Page 1345 - 1360

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 4

2026

Arbitrary Freezing of Bank Accounts in Cyber Crime Investigations: A Critical Analysis of Section 106 BNSS and the Plight of the Innocent

BHAWNA SHARMA*

ABSTRACT

With the rapid acceleration of digital transactions in India, driven by the Unified Payments Interface, immediate payment services and e-commerce ecosystems, the National Cyber Crime Reporting Portal has become a frontline mechanism for law enforcement agencies seeking to contain online financial fraud. The operationalisation of cyber fraud reporting, and in particular the automated and unverified issue of debit-freeze instructions, has nevertheless produced severe procedural irregularity and serious rights concerns. Under Section 106 of the Bharatiya Nagarik Suraksha Sanhita, 2023, formerly Section 102 of the Code of Criminal Procedure, 1973, police officers routinely instruct banks to freeze operational accounts, and those instructions frequently extend to distant, multi-layered downstream transactions at Layer 1, Layer 2 and Layer 3 without prior verification, notice or judicial oversight. This paper critically evaluates the statutory, procedural and constitutional mechanisms governing the freezing of bank accounts during cybercrime investigations. It shows how automated portal complaints are increasingly used to settle private commercial disputes, contractual disagreements and service delivery conflicts, effectively criminalising routine civil transactions. It subjects these administrative actions to constitutional scrutiny under Articles 14, 19(1)(g) and 21 of the Constitution of India, emphasising the systemic violation of the cardinal principle of natural justice, audi alteram partem, and it analyses the precedents of the High Courts and the Supreme Court that press for a balanced investigative protocol. The paper closes with legislative and administrative recommendations, arguing for a mandatory preliminary inquiry, the strict enforcement of lien-marking restricted to the disputed quantum of funds, time-bound portal mechanisms and deterrent penalties for frivolous complaints.

Keywords: *cyber crime, national cyber crime reporting portal, section 106 BNSS, section 102 CrPC, debit freeze, lien-marking, Article 21, Article 19(1)(g), natural justice, commercial disputes, proportionality, cyber law jurisprudence*

---

* Author is a Student at Sanskaram University, Jhajjar, Haryana, India.

I. Introduction

A. The Digital Payment Revolution and the Rise of Cyber Fraud

The rapid digitisation of the Indian economy over the past decade stands as one of the most remarkable transformations in contemporary financial governance. The advent of the Unified Payments Interface (UPI), digital wallets, real-time gross settlement systems and interconnected e-commerce payment gateways has democratised access to the banking sector. While this transition from cash-based transactions to instantaneous electronic fund transfers has brought unprecedented convenience, commercial speed and financial inclusion, it has simultaneously opened new avenues for sophisticated digital financial crime.

Cybercriminals today operate through complex, distributed networks. They use tactics such as phishing, identity theft, vishing, SIM swapping, fake merchant setups and malicious payment links to deceive unsuspecting victims into transferring substantial sums of money. The velocity with which these illicit transactions take place presents a formidable challenge to law enforcement agencies. Money transferred from a victim's account is often routed through multiple intermediary accounts within minutes, making recovery nearly impossible once the funds are withdrawn as cash or converted into cryptocurrency.

B. Law Enforcement Responses: The Emergency Helpline 1930 and the National Cyber Crime Reporting Portal

To address the mounting threat of online financial crime, the Ministry of Home Affairs (MHA), under the aegis of the Indian Cyber Crime Coordination Centre (I4C), conceptualised and deployed the National Cyber Crime Reporting Portal (NCRP) alongside the emergency helpline number 1930.[1] This centralised framework was created to facilitate real-time tracking, reporting and interception of the proceeds of crime. When a victim of financial fraud reports a transaction, the portal alerts recipient financial institutions and law enforcement agencies across jurisdictions, enabling investigating officers to trace the chain of funds and to freeze them before they are siphoned away.

