FREEZING OF BANK ACCOUNTS IN THE DIGITAL ERA: CONSTITUTIONAL CONCERNS AND THE NEED FOR PROCEDURAL SAFEGUARDS

Aadi Bodh Pushkale*

ABSTRACT

The automated architecture built to combat online financial fraud in India has, in the last three years, become one of the most common sources of grievance against the administration of criminal justice. Every complaint filed on the National Cyber Crime Reporting Portal triggers a mechanical trace of the underlying transaction chain, and every account through which even a fraction of the disputed sum passed is liable to be frozen, irrespective of the remoteness of the individual to the alleged action. This article examines the statutory foundation of this power under Section 106 of the Bharatiya Nagarik Suraksha Sanhita 2023 and its predecessor, Section 102 of the Code of Criminal Procedure 1973, and traces the doctrinal distinction, now firmly established by the High Courts, distinguishing executive seizures executed pursuant to Section 106 from the formal judicial attachments ordered under Section 107. It argues that blanket, indefinite and unreported freezing of entire accounts is difficult to reconcile with Article 300A, Article 21 and Article 19(1)(g) of the Constitution. Surveying the rapid judicial development between 2024 and 2026, from the Supreme Court's ruling in Shento Varghese to the Bombay High Court's decisive intervention in Kartik Yogeshwar Chatur, the article demonstrates the emergence of a judicial consensus around proportionality, mandatory magisterial oversight and timely notice. It concludes by arguing that the pending petition in Vivek Varshney v Union of India, together with the Ministry of Home Affairs' 2026 Standard Operating Procedure, presents a rare opportunity to convert scattered judicial correctives into a uniform, codified framework that protects both the integrity of criminal investigation and the economic dignity of the citizen.

*BA LLB, FIRST YEAR, OP JINDAL GLOBAL UNIVERSITY, SONIPAT.

Keywords: Bank Account Freezing, Cybercrime Investigation, Proportionality, National Cyber Crime Reporting Portal, Right to Livelihood.

INTRODUCTION

Imagine waking up to find that every bank account in your name has stopped working overnight. Rent cannot be paid, tuition fees lapse, salaries owed to employees cannot be released, and a debit card is declined at a pharmacy counter not because of any wrongdoing, but because a small, legitimate payment received days or weeks earlier happened to sit somewhere along a digital money trail that a cyber cell, in some other state, is investigating.

This is no longer a hypothetical. It is an increasingly ordinary experience for account holders across India. The mechanism built to combat online financial fraud: automated, high-volume, and almost entirely executed through emails and portal-generated notices from state cyber cells to banks has produced a pattern of collateral damage that is, by now, well documented in the law reports: street vendors whose entire savings are frozen over amounts as small as ₹105 or ₹200; gold retailers unable to disburse salaries because a customer, several transactions removed, later became a suspect; and companies holding balances in the tens of crores rendered unable to operate because of a single incidental credit.[1]

Law enforcement undoubtedly has a legitimate interest in preserving suspected proceeds of crime while an investigation is pending. But the manner in which that interest has been pursued through blanket freezing orders issued without magisterial oversight, without written reasons, and often without any communication to the account holder at all has increasingly come into conflict with basic constitutional guarantees. Between 2024 and 2026, the Supreme Court and at least five High Courts have been called upon to draw the line between legitimate investigative caution and arbitrary deprivation of property. This article traces that development, situates it within the constitutional text, and argues for a codified, proportionate and time-bound framework going forward.

The scale of the problem is a direct function of the design of India's cybercrime reporting infrastructure. Because that infrastructure is centralised, automated and national in reach, a single fraud complaint can generate freeze instructions to dozens of accounts across several states within hours, long before any human officer has examined whether a particular recipient

[1] See Part VI below, discussing inter alia *Pawan Kumar Rai v Union of India* 2024 SCC OnLine Del 8936 and *Neelkanth Pharma Logistics (P) Ltd v Union of India* 2025 SCC OnLine Del 1055.

had any knowledge of, or connection to, the underlying offence. The resulting grievances are not isolated or anecdotal: they recur with sufficient regularity, and in sufficiently similar factual patterns, a small, incidental credit followed by the freezing of an entire account, sometimes worth many multiples of the disputed sum, that at least six High Courts in addition to the Supreme Court themselves have remarked is mandatory to intervene in a period of two years. This article proceeds in several movements: it first sets out the statutory architecture governing seizure and, more recently, attachment of bank accounts; it then situates that architecture within the constitutional guarantees it most directly implicates; it surveys, chronologically, the resulting body of case law; it draws a brief comparison with an analogous regime in English law; and it concludes with a set of concrete recommendations for reform.

