering Digital Financial Frauds*, 8 J. Victimology & Victim Just. 65, 79–81 (2025).

acts referred to in section 43 when committed dishonestly or fraudulently. Section 66C applies where another person's electronic signature, password, or unique identification feature is fraudulently or dishonestly used, whereas section 66D punishes cheating by personation through a communication device or computer resource.¹² In *Shreya Singhal v. Union of India*, the Supreme Court emphasised that mens rea is integral to section 66 and treated sections 66C and 66D as provisions with defined ingredients, unlike the invalidated section 66A.¹³ Consequently, financial loss cannot replace proof of unauthorised conduct, identity misuse, or digital personation.

The Bharatiya Nyaya Sanhita, 2023 addresses the deception, coercion, and property dimensions of the transaction. Section 318 governs cheating, including dishonest inducement resulting in the delivery of property; section 319 concerns cheating by personation. Where money is obtained by intentionally creating fear of injury, section 308 on extortion may be relevant. Sections 335, 336, and 340 may apply where a false electronic record is made, forged, or knowingly used as genuine, but falsity alone is insufficient unless the statutory requirements of a false electronic record and the required intention are established.¹⁴

A single course of conduct may therefore attract both technology-specific and general penal provisions. In *Rajendra Singh v. State of Madhya Pradesh*, the Supreme Court dealt with an FIR alleging investment fraud under the cheating and forgery provisions of the Penal Code, together with sections 66C and 66D of the Information Technology Act.¹⁵ The order illustrates the practical coexistence of these charges; it does not establish that every digital fraud automatically satisfies all of them. Proper classification requires investigators to identify who was deceived or threatened, what representation was made, how access or credentials were obtained, what property was transferred, and which electronic record enabled the transaction.

The principal deficiency is not necessarily an absence of criminalisation. Overlapping provisions can capture distinct components of wrongdoing, but indiscriminate charging may obscure the prosecution's theory, while narrow charging may omit the technological act enabling the loss. More fundamentally, offence provisions determine criminal liability and punishment; they do not explain how disputed money is traced, restrained, judicially attached, or restored.¹⁶

¹² The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 43, 66, 66C–66D.

¹³ *Shreya Singhal v. Union of India*, (2015) 5 S.C.C. 1.

¹⁴ The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, §§ 308, 318–319, 335–336, 340.

¹⁵ *Rajendra Singh v. State of Madhya Pradesh*, Criminal Appeal No. 1736 of 2025 (India).

¹⁶ Compare The Information Technology Act, 2000, §§ 66C–66D, and The Bharatiya Nyaya Sanhita, 2023, §§ 308, 318–319, 335–336, 340, with The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023, §§ 106–107; see also Dakshina Chandra, *Examining the Contours and Challenges of the National Cybercrime Reporting Portal in Countering Digital Financial Frauds*, 8 J. Victimology & Victim Just. 65, 66–68, 79–81 (2025).

The framework therefore depends upon connecting accurate classification with a coherent procedural route from complaint to restitution.

IV. NCRP COMPLAINTS, FIR REGISTRATION, AND JURISDICTION

The National Cybercrime Reporting Portal provides a digital entry point for complaints, but the portal acknowledgement and an FIR perform different legal functions. The Ministry of Home Affairs states separately that incidents reported on the NCRP, their conversion into FIRs, and subsequent action are handled by the concerned State or Union Territory law-enforcement agencies.¹⁷ This indicates that submission of a complaint does not automatically complete FIR registration. The distinction matters because portal reporting may initiate urgent financial intervention, whereas an FIR records information concerning a cognizable offence and activates the investigation process.

Section 173(1) of the Bharatiya Nagarik Suraksha Sanhita, 2023 permits information relating to a cognizable offence to be given to the officer in charge of a police station, irrespective of the area in which the offence was committed, orally or through electronic communication. Electronic information must be signed within three days, and a copy of the recorded information must be supplied free of cost to the informant or victim.¹⁸ The provision recognises electronic reporting and removes territorial jurisdiction as a basis for refusing information initially.

The duty to register must, however, be read with section 173(3). In *Lalita Kumari v. Government of Uttar Pradesh*, the Supreme Court held, under section 154 of the CrPC, that registration is mandatory where information discloses a cognizable offence, subject to the limited inquiry recognised in that judgment.¹⁹ The post-BNSS position was clarified in *Imran Pratapgarhi v. State of Gujarat*. The Supreme Court held that section 173(1) substantially corresponds to section 154 of the CrPC, but section 173(3) creates a statutory exception: for cognizable offences punishable with three years or more but less than seven years, the officer may, with the prior permission of the specified superior officer, conduct a preliminary inquiry within fourteen days to determine whether a prima facie case exists.²⁰ If it exists, the FIR must be registered; if not, the informant must be told so that the remedy under section 173(4) can be pursued.