C. The Emerging Crisis: Blanket Freezes and Procedural Overreach

While the statutory intent behind the real-time interception of the proceeds of crime is unquestionably legitimate, the practical execution of this mechanism has generated a parallel

[1] Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C). The National Cyber Crime Reporting Portal and the toll-free helpline 1930 are operated under I4C, and the Citizen Financial Cyber Fraud Reporting and Management System was launched under it in 2021 to enable the near real-time reporting of financial cyber fraud to banks, wallets and other intermediaries.

administrative crisis. Investigating officers, heavily reliant on automated complaint feeds from the NCRP, frequently issue administrative orders to banking entities instructing them to execute complete debit freezes on target accounts.

Crucially, these freezing directions are rarely confined to the primary recipient account (Layer 1). They routinely cascade down through secondary (Layer 2) and tertiary (Layer 3) accounts. As a result, legitimate business entities, logistics operators, traders, service providers and ordinary citizens find their primary operational bank accounts frozen without prior warning or an opportunity to be heard.

When a business's operational account is subjected to a total debit freeze, the consequences are immediate and severe. Business owners are rendered unable to pay employee salaries, discharge tax obligations, service bank loans or meet routine vendor invoices. What was designed as a protective, emergency mechanism to preserve the proceeds of crime has thus evolved into a blunt instrument of procedural harassment, raising profound questions of administrative accountability, statutory compliance and fundamental constitutional guarantees.

II. Statutory Framework and the Power of Freezing

A. The Transition from Section 102 CrPC to Section 106 BNSS

The legal authority exercised by police authorities to freeze bank accounts during a criminal investigation was historically derived from Section 102 of the Code of Criminal Procedure, 1973 (CrPC). With the enactment of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), the corresponding power is now codified in Section 106 of the BNSS.[2]

Section 106(1) of the BNSS provides:

> Any police officer may seize any property which may be alleged or suspected to have been stolen, or which may be found under circumstances which create suspicion of the commission of any offence.[3]

Section 106(2) requires a police officer who is subordinate to the officer in charge of a police station to report the seizure forthwith to that officer. Section 106(3) mandates that every police officer acting under sub-section (1) shall forthwith report the seizure to the Magistrate having jurisdiction, and permits custody of the property to be given to any person on a bond where the

[2] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 106 (India), replacing Code of Criminal Procedure, No. 2 of 1974, § 102 (India).
[3] Bharatiya Nagarik Suraksha Sanhita § 106(1).

property cannot conveniently be transported to the court or where its continued retention in police custody is not considered necessary for the investigation.[4]

The key elements of the Section 106 framework may be stated as follows:

- Statutory mandate: a reasonable suspicion that the property, including a credit balance in a bank account, is linked to an offence.
- Seizure or freeze power: the issuance of debit-freeze directions to banks.[5]
- Judicial duty: the mandatory and immediate reporting of the freeze to the jurisdictional Magistrate.

B. Legislative Intent and Comparative Nuances between Section 102 CrPC and Section 106 BNSS

While Section 106 of the BNSS largely mirrors the textual construction of Section 102 of the CrPC, the broader statutory context of the BNSS emphasises digital evidence handling, swift investigative timelines and a modernised criminal administration. This legislative modernisation has nevertheless left a statutory gap in relation to digital assets and electronic bank accounts. Unlike physical property, money in a bank account is fungible and highly dynamic.

When Section 102 of the CrPC was framed in 1973, electronic banking, instant payment gateways and automated algorithms did not exist. The application of a general property seizure provision to virtual, fluid bank balances creates structural friction. Section 106 of the BNSS introduces no procedural safeguard, and no statutory distinction, between tangible physical property such as vehicles, weapons or currency notes and credit balances held in commercial banking accounts. Consequently, investigating officers apply powers designed for physical seizure to intangible financial balances, resulting in blanket freezes rather than precise lien-marking.[6]

---

[4] *Id.* § 106(2)-(3).

[5] *But see Malabar Gold and Diamond Ltd. v. Union of India*, 2026 SCC OnLine Del 297 (Del. HC) (holding that § 106 of the BNSS authorises seizure for evidentiary purposes alone, that the freezing of a bank account amounts to attachment rather than seizure, and that attachment requires an order of the competent Magistrate under § 107 of the BNSS).