THE STATUTORY BASIS OF BANK ACCOUNT FREEZES

The power of the police to interfere with a bank account has always rested on the general power of seizure, not on any provision drafted specifically with digital banking in mind. Under the Code of Criminal Procedure 1973, that power was found in Section 102, which allows any police officer the right to confiscate properties believed to be involved with the alleged or believed to be stolen, or found under circumstances creating suspicion of the commission of an offence.[2] "With effect from 1 July 2024, the CrPC was replaced by the Bharatiya Nagarik Suraksha Sanhita 2023 (BNSS), and the equivalent power now appears, in materially identical language, in Section 106."[3]

Neither provision was drafted with bank accounts in mind, and neither uses the word "freeze". It was left to judicial interpretation to determine whether a bank account could be "property" for this power at all. The Supreme Court answered that question in 1999, in *State of Maharashtra v Tapas D Neogy*, holding that the term "any property" in Section 102(1) was wide enough to include a bank account, so long as a direct link could be shown between the account and the alleged offence.[4] That ruling remains good law and now applies equally to Section 106 of the BNSS.

What is often overlooked, however, is the safeguard built into the very same provision. Sub-section (3) requires that every seizure be reported "forthwith" to the jurisdictional Magistrate,

[2] Code of Criminal Procedure 1973, s 102(1)
[3] Bharatiya Nagarik Suraksha Sanhita 2023, s 106(1)
[4] *State of Maharashtra v Tapas D Neogy* (1999) 7 SCC 685

who then assumes supervisory control over the property.[5] The seizure contemplated by the provision is, on its face, an interim, exploratory mechanism designed to keep evidence safe, not a mechanism of indefinite financial punishment. In practice, this reporting requirement has been observed more often in the breach than in compliance, and it is this gap between statutory design and administrative practice that has generated the bulk of recent litigation.

SEIZURE AND ATTACHMENT: A CRITICAL DISTINCTION

A doctrinal development of particular significance in this area is the judicial recognition that Section 106 BNSS and Section 107 BNSS perform two entirely different functions, and that police and banks have, for several years, been conflating the two. Section 106 empowers a police officer to seize property by an executive, investigative act, immediately reportable to the Magistrate. Section 107, by contrast, is a new provision, without a direct predecessor in the CrPC outside limited contexts, which vests in the Magistrate alone the power to order attachment of property connected to criminal activity.

The Kerala High Court was among the first to draw this distinction out clearly, holding in *Headstar Global (P) Ltd v State of Kerala* that the introduction of Section 107 filled a gap that previously did not exist in the CrPC, and that an investigating agency cannot bypass the Magistrate's attachment jurisdiction by dressing up what is, in substance, an attachment as a mere “seizure” under Section 106.[6] The Bombay High Court, sitting at Nagpur, went further in *Kartik Yogeshwar Chatur v Union of India*, holding in the most comprehensive ruling on the point to date that the investigating party does not posess the right to impose debit freeze on a bank account under Section 106 BNSS; such a freeze, which strips the account holder of any access to their own funds, is functionally an attachment and can only be ordered by a Magistrate exercising the power conferred by Section 107. Banks and other intermediaries, the Bombay High Court held, are at most empowered to mark a lien over the specific disputed sum, not to disable the account in its entirety.[7]

This is not a mere technicality. The difference between a lien on a disputed sum and a complete debit freeze is, in practical terms, the difference between an account holder continuing to pay rent and salaries while an investigation proceeds, and an account holder facing complete economic paralysis for months while a Magistrate's file gathers dust. The seizure–attachment

[5] Bharatiya Nagarik Suraksha Sanhita 2023, s 106(3).
[6] *Headstar Global (P) Ltd v State of Kerala* 2025 SCC OnLine Ker 3546.
[7] *Kartik Yogeshwar Chatur v Union of India* 2025 SCC OnLine Bom 4778.

distinction therefore operationalises, at the level of ordinary statutory interpretation, the constitutional concerns discussed in Part V below.