¹⁷ Ministry of Home Affairs, Government of India, Lok Sabha Unstarred Question No. 4118, Cyber Crime Cases 2–3 (Mar. 17, 2026).

¹⁸ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023, § 173(1)–(2).

¹⁹ *Lalita Kumari v. Government of Uttar Pradesh*, (2014) 2 S.C.C. 1.

²⁰ *Imran Pratapgarhi v. State of Gujarat*, (2025) INSC 410; The Bharatiya Nagarik Suraksha Sanhita, 2023, § 173(3)–(4).

The phrase “irrespective of the area” also supports the Zero FIR. Its function is to ensure that recording is not defeated because the victim, offender, recipient account, or intermediary is located elsewhere. In *Satvinder Kaur v. State (Government of NCT of Delhi)*, the Supreme Court held that uncertainty regarding territorial jurisdiction at the investigative stage does not justify quashing the investigation; the police may investigate and, if the offence is found to lie outside their jurisdiction, forward the case appropriately.²¹ For digital financial fraud, this principle is important because the victim may act in one State, the communication may originate elsewhere, and the transferred money may move through accounts maintained in several jurisdictions.

The Zero FIR, however, resolves access to registration, not the allocation of investigation. Section 175 authorises the officer in charge to investigate a cognizable case that a court having local jurisdiction could inquire into or try. Section 202 recognises multiple connecting factors for cheating through electronic communications: the place from which the communication was sent or received, and the place where property was delivered by the deceived person or received by the accused.²² These factors broaden jurisdiction but may create concurrent claims among police stations and courts.

The difficulty is institutional rather than purely doctrinal. The NCRP centralises complaint receipt, while investigation, evidence collection, account action, and prosecution remain territorially distributed. Relevant data may be held by banks, intermediaries, or platforms outside the investigating State or outside India.²³ A coherent framework therefore requires prompt FIR determination, recorded transfer between agencies, continuity of emergency fund-preservation measures, and clear identification of the responsible investigating officer. Without such continuity, centralised reporting may coexist with fragmented enforcement, allowing delay at jurisdictional boundaries to weaken prosecution and victim recovery in actual legal practice.

V. INTERCEPTING AND RESTORING FRAUD PROCEEDS: LIEN, SEIZURE, ATTACHMENT, AND RESTITUTION UNDER THE BNSS

Digital financial fraud requires intervention before disputed money is dispersed through successive accounts, converted into other assets, or withdrawn. Yet speed cannot dissolve legal distinctions. A lien placed through the Citizen Financial Cyber Fraud Reporting and Management System, a police seizure under section 106 of the Bharatiya Nagarik Suraksha Sanhita, 2023, a judicial attachment under section 107, and the final restoration of funds to a

²¹ *Satvinder Kaur v. State (Government of NCT of Delhi)*, (1999) 8 S.C.C. 728.

²² The Bharatiya Nagarik Suraksha Sanhita, 2023, §§ 175(1)–(2), 202(1).

²³ Jean-Baptiste Maillart, *The Limits of Subjective Territorial Jurisdiction in the Context of Cybercrime*, 19 ERA F. 375, 376–80 (2019).

victim are separate measures with different purposes and safeguards. The central defect is not the absence of powers, but the failure to state clearly when an emergency administrative restraint must become a judicially supervised proceeding.

The first stage is complaint-based preservation. The Delhi High Court in *Malabar Gold and Diamond Ltd. v. Union of India* reproduced the CFCFRMS clarification that a bank or intermediary may place the disputed amount on lien on the basis of an acknowledgement number generated through the helpline or the NCRP, so that the amount may later be refunded after investigation. The Court distinguished such an amount-specific lien from debit-freezing the entire account.²⁴ This distinction is essential. A lien preserves a quantified sum; it neither proves that the account holder participated in the fraud nor finally determines the complainant's entitlement. The portal mechanism therefore performs a preventive, not an adjudicatory, function.

The 2026 Standard Operating Procedure now provides a uniform administrative process governing temporary holds, seizure, interim custody, restoration, and grievance redressal within the NCRP–CFCFRMS framework. The Supreme Court has directed the Ministry of Home Affairs to formally adopt and implement the SOP throughout the country and has required adjudicating authorities to comply with it. The legal issue is therefore no longer the complete absence of an administrative process, but whether the statutory basis, duration, and scope of a temporary hold are sufficiently clear, and whether continued restraint is promptly transferred to an appropriate statutory or judicial process.²⁵

The restraint is implemented by banks or financial intermediaries, often after police communication, within the CFCFRMS workflow. Its legitimacy must therefore depend on a narrowly defined emergency purpose, identification of the disputed amount, and transition to statutory process. Otherwise, an administrative hold may continue without the safeguards attached to seizure or attachment.