[6] BHARATIYA NAGARIK SURAKSHA SANHITA § 107 (attachment, forfeiture or restoration of property: a police officer who has reason to believe that property is derived from criminal activity must, with the approval of the Superintendent or Commissioner of Police, apply to the Court or Magistrate, which issues a show-cause notice returnable in fourteen days before passing an order of attachment).

C. Bank Accounts as "Property" and the Essential Preconditions

The jurisprudence treating money in a bank account as "property" capable of seizure under procedural criminal law was settled by the Supreme Court of India in *State of Maharashtra v. Tapas D. Neogy*. The Court held that the term "property" in Section 102 of the CrPC, now Section 106 of the BNSS, is broad enough to include a bank account where there is a direct connection between that account and the alleged criminal activity.[7]

The exercise of this power is not, however, unfettered. The statutory framework imposes three indispensable prerequisites:

- Direct nexus: there must exist a verifiable, direct connection between the bank account, or the specific funds within it, and the alleged crime.
- Reasonable suspicion: the investigating officer must entertain a suspicion founded on objective, credible material rather than on subjective speculation or an unverified claim.
- Mandatory reporting to the Magistrate: the act of freezing must be reported forthwith to the jurisdictional Magistrate, a requirement that serves as a vital judicial check on arbitrary executive action.[8]

D. The Role of the Information Technology Act, 2000

In cybercrime investigations, Section 106 of the BNSS operates alongside the provisions of the Information Technology Act, 2000 (IT Act). Section 66D of the IT Act prescribes punishment for cheating by personation using a computer resource.[9] Investigating agencies routinely invoke Section 91 of the CrPC, now Section 94 of the BNSS, to require intermediaries and financial institutions to produce transactional records, internet protocol logs and system audit trails, while Section 79A of the IT Act supplies the machinery by which a notified Examiner of Electronic Evidence gives expert opinion on the electronic records so obtained.[10]

---

[7] *State of Maharashtra v. Tapas D. Neogy*, (1999) 7 SCC 685 (India) (a bank account is "property" within § 102 of the CrPC, the two conditions being the existence of property and a suspicion of the commission of an offence in respect of that specific property).

[8] *Id.*; BHARATIYA NAGARIK SURAKSHA SANHITA § 106(3).

[9] INFORMATION TECHNOLOGY ACT, No. 21 of 2000, § 66D (India).

[10] BHARATIYA NAGARIK SURAKSHA SANHITA § 94 (summons to produce a document or other thing, replacing § 91 of the CrPC); INFORMATION TECHNOLOGY ACT § 79A (empowering the Central Government to notify any Department, body or agency as an Examiner of Electronic Evidence to give expert opinion on evidence in electronic form).

 [ISSN 2581-5369]

E. The Practical Reality: Automated Execution versus Statutory Mandates

Although the statutory framework contemplates judicial oversight and a reasonable suspicion founded on objective material, the operational implementation of the NCRP diverges significantly from these principles. In practice, the system functions as follows:

- Step 1: a complainant logs a report on the 1930 helpline or the NCRP portal alleging financial loss.
- Step 2: the automated portal traces the path of the funds on the basis of the account details supplied by the complainant.
- Step 3: the portal automatically generates freeze alerts to the compliance desks of the destination banks.
- Step 4: police authorities endorse these automated alerts without conducting any preliminary verification, issuing formal directions to banks under Section 106 of the BNSS.
- Step 5: banks execute a total debit freeze on the target accounts without verifying whether the account balance exceeds the disputed amount, and without evaluating the *bona fides* of the account holder.

This administrative workflow bypasses the requirement of objective assessment, turning a power intended for extraordinary circumstances into a routine administrative reflex.

III. Weaponisation of Cyber Portals: Commercial Disputes versus Cyber Fraud

A. The Conversion of Civil Transactions into Criminal Offences

One of the most troubling outcomes of the current automated freezing system is the conversion of routine civil and commercial disputes into cybercrime investigations. The process flow of account freezing in a commercial dispute is as follows:

- A disgruntled customer files a false or exaggerated fraud report on the NCRP or the 1930 portal.
- An automated NCRP alert is sent directly to the compliance desks of the recipient banks.
- A notice under Section 106 of the BNSS is issued without any preliminary verification.
- The operational account of the merchant or business is frozen overnight.