THE DIGITAL FRAUD INVESTIGATION MECHANISM

The scale of the present problem cannot be understood without appreciating how digital fraud investigation actually works. Every complaint filed on the National Cyber Crime Reporting Portal (NCCRP) triggers an automated process that traces the flow of the disputed funds across the banking system, from the account originally debited by the victim to every subsequent account to which any part of that sum was transferred. Because fraudsters typically move stolen money rapidly across multiple accounts, often within minutes, using layering techniques designed to defeat precisely this kind of tracing, the freeze notices generated by the portal tend to cascade well beyond the original suspect, reaching second, third and fourth-degree recipients who had no reason to suspect that the funds they received were tainted.

The consequence is that freelancers paid for legitimate work, small retailers who accepted a card payment, peer-to-peer traders, and even large companies that sold goods on ordinary commercial terms have found themselves receiving communications, sometimes no more than an email or a telephone call to their bank, without any written order at all informing them, after the fact, that their account has been frozen. In several of the cases discussed in Part VI, the sum actually connected to the alleged offence was a trivial fraction of the account balance frozen: ₹200 out of more than ₹93 crore in one case, and ₹105 in another.

First, because freeze notices are often issued directly by banks acting on cyber cell communications rather than through a formal written seizure order, there is frequently no compliance at all with the Section 106(3) requirement of reporting to the jurisdictional Magistrate, leaving the account holder with no forum to approach for months. Second, because cybercrime complaints frequently name multiple, geographically dispersed cyber cells as sources of a freeze instruction, a single account can be the subject of several overlapping and uncoordinated freeze directions from different states, each of which must be separately resolved before the account is restored to full operation.

CONSTITUTIONAL CONCERNS

Article 300A and the Right Against Arbitrary Deprivation of Property: Article 300A of the Constitution states that no property shall be taken from individuals save by authority of law.[8] Although the property right ceased to be a fundamental right after the Forty-Fourth Amendment, the Supreme Court has on multiple occasions emphasised that Article 300A continues to guarantee a constitutional as opposed to merely statutory protection against arbitrary executive action, and that any deprivation and confiscation of property must be authorised by a validly enacted law, applied through a fair procedure.[9] A bank balance is unambiguously "property" within the meaning of this guarantee. Where an account is frozen without a formal order, without magisterial oversight, and without any temporal limit, the deprivation in question is difficult to characterize as one occurring "by authority of law" in the sense Article 300A requires; it more closely resembles action by executive fiat, restrained only by the eventual willingness of a High Court to intervene under Article 226.

Article 21 and the Right to Livelihood: The Supreme Court has long recognised that the right to life under Article 21 is not confined to physical survival but extends to the means necessary to live with dignity, including the right to livelihood.[10] In *Maneka Gandhi v Union of India*, the Court held that any procedure depriving a person of a right under Article 21 must be fair, just and reasonable, and not arbitrary or oppressive.[11] A complete freeze of every account held by an individual or a business, cutting off the ability to pay rent, wages, school fees or medical expenses, is a form of economic paralysis that strikes directly at this constitutional guarantee, particularly where the freeze is imposed without notice, without a hearing, and without any indication of when it might be lifted. Courts confronting these facts have not hesitated to describe a bank account as the essential mechanism through which a person's economic existence in a digitised economy is sustained, and have treated indefinite, unexplained freezing as inconsistent with the demands of Article 21.

Article 19(1)(g) and the Freedom to Carry on Trade or Business: For proprietorships, partnerships and companies, an operative bank account is not merely convenient but indispensable to the freedom to carry on any trade, business or profession guaranteed under Article 19(1)(g). The Supreme Court has recognised, in the context of banking access more generally, that in an economy where cash transactions are increasingly restricted, banking channels function as the lifeline of trade and commerce, and that depriving an entity of the ability to operate its account effectively shuts down its business, placing the burden squarely

[8] Constitution of India, art 300A.
[9] *K T Plantation (P) Ltd v State of Karnataka* (2011) 9 SCC 1.
[10] Constitution of India, art 21; *Olga Tellis v Bombay Municipal Corporation* (1985) 3 SCC 545.
[11] *Maneka Gandhi v Union of India* (1978) 1 SCC 248.

on the state to justify such a restriction as reasonable and proportionate.[12] Where an entire corporate account is frozen on account of a single incidental transaction with no allegation of complicity against the company itself, the restriction is difficult to defend as a reasonable restriction within the meaning of Article 19(6).

THE JUDICIAL RESPONSE: A CHRONOLOGICAL SURVEY (2024–2026)

The period between 2024 and 2026 has produced a remarkably consistent, if incrementally developed, body of case law addressing these concerns.