Section 106 of the BNSS authorises a police officer to seize property alleged or suspected to have been stolen, or found in circumstances that create suspicion of an offence, and requires the seizure to be reported forthwith to the jurisdictional Magistrate.²⁶ The provision substantially carries forward section 102 of the CrPC. In *State of Maharashtra v. Tapas D. Neogy*, the

²⁴ *Malabar Gold & Diamond Ltd. v. Union of India*, W.P.(C) 4198/2025 (Delhi H.C.).

²⁵ Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, STANDARD OPERATING PROCEDURE FOR NCRP–CFCFRMS: PUTTING ON HOLD, SUSPENSION, SEIZURE, INTERIM CUSTODY, RESTORATION OF MONEY AND GRIEVANCE REDRESSAL (Jan. 2, 2026); In re Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Criminal) No. 3 of 2025.

²⁶ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023, § 106.

Supreme Court treated a bank account as “property” capable of seizure under the former provision. In *Shento Varghese v. Julfikar Husen*, the Court explained that the seized property must have a direct or close link with the alleged offence, while holding that delayed reporting to the Magistrate does not automatically nullify the seizure.²⁷ These decisions remain relevant to section 106, but they arose under the earlier Code and did not interpret the separate attachment-and-restoration design now found in section 107.

Section 107 addresses property believed to have been derived or obtained, directly or indirectly, from criminal activity or the commission of an offence. An investigating officer may, with the approval of the Superintendent or Commissioner of Police, apply to the competent Court or Magistrate for attachment. Ordinarily, a fourteen-day show-cause notice and a reasonable opportunity of hearing must be provided. An interim ex parte order is permitted where notice would defeat the object of the attachment or seizure. After examining the material and the explanation, the Court or Magistrate may determine whether the property constitutes proceeds of crime.²⁸ This structure requires more than suspicion associated with a transaction chain: it requires senior approval, judicial scrutiny, and an opportunity to contest the alleged nexus.

The remedial importance of section 107 lies in subsections (6) to (8). Once the Court or Magistrate finds the property to be proceeds of crime, the District Magistrate is directed to distribute it rateably among the persons affected by the crime. Distribution must occur within sixty days from receipt of the order. Where no claimant is ascertainable, or a surplus remains after satisfying claimants, the property stands forfeited to the Government.²⁹ The provision therefore connects attachment with restoration, but leaves important matters unresolved: the time within which an emergency lien must be placed before a Magistrate; the evidentiary standard for verifying claimants; the treatment of multiple victims claiming the same amount; and the position of bona fide recipients who supplied goods or services before receiving tainted funds.

Sections 497 and 503 provide additional powers concerning the custody, disposal, and delivery of property. Section 497 applies where property is produced before a criminal court or Magistrate during investigation, inquiry, or trial; section 503 applies where a police seizure is reported but the property is not produced before a criminal court. These provisions may support interim custody or delivery to the person entitled to possession. They should not be used to bypass section 107 where the real objective is the attachment and rateable distribution of alleged

²⁷ State of Maharashtra v. Tapas D. Neogy, (1999) 7 S.C.C. 685 (India); *Shento Varghese v. Julfikar Husen*, (2024) INSC 407.

²⁸ The Bharatiya Nagarik Suraksha Sanhita, 2023, § 107(1)–(5).

²⁹ Id. § 107(6)–(8).

proceeds. Section 107 is the specific restitution-oriented provision; sections 497 and 503 are principally custody-and-possession provisions.³⁰

The emerging High Court jurisprudence initially favoured this separation. In *Headstar Global Pvt. Ltd. v. State of Kerala*, *Kartik Yogeshwar Chatur v. Union of India*, and *Malabar Gold*, the courts reasoned that debit-freezing directed at securing proceeds should follow section 107 rather than the general seizure power in section 106. That position cannot now be described as settled. In December 2025, the Supreme Court expressly recorded the conflicting views of the Kerala High Court in *Rasmi K.R. v. NCCRP* and the Bombay High Court in *Kartik Yogeshwar Chatur v. Union of India*. Pending further consideration, it directed that where an amount lying in a bank account is prima facie traceable to a digital-arrest or other cybercrime already reported to the State police, the CBI, or the NCRP, the authorities may freeze the account with or without an FIR. In February 2026, the Court further directed the nationwide adoption and implementation of the NCRP–CFCFRMS SOP. These interim directions facilitate immediate preservation but do not finally settle the statutory relationship between seizure under section 106 and attachment or restoration under section 107.³¹