In standard commercial relationships, such as supply chains, logistics, real estate services and e-commerce, disputes frequently arise over payment schedules, quality of goods, delivery delays or contractual breaches. Such matters fall within the realm of civil law and are governed by the Indian Contract Act, 1872, the Sale of Goods Act, 1930, and the Specific Relief Act, 1963.[11]

Disgruntled contracting parties have discovered, however, that filing a civil suit requires court fees, procedural compliance and time. By contrast, lodging a complaint on the NCRP portal alleging online financial fraud provides immediate, unilateral leverage. Because the portal does not require the submission or evaluation of contracts, delivery receipts or invoices before a freeze alert is issued, a bad-faith complainant can effectively freeze a business partner's bank account overnight.

B. Impact on the Logistics, Transportation and Trade Sectors

The logistics and transport sectors illustrate the practical impact of this problem. Vehicle transport operators, freight forwarding agencies and goods carriers frequently require advance payments before dispatching consignments. If a dispute arises over transit delays, minor damage to goods or demurrage charges, clients sometimes lodge cybercrime complaints alleging that the advance payment was siphoned through online fraud. The Delhi High Court has recently had occasion to consider precisely such a freeze imposed on the account of a pharmaceutical logistics company.[12]

Upon receipt of the automated alert, the transport operator's bank account is placed under a total debit freeze. The operator is then unable to purchase fuel, pay toll charges or settle driver allowances, paralysing an entire fleet.

C. The Cascading "Layering" Effect on Downstream Accounts

The problem is further exacerbated by the tracking of downstream accounts (Layer 1, Layer 2 and Layer 3). In modern banking, funds move continuously through multiple transactions. The transaction flow operates as follows:

> Alleged fraud source -> Layer 1 account (primary recipient) -> Layer 2 account (vendor or fuel station) -> Layer 3 account (employee salary or third party)

---

[11] INDIAN CONTRACT ACT, No. 9 of 1872 (India); SALE OF GOODS ACT, No. 3 of 1930 (India); SPECIFIC RELIEF ACT, No. 47 of 1963 (India).

[12] *Neelkanth Pharma Logistics Pvt. Ltd. v. Union of India*, 2025 SCC OnLine Del 1055 (Del. HC) (observing that the possibility of marking a lien on the disputed amount, wherever identifiable, should be explored as the more appropriate interim measure, and directing that the judgment be forwarded to the MINISTRY OF HOME AFFAIRS for the framing of uniform standard operating procedures).

Consider the following scenario:

- Layer 1: a merchant receives Rs. 50,000 for goods sold to a buyer who later lodges a fraud complaint.
- Layer 2: the merchant uses those funds alongside legitimate revenues to pay a fuel supplier Rs. 20,000 and a raw material vendor Rs. 30,000.
- Layer 3: the fuel supplier uses those receipts to pay employee wages.

Under current portal workflows, automated tracking alerts are sent along the entire transactional chain. Investigating officers routinely issue blanket freeze notices under Section 106 of the BNSS to the fuel supplier at Layer 2 and to the employee at Layer 3. These third parties, who have no knowledge of and no connection with the underlying dispute, find their bank accounts frozen simply because they received payment from an account flagged on the portal. This multi-layered freezing creates significant financial distress across entire supply chains.[13]

D. The Role of FinTech Intermediaries, Payment Gateways and Nodal Accounts

Modern e-commerce ecosystems rely heavily on an intermediary FinTech architecture that includes payment gateways and nodal escrow accounts. When a disputed transaction occurs on an e-commerce platform, the automated NCRP mechanism sends freezing directives not only to individual bank accounts but also to the merchant nodal accounts held with FinTech platforms.

Because FinTech intermediaries operate pooled nodal accounts containing funds belonging to thousands of independent merchants, a freeze notice issued against one registered merchant often leads compliance desks to lock the entire nodal sub-wallet. This creates a severe multiplier effect, in which hundreds of unrelated small vendors find their daily settlements withheld by payment gateways complying with broad police notices. The absence of granular, transaction-specific hold capabilities within traditional bank and intermediary integration protocols turns administrative efficiency into an instrument of widespread collateral commercial damage.