Shento Varghese v Julfikar Husen: The starting point is the Supreme Court's ruling clarifying the meaning of the word “forthwith” in the reporting requirement under Section 102(3) CrPC (now Section 106(3) BNSS). The Madras High Court had earlier held that any delay in reporting a seizure to the Magistrate automatically vitiated the seizure itself. The Supreme Court disagreed, holding that “forthwith” means with reasonable promptness and without unnecessary delay, not literal instantaneity, and that a delayed report is a curable irregularity rather than a ground to nullify the seizure outright. At the same time, the Court made clear that unexplained or deliberate delay is not without consequence: the Magistrate, on receiving a late report, must examine the reasons for the delay and may direct departmental action against an erring officer. Critically, the Court reaffirmed that the precondition for the exercise of the seizure power in the first place is a direct link between the property and the alleged offence, and that the absence of such a link remains a valid ground of challenge.[13]

Pawan Kumar Rai v Union of India: This case became something of a symbol for the disproportion inherent in the automated freezing pipeline. The petitioner, a street vendor selling snacks for a living, had his entire account frozen because ₹105 traceable to an alleged fraud chain had passed through it; he was neither an accused nor a suspect in any investigation. The Delhi High Court ordered the account defrozen, holding that freezing without compliance with the mandatory reporting requirement under Section 106(3) could not be sustained, and that innocent account holders cannot be financially crippled merely because of incidental, downstream credits. The Court expressly linked its reasoning to the fundamental right to livelihood under Article 21.[14]

---

[12] *Internet and Mobile Association of India v Reserve Bank of India* (2020) 10 SCC 274.
[13] *Shento Varghese v Julfikar Husen* 2024 SCC OnLine SC 895.
[14] *Pawan Kumar Rai v Union of India* 2024 SCC OnLine Del 8936.

Mohammed Saifullah v Reserve Bank of India: Here, a bank had frozen the petitioner's entire account with a balance exceeding ₹9.69 lakh on the strength of an informal communication from an out-of-state cybercrime bureau, without any written order and without any judicial sanction, even though only around ₹2.48 lakh was said to be linked to the alleged offence. The Madras High Court held that a bank cannot act on a verbal or email communication from the police; a lawful written order is a precondition. It further held that any restriction must be proportionate: only the specific disputed sum may be placed under lien, and the remainder of the balance must remain accessible to the account holder.[15]

Headstar Global (P) Ltd v State of Kerala: Discussed above in Part III, this decision crystallised the distinction between Section 106 seizure and Section 107 attachment, holding that the introduction of a dedicated attachment provision in the BNSS means that a debit freeze can no longer be sustained on the strength of Section 106 alone.[16]

Abdul Basith v Cyber, Economic and Narcotic Crime: Building on the proportionality principle first articulated in *Mohammed Saifullah*, the Kerala High Court quashed a freeze order to the extent that it extended beyond the ₹43,000 actually connected to the alleged offence, holding that an investigating agency cannot suspend access to an entire account merely because a fraction of its balance is under suspicion.[17]

Neelkanth Pharma Logistics (P) Ltd v Union of India: In perhaps the most striking illustration of disproportion in this entire line of cases, a company holding a balance in excess of ₹93.5 crore had its account frozen by its bank on the strength of a police direction concerning a credit of ₹200. Although the petition was ultimately disposed of as withdrawn after the investigating agency itself directed that the debit freeze be lifted (retaining only a lien over the ₹200 in question), the Delhi High Court made pointed observations about the recurring pattern of blanket freezing based on trivial or uncertain links to an alleged offence, and directed that a copy of its order be forwarded to the Ministry of Home Affairs, recommending the development of a uniform, nationally applicable policy and standard operating procedure in consultation with the states and union territories.[18]

---

[15] *Mohammed Saifullah v Reserve Bank of India* 2024 SCC OnLine Mad 5604.
[16] *Headstar Global* (n 6).
[17] *Abdul Basith v Cyber, Economic and Narcotic Crime* 2025 SCC OnLine Ker 83.
[18] *Neelkanth Pharma Logistics (P) Ltd v Union of India* 2025 SCC OnLine Del 1055.

Kartik Yogeshwar Chatur v Union of India: As discussed in Part III, this is the most comprehensive statement yet on the seizure–attachment distinction, holding definitively that an investigating agency has no power under Section 106 BNSS to impose a debit freeze, and that banks may, absent a Magistrate's attachment order, do no more than mark a lien on the disputed amount. The Court quashed the debit-freeze orders under challenge and permitted the affected petitioners to pursue compensation for wrongful freezing.