This unsettled position strengthens the need for a coherent statutory sequence. Emergency preservation may occur, but its scope should remain confined to the traceable disputed amount. Continued restraint should be supported by recorded reasons, prompt reporting, identification of the responsible investigator, and timely recourse to judicial supervision. The law should distinguish evidentiary seizure from proceeds-based attachment without disabling urgent intervention. Only such a sequence can transform the CFCFRMS from a mechanism that temporarily interrupts dissipation into one that lawfully identifies, preserves, and restores fraud proceeds.

VI. JUDICIAL SAFEGUARDS AND THE RIGHTS OF ACCOUNT HOLDERS

Account restraint affects more than the disputed transaction. It may prevent the payment of salaries, taxes, suppliers, and household expenses, while dishonoured instructions can damage credit and commercial reputation. The legal question is not whether suspected fraud proceeds may be preserved, but whether the measure has statutory authority, a demonstrable nexus with the offence, proportionate scope, and effective judicial review. Victim protection and account-

³⁰ Id. §§ 497, 503.

³¹ *Headstar Global Pvt. Ltd. v. State of Kerala*, (2025) INDKER 39285; *Kartik Yogeshwar Chatur v. Union of India*, (2025) INBHC-NAG 12612; *Malabar Gold & Diamond Ltd. v. Union of India*, W.P.(C) 4198/2025 (Delhi H.C.); *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025.

holder rights are not opposing objectives: arbitrary freezing can undermine confidence in the very payment system that rapid intervention seeks to protect.

The starting point remains *State of Maharashtra v. Tapas D. Neogy*, where the Supreme Court held that a bank account is “property” capable of seizure under section 102 of the CrPC.³² That proposition prevents funds connected with crime from becoming immune merely because they exist as a bank balance. It does not authorise restraint without a transaction nexus. In *Shento Varghese v. Julfikar Husen*, the Supreme Court emphasised that property seized under section 102 must have a direct or close link with the alleged offence. The Court also held that delayed reporting to the Magistrate is an irregularity rather than an automatic ground for nullification, while recognising that the officer remains accountable.³³ Applied to section 106 of the BNSS, these principles support both effective preservation and procedural supervision.

Recent High Court decisions have developed a stricter distinction between seizure and attachment. In *Neelkanth Pharma Logistics Pvt. Ltd. v. Union of India*, the Delhi High Court criticised the freezing of an entire account because an identifiable amount connected with cyber fraud had entered it, particularly where the holder was neither accused nor suspected. *Malabar Gold and Diamond Ltd. v. Union of India* similarly treated indefinite and unreasoned restraint as unjustified where the authorities could not demonstrate complicity.³⁴ The decision stressed that innocent recipients should not suffer merely because suspected proceeds temporarily passed through their accounts, and preferred an amount-specific lien over blanket debit-freezing.

These decisions express a persuasive proportionality principle, but their statutory conclusion must be presented cautiously. *Headstar Global* and *Kartik Yogeshwar Chatur* held that debit-freezing to secure alleged proceeds must proceed under section 107 rather than section 106. The Supreme Court subsequently recorded the conflicting High Court views in its digital-arrest suo motu case and, in March 2026, stayed the operation of *Kartik*.³⁵ The national position remains unsettled. A publication-oriented analysis should not describe the section 106–107 distinction as conclusively settled; it should identify the competing need for immediate preservation and the safeguards attached to continued restraint.

Constitutional scrutiny supplies the governing standard. An unexplained distinction between similarly situated account holders may attract Article 14; disabling a business account may

³² *State of Maharashtra v. Tapas D. Neogy*, (1999) 7 S.C.C. 685 (India).

³³ *Shento Varghese v. Julfikar Husen*, (2024) INSC 407.

³⁴ *Neelkanth Pharma Logistics Pvt. Ltd. v. Union of India*, (2025) INDEL 1214; *Malabar Gold & Diamond Ltd. v. Union of India*, W.P.(C) 4198/2025 (Delhi H.C.).

³⁵ *Headstar Global Pvt. Ltd. v. State of Kerala*, (2025) INDKER 39285; *Kartik Yogeshwar Chatur v. Union of India*, (2025) INBHC-NAG 12612; *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025; *Union of India v. Kartik Yogeshwar Chatur*, SLP (Crl.) Diary No. 72660 of 2025.

burden Article 19(1)(g); prolonged restraint affecting subsistence may implicate Article 21; and deprivation of access to property requires the authority of law under Article 300A.³⁶ These guarantees do not necessarily require advance notice, since prior notice may facilitate the withdrawal of the disputed amount. They do require recorded reasons, restraint limited to what is traceable, prompt post-restraint notice, disclosure sufficient to challenge the measure, and access to a judicial forum.