IV. Constitutional Scrutiny and the Violation of Natural Justice

The practice of executing blanket account freezes on the basis of unverified, automated complaints raises significant constitutional concerns.

[13] *See Neelkanth Pharma Logistics Pvt. Ltd.*, *supra* note 12 (deprecating the freezing of an entire account where the holder is not shown to be complicit in the offence).

A. Denial of Natural Justice (Audi Alteram Partem)

The principle of *audi alteram partem*, that no person should be condemned unheard, is a core requirement of administrative and criminal procedure. It requires that an individual affected by an adverse administrative or statutory order be given adequate notice and an opportunity to present their case.[14]

Under current freezing practices, account holders receive no prior notice, no explanation and no opportunity to produce invoices, bills or proof of service delivery before a debit freeze is applied. Account holders typically learn of the freeze only when an attempted transaction, such as a card payment or a cheque presentation, is declined by the bank.

While emergency provisions under criminal procedure may justify a temporary interim action without prior notice in exceptional situations, the complete absence of a mandatory post-decisional hearing or of any rapid administrative remedy violates established principles of procedural fairness.

B. Deprivation of the Right to Livelihood (Article 21)

Article 21 of the Constitution of India guarantees that no person shall be deprived of life or personal liberty except according to procedure established by law. The Supreme Court expanded the scope of Article 21 in *Olga Tellis v. Bombay Municipal Corporation* and *Maneka Gandhi v. Union of India*, establishing that the right to life includes the right to live with human dignity and the right to a livelihood.[15,16]

The key constitutional rights implicated are the following:[17]

- Article 14: equality before the law and protection against arbitrary state action.
- Article 19(1)(g): the right to practise any trade, business or profession.
- Article 21: the right to life and livelihood and the requirement of a fair procedure.

When an individual's entire bank account, containing working capital, personal savings and business funds, is subjected to a complete debit freeze, that person is deprived of the financial means required to meet basic needs such as the purchase of food, medical expenses and rent. Subjecting citizens to total financial paralysis without procedural safeguards represents an unconstitutional infringement of Article 21.

---

[14] *Maneka Gandhi v. Union of India*, (1978) 1 SCC 248 (India) (a procedure that deprives a person of a right under Article 21 must be just, fair and reasonable).
[15] *Olga Tellis v. Bombay Municipal Corporation*, (1985) 3 SCC 545 (India).
[16] *Maneka Gandhi*, *supra* note 14.
[17] INDIA CONST. arts. 14, 19(1)(g), 21.

C. Infringement of the Right to Trade and Business under Article 19(1)(g)

Article 19(1)(g) guarantees to all citizens the right to practise any profession, or to carry on any occupation, trade or business. That right is subject only to reasonable restrictions imposed by law under Article 19(6) in the interests of the general public.[18]

For a restriction to be considered reasonable under Article 19(6), it must satisfy the test of proportionality articulated in *Modern Dental College & Research Centre v. State of Madhya Pradesh* and reaffirmed in *Justice K.S. Puttaswamy (Retd.) v. Union of India*.[19,20] The test of proportionality requires that:

- the measure must serve a legitimate state goal;
- the measure must be rationally connected to that goal;
- the measure must be the least restrictive means available to achieve the objective; and
- the measure must not have a disproportionate impact on the rights of the individual.

Executing a total debit freeze on an operational business account containing lakhs of rupees on account of a disputed transaction involving a fraction of that amount fails the test of proportionality. A less restrictive alternative, namely placing a hold or lien exclusively on the disputed sum, achieves the investigative goal of preserving the proceeds of crime without causing the collapse of the business. Total account freezes therefore represent an unreasonable restriction on the fundamental right guaranteed by Article 19(1)(g).

V. Judicial Trends and Precedents

The High Courts and the Supreme Court of India have increasingly intervened to curb the improper exercise of the power to freeze bank accounts under Section 102 of the CrPC, now Section 106 of the BNSS.