Malabar Gold and Diamond Ltd v Union of India: A jewellery retailer that had sold goods worth approximately ₹14.2 crore to a customer subsequently accused of cybercrime, with no FIR or allegation against the retailer itself, found more than ₹80 lakh across two of its accounts frozen, disrupting its ability to pay salaries and meet ordinary business expenses. The Delhi High Court concluded that freezing of an account without any allegation of complicity, without a Magistrate's order, and without demonstrating a nexus between the account holder and the offence under investigation was unjustified and unlawful, and directed immediate defreezing, while leaving it open to the investigating agency to proceed against the company if genuine material of complicity later emerged.[19]

Dekain Perfect Tech Ksolution (P) Ltd v IDFC First Bank: Following its own earlier ruling in *Malcolm Murayis v State Bank of India*, the Madhya Pradesh High Court directed the bank to unfreeze the petitioner company's account, while protecting the sum actually in dispute by directing that it be placed in a separate fixed deposit, to be liquidated only once the jurisdictional Magistrate finally decided the underlying question of alleged cyber fraud. The Court was critical of what it described as the poor functioning and irresponsible approach of the cyber cells whose communications had triggered the freeze in the first place, and gave the Magistrate a three-month timeline within which to resolve the matter.[20]

International School Bangalore v Standard Chartered Bank: Most recently, the Karnataka High Court held that freezing an educational institution's entire account merely because it had received a fee payment from a parent later implicated in a cybercrime investigation was arbitrary and disproportionate, directing that only a lien to the extent of the specific disputed

[19] *Malabar Gold and Diamond Ltd v Union of India* 2026 SCC OnLine Del 297.
[20] *Dekain Perfect Tech Ksolution (P) Ltd v IDFC First Bank* 2026 SCC OnLine MP 17717; *Malcolm Murayis v State Bank of India* (MP HC, April 2024).

sum be marked, and emphasising that a bank functions merely as a custodian of an account, not as an extension of the investigating agency's enforcement machinery.[21]

Read together, these decisions disclose a clear and converging judicial position: seizure under Section 106 BNSS is a legitimate but narrow and temporary investigative tool, contingent on a demonstrable nexus between the account and the alleged offence; a full debit freeze is, in substance, an attachment that requires a Magistrate's order under Section 107; any restriction that is imposed must be proportionate to the sum genuinely in dispute; and the convenience of investigation cannot be allowed to override the constitutional protections examined in Part V.

THE NEED FOR UNIFORM NATIONAL GUIDELINES

The volume and geographic spread of this litigation spanning the Delhi, Bombay, Madras, Kerala, Madhya Pradesh and Karnataka High Courts within roughly two years, is itself evidence that the problem cannot be resolved through case-by-case adjudication alone. That recognition has now reached the Supreme Court. In January 2026, the Court issued notice in a writ petition filed under Article 32 by Vivek Varshney and another petitioner, whose bank accounts had been frozen by a state cyber cell without any prior notice, communication, or judicial approval. The petition seeks, among other reliefs, a direction to the Union of India and the Reserve Bank of India to frame a uniform, nationwide protocol regulating bank account restrictions within digital fraud probes. This includes mandates stipulating that any block necessitates a justified, written directive, alongside mandatory notification to the affected party within a fixed period and mandatory, prompt reporting to the jurisdictional Magistrate. The petition was subsequently found to overlap with a related suo motu proceeding before the Court concerning procedural safeguards in cybercrime investigations, and has accordingly been placed before the Chief Justice of India for further directions.[22]

In parallel, the Ministry of Home Affairs introduced an administrative framework in early 2026 targeting digital financial freezes. This protocol prioritises balanced enforcement by restricting only the specific contested funds, an ultimate remedy, establishing rigid review schedules and formalising an account holder’s right to natural justice, and recognises the account holder's

---

[21] *International School Bangalore v Standard Chartered Bank*, Writ Petition No. 9430 of 2026 (GM-Police) (Karnataka HC, 27 March 2026).
[22] *Vivek Varshney v Union of India* Writ Petition (Civil) (SC, notice issued 6 January 2026).

right to be heard.[23] Whether this administrative instrument achieves compliance in practice, given the same enforcement gaps that produced the litigation discussed above, remains to be seen; but its existence, together with the pending Supreme Court petition, marks the first genuine attempt at a coordinated, rather than piecemeal, response to a problem that judicial review alone has proved ill-suited to resolve at scale.