Special protection is required for downstream recipients. Transaction-layer proximity is not equivalent to culpability. A merchant may receive payment for genuine goods, an employee may receive salary, or an intermediary may process funds without knowledge of the fraud. Continued restraint should depend on material showing complicity, conscious receipt, or a legally traceable claim to the disputed amount.³⁷ Where the account contains both legitimate and disputed funds, the least restrictive measure is a lien confined to the quantified amount.

Courts should apply a structured test: identify the statutory source; establish the account's direct nexus with the offence; state the exact amount restrained; explain why a narrower measure is inadequate; confirm reporting or application to the competent Magistrate; provide an opportunity for review; and reassess necessity periodically. Emergency action may precede a hearing, but it cannot mature into an indefinite financial disability. Judicial supervision should convert temporary preservation into a reasoned determination of whether the money must remain restrained, be released, or proceed towards restoration.

VII. REFORMING THE RESTITUTION FRAMEWORK: RECOMMENDATIONS AND CONCLUSION

India now possesses an administrative pathway connecting cybercrime reporting, emergency restraint, interim custody, and restitution, but uncertainty remains regarding its statutory foundation, uniform implementation, and judicial supervision. The 2026 NCRP–CFCFRMS Standard Operating Procedure addresses this problem by introducing a Money Restoration Module, alternative processes for interim custody, procedures for competing claims, and a grievance mechanism.³⁸ Its practical value is substantial, but an administrative SOP cannot resolve the statutory ambiguity concerning the relationship among lien, seizure under section

³⁶ India Const. arts. 14, 19(1)(g), 21, 300A.

³⁷ *Malabar Gold & Diamond Ltd. v. Union of India*, W.P.(C) 4198/2025 (Delhi H.C.); Dakshina Chandra, *Examining the Contours and Challenges of the National Cybercrime Reporting Portal in Countering Digital Financial Frauds*, 8 J. Victimology & Victim Just. 65, 79–81 (2025).

³⁸ Indian Cyber Crime Coordination Centre, Ministry of Home Affairs, STANDARD OPERATING PROCEDURE FOR NCRP–CFCFRMS: PUTTING ON HOLD, SUSPENSION, SEIZURE, INTERIM CUSTODY, RESTORATION OF MONEY AND GRIEVANCE REDRESSAL 22–28 (Jan. 2, 2026), https://i4c.mha.gov.in/theme/resources/SOP_Layout_04_with%20Cover%20and%20back.pdf.

106, judicial attachment under section 107, and disposal under sections 497 and 503 of the BNSS.³⁹

Reform should establish a defined sequence: complaint-based preservation of the traceable amount; prompt verification and FIR determination; identification of the investigating officer; judicial recourse where continued restraint, attachment, or competing ownership claims arise; and restoration to the verified claimant. Whole-account debit-freezing should remain exceptional. The Delhi High Court in *Malabar Gold and Diamond Ltd. v. Union of India* treated the blanket and indefinite freezing of an account holder not shown to be complicit as disproportionate, while the Supreme Court has acknowledged the conflicting High Court views on the source of freezing powers under the BNSS.⁴⁰ Until that conflict is authoritatively resolved, restraint should follow the least restrictive, reasoned, and reviewable course.

The SOP's grievance timelines, digital tracking, and proposed integration of the Money Restoration Module with e-Courts should be supported by binding rules, uniform bank directions, and the publication of outcome data.⁴¹ Official reporting must distinguish amounts reported lost, placed on hold, released, judicially attached, given in interim custody, and finally restored.

India does not primarily lack cyber-fraud offences. It lacks procedural coherence between technological intervention and enforceable restitution. A victim-centred framework must preserve speed without normalising indefinite restraint, protect innocent account holders without frustrating tracing, and convert intercepted funds into timely, lawful, and reviewable recovery.

³⁹ The Bharatiya Nagarik Suraksha Sanhita, 2023, No. 46, Acts of Parliament, 2023, §§ 106–107, 497, 503 (India).

⁴⁰ *Malabar Gold & Diamond Ltd. v. Union of India*, W.P.(C) 4198/2025 (Delhi H.C.); *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Criminal) No. 3 of 2025.

⁴¹ Indian Cyber Crime Coordination Centre, *supra* note 38, at 22–28.