A. The Doctrine of Lien-Marking: Proportionality in Practice

Courts have frequently addressed orders that freeze entire accounts where the alleged fraudulent amount represents only a small portion of the total balance.

In *Dr. Sajeer v. Reserve Bank of India*, the High Court of Kerala examined a batch of petitions by traders whose operational accounts had been frozen in full after cyber fraud complaints, although the police requisitions specified the exact sums suspected to have been credited to those accounts. The Court directed that freezing orders be confined to the amount involved in

---

[18] India Const. art. 19(1)(g), (6).

[19] *Modern Dental College & Research Centre v. State of Madhya Pradesh*, (2016) 7 SCC 353 (India).

[20] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).

the alleged crime as mentioned in the requisition, leaving the account holder free to operate the remaining balance.[21]

Similarly, in *Teesta Atul Setalvad v. State of Gujarat*, while the Supreme Court upheld the power to freeze accounts where the proceeds of crime are directly traced, it emphasised that the power under criminal procedure must be exercised strictly within statutory limits and subject to judicial review, and that the investigating officer should issue instructions for de-freezing once satisfied with the explanation offered.[22]

Decision	Principle
State of Maharashtra v. Tapas D. Neogy, (1999) 7 SCC 685	A bank account is "property" for the purposes of Section 102 of the CrPC, now Section 106 of the BNSS, but a direct nexus with the alleged offence must be shown.
Dr. Sajeer v. Reserve Bank of India, WP(C) No. 12960 of 2023 (Ker. HC)	A freeze must be confined to the amount specified in the police requisition; the remaining balance must stay operable.
Nevada Properties Pvt. Ltd. v. State of Maharashtra, (2019) 20 SCC 119	The expression "any property" in Section 102 of the CrPC does not extend to immovable property; the power is bounded by statutory limits and by the duty of immediate reporting to the court.
Neelkanth Pharma Logistics Pvt. Ltd. v. Union of India, 2025 SCC OnLine Del 1055	A lien on the identifiable disputed amount should be the first option rather than a blanket freeze; the Ministry of Home Affairs was directed to frame uniform standard operating procedures.

Table 1: Key judicial precedents on the freezing of bank accounts

B. Protection of Bona Fide Merchants and Third Parties

High Courts have also addressed downstream freezing at Layer 2 and Layer 3. In *Sri Sai Wines v. Union of India*, the High Court of Andhra Pradesh ordered the de-freezing of a vendor's account which had been frozen because a customer who had paid Rs. 1,000 through a UPI application was subsequently implicated in a cheating case registered elsewhere. The Court held that a seller cannot be expected to verify the credentials or criminal antecedents of every customer paying through a UPI application, and that freezing a merchant's account without material showing its involvement in the alleged offence is contrary to law.[23]

[21] *Dr. Sajeer v. Reserve Bank of India*, WP(C) No. 12960 of 2023 (Ker. HC, Oct. 19, 2023) (directing banks to confine freezing orders, in respect of accounts credited through UPI as part of an alleged cyber financial crime, to the amount mentioned in the requisition issued by the police authorities).
[22] *Teesta Atul Setalvad v. State of Gujarat*, (2018) 2 SCC 372 (India).
[23] *Sri Sai Wines v. Union of India*, W.P. No. 969 of 2026 (A.P. HC, June 22, 2026).

The principle that emerges is that funds received by a *bona fide* trader, merchant or service provider in exchange for goods supplied or services rendered cannot automatically be characterised as stolen property or as the proceeds of crime merely because the sender acquired those funds by illicit means. A merchant who accepts payment in good faith and for valuable consideration is a transferee for value, and unless the investigating authority demonstrates *prima facie* collusion, active conspiracy or prior knowledge of the crime, the merchant's account ought not to be subjected to a debit freeze.[24]

C. Judicial Directions on Mandatory Reporting to Magistrates

High Courts have further reiterated that a failure to comply with Section 106(3) of the BNSS, formerly Section 102(3) of the CrPC, which requires the immediate reporting of a freeze to the jurisdictional Magistrate, vitiates the freeze. In *Khalsa Medical Store v. Reserve Bank of India*, a Division Bench of the Allahabad High Court held that a blanket notice to a bank that does not indicate the amount over which a lien is sought is illegal and arbitrary, that a freeze request must be accompanied by the first information report or the information received, and that the investigating officer must intimate the jurisdictional Judicial Magistrate within 24 hours, a failure to do so rendering the action void.[25] The requirement of informing the Magistrate is the essential safeguard that keeps executive action under judicial oversight.

VI. A Reform Framework and Recommendations

To address the difficulties created by automated freezing mechanisms while preserving an effective capacity to investigate cybercrime, systemic procedural and statutory reform is required. The proposed reforms are: a mandatory preliminary inquiry within a 48-hour window; the strict application of lien-marking to the disputed amount alone; time-bound unfreezing with automatic expiry after 30 days; a dedicated merchant dispute redressal portal; and the penalisation of frivolous complaints coupled with a compensation mechanism.

A. Mandatory Preliminary Verification Protocol

Investigating agencies should not issue debit-freeze directions solely on the basis of an unverified automated entry on the NCRP portal. A mandatory preliminary verification process should be established, comprising:

- Time-bound assessment: investigating officers must conduct a preliminary review within 48 hours of a complaint being logged.

[24] *See also Neelkanth Pharma Logistics Pvt. Ltd.*, *supra* note 12.
[25] *Khalsa Medical Store v. Reserve Bank of India*, 2026:AHC-LKO:3701-DB, Writ-C No. 12211 of 2025 (All. HC, Jan. 30, 2026) (Saraf and Shukla, JJ.).

 [ISSN 2581-5369]

- Distinction between civil and criminal claims: officers must review the documentation submitted in order to determine whether the claim stems from a contractual dispute, a delivery issue or a service disagreement before issuing a freeze order.
- Threshold requirements: automated freezes should be restricted to cases involving clear evidence of cyber fraud, such as unauthorised account access, identity theft or deceptive payment gateways.

B. Strict Enforcement of Lien-Marking and Integration with RBI Standard Operating Procedures

Regulatory instruments issued by the Reserve Bank of India (RBI) should expressly mandate lien-marking in preference to total debit freezes:[26]

- Quantified lien orders: police directions to banks must specify the precise amount to be placed on hold.
- Operational account access: banks must be prohibited from freezing account balances beyond the specified disputed sum.
- System automation: banking compliance systems should automatically restrict holds to the disputed sum without requiring manual intervention for every transaction.
- Standard operating procedures: the RBI, in consultation with the Indian Banks' Association and the MHA, should issue binding standard operating procedures for bank compliance desks, mandating that on receipt of an NCRP alert a bank may place a lien only on the flagged amount and must allow normal debit and credit operations on the remaining balance.

C. Time-Bound Unfreezing Protocols and Automatic Expiry

To prevent accounts from remaining frozen indefinitely while an investigation stalls, clear statutory timelines should be introduced:

- The 30-day rule: if no first information report is registered under Section 173 of the BNSS within 30 days of a freeze, or if the complainant fails to furnish supporting evidence, the freeze should expire automatically.[27]

[26] RESERVE BANK OF INDIA (Fraud Risk Management in Commercial Banks (including Regional Rural Banks) and All India Financial Institutions) Directions, 2024, which supersede the RESERVE BANK OF INDIA (Frauds: Classification and Reporting by Commercial Banks and Select FIs) Directions, 2016.

[27] BHARATIYA NAGARIK SURAKSHA SANHITA § 173 (information in cognizable cases).

- NCRP portal integration: the portal should incorporate an automatic unfreezing mechanism that issues directions to the recipient banks where the investigating officer does not periodically extend the freeze with judicial approval.

D. Establishment of a Merchant Dispute Redressal Portal

A dedicated module should be integrated into the NCRP framework to allow an affected account holder to respond:

- Document upload: merchants and service providers should be able to upload relevant documentation, such as invoices, bills of lading, GST receipts and service completion certificates, immediately upon receiving notice of a hold.
- Fast-track review: a specialised administrative unit should review the documents submitted within 72 hours in order to resolve genuine commercial disputes without recourse to formal court proceedings.

E. Penalties for Frivolous Complaints and Statutory Compensation

To prevent the misuse of cyber reporting portals as commercial leverage, strong deterrents are necessary:

- Penal action: a false or misleading complaint on the NCRP portal should attract the express application of Section 217 of the Bharatiya Nyaya Sanhita, 2023, which penalises the furnishing of false information with intent to cause a public servant to use his lawful power to the injury of another person.[28]
- Financial compensation: where an account holder demonstrates that a false complaint was lodged in order to evade a civil obligation, courts and administrative authorities should award costs and compensation payable by the complainant to cover the losses caused by the freeze.

VII. Comparative Analysis: International Practice

A comparison with other legal systems offers useful insight into the balance between financial crime enforcement and procedural protection[29,30,31].

---

[28] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 217 (India).
[29] 18 U.S.C. § 981; Bank Secrecy Act, 31 U.S.C. §§ 5311-5336.
[30] Proceeds of Crime Act 2002, c. 29, §§ 303Z1-303Z3 (UK), inserted by the Criminal Finances Act 2017, c. 22, § 16. An account freezing order is applied for under § 303Z1 and may not be made for a period exceeding two years.
[31] Directive 2014/42/EU of the European Parliament and of the Council of 3 April 2014 on the Freezing and Confiscation of Instrumentalities and Proceeds of Crime in the European Union, 2014 O.J. (L 127) 39, arts. 7-8.

Jurisdiction	Legal framework	Freezing mechanism	Safeguards and rights protection
United States	18 U.S.C. § 981; the Bank Secrecy Act	Seizure orders require a judicial warrant founded on probable cause; the Financial Crimes Enforcement Network uses targeted holds.	*Ex parte* freezes require prompt post-seizure hearings within short statutory deadlines, with full due process protections.
United Kingdom	Proceeds of Crime Act 2002; Criminal Finances Act 2017	An account freezing order is made by a magistrates' court on the application of a senior officer.	Judicial approval is required before any prolonged freeze; the order may not exceed two years and exclusions for living expenses are available.
European Union	Directive 2014/42/EU on the freezing and confiscation of instrumentalities and proceeds of crime	Standardised procedures across Member States for the execution of freezing orders.	An effective remedy, prompt communication of the order with reasons, and an effective opportunity to challenge it.
India (proposed reform model)	Section 106 of the BNSS read with reformed NCRP guidelines	Automated alerts replaced by mandatory lien-marking with reporting to the Magistrate.	Mandatory preliminary inquiry, lien-marking, automatic unfreezing and a dispute redressal portal.

Table 2: Comparative frameworks governing the freezing of funds held in bank accounts

VIII. Conclusion

The establishment of the National Cyber Crime Reporting Portal and the 1930 emergency helpline represents an important step in India's effort to combat online financial crime. In an era of rapid digital transactions, the ability to trace and intercept the proceeds of crime in real time is essential to maintaining public trust in the financial system.

The current operational model, however, characterised by automated freeze alerts, blanket account blocks and the extension of freezing to Layer 2 and Layer 3 accounts, creates substantial procedural difficulty. The absence of preliminary verification has enabled bad-faith actors to weaponise cybercrime portals in order to settle civil commercial disputes, imposing significant financial strain on *bona fide* merchants, logistics providers and ordinary citizens.

These practices raise serious constitutional concerns under Articles 14, 19(1)(g) and 21 of the Constitution of India, as well as under the core principles of natural justice. Depriving individuals and businesses of their financial resources without notice, without an opportunity to be heard and without any proportionality check is inconsistent with the standards of procedural fairness that the courts have repeatedly affirmed.

Addressing these difficulties does not require dismantling the cybercrime reporting machinery. It requires structured administrative safeguards. By introducing a mandatory preliminary inquiry, enforcing lien-marking limited to the disputed amount, implementing time-bound automatic unfreezing, establishing a dedicated merchant redressal module and penalising false complaints, India can build a balanced cyber jurisprudence that keeps law enforcement effective while safeguarding fundamental rights and the economic activity on which the digital economy depends.

*****