A COMPARATIVE NOTE: THE ENGLISH ACCOUNT FREEZING ORDER

Chapter 3B of Part 5 of the Proceeds of Crime Act 2002 institutionalised a specific framework for freezing orders. Under these provisions, should an investigator surmise that an account balance constitutes illicit proceeds or is earmarked for criminal enterprises, a formal petition must be presented before a magistrates' court. Consequently, administrative directives to financial intermediaries are insufficient: explicit judicial concurrence regarding the underlying suspicion is mandatory. [24] The order is, moreover, subject to a statutory outer limit: it may not, even on repeated extension, remain in force for more than two years from the date it was first made, and the enforcement authority must return to court at intervals to justify its continuation.[25] The Act further provides an express statutory right to compensation where an account freezing order is discharged, and the court is satisfied that the applicant authority acted improperly in seeking it.[26]

The contrast with the position that has prevailed in India is instructive. Under the English scheme, prior judicial authorisation is a precondition of the freeze itself, not merely a safeguard triggered after the fact by a reporting obligation that is honoured inconsistently; the freeze is inherently time-limited by statute rather than continuing indefinitely until a Magistrate happens to take up the file; and an account holder whose account was frozen without proper justification has a defined statutory remedy in damages, rather than having to rely on the residual, discretionary power of a High Court under Article 226 to award compensation. None of this is to suggest that the English model should be transplanted wholesale; the institutional capacity of magistrates' courts, the volume of cybercrime complaints, and the realities of Indian criminal procedure are all materially different. But the structural features of the English scheme prior judicial sanction, a statutory cap on duration, and a built-in compensation mechanism map

[23] Ministry of Home Affairs, 'Standard Operating Procedure on Freezing and De-Freezing of Bank Accounts in Cybercrime Cases' (January 2026)
[24] Proceeds of Crime Act 2002, s 303Z1
[25] Proceeds of Crime Act 2002, s 303Z3(4)
[26] Proceeds of Crime Act 2002, s 303Z18

closely onto precisely the three gaps that Indian courts have, case by case, been attempting to close through interpretation of Sections 106 and 107 of the BNSS. A legislative or SOP-based framework that borrowed these three structural features would go a considerable distance toward converting today's ad hoc judicial correctives into a stable, predictable system.

TOWARDS A BALANCED FRAMEWORK

The case law surveyed in Part VI, read alongside the constitutional concerns in Part V, points toward the essential elements of a workable framework, one that protects the legitimate investigative interest in preserving suspected proceeds of crime without converting that interest into a tool of indiscriminate financial punishment.

First, any restriction on a bank account should, as a default rule, take the form of a lien confined to the specific sum genuinely traceable to the alleged offence, rather than a blanket freeze of the entire balance. A complete debit freeze should be treated as an exceptional measure, available only where a demonstrable and specific risk to the remainder of the funds can be shown, and even then, only pursuant to a Magistrate's order under Section 107 BNSS rather than a unilateral police communication under Section 106.

Second, compliance with the reporting obligation under Section 106(3) should be treated as a genuine, monitored requirement rather than a formality honoured in the breach. A workable framework would require banks to record, and be able to produce on demand, the written order and the date on which it was reported to the jurisdictional Magistrate, with clear departmental consequences, and where appropriate, compensatory for non-compliance.

Third, account holders should receive prompt written notice of any freeze, including the identity of the investigating authority, the specific sum in question, and the procedure for seeking review, rather than learning of the restriction only when a transaction is declined.

Fourth, given that a single account can be the subject of multiple, uncoordinated freeze directions from different states in relation to a single underlying fraud chain, there is a strong case for a centralised, portal-based mechanism through which banks and cyber cells across jurisdictions can coordinate and consolidate freeze instructions relating to the same account, rather than requiring an account holder to separately litigate or negotiate with each originating cyber cell.

Finally, defined timelines for magisterial review of the kind directed in *Dekain Perfect Tech Ksolution*, where a three-month outer limit was set, and reinforced by the statutory two-year outer cap found in the English account freezing order regime discussed above, should be built into the standard operating procedure itself, rather than left to the discretion of individual courts on a case-by-case basis.

None of these five elements is, individually, a novel proposition; each has already been articulated, in one form or another, by a High Court confronting a particular set of facts. What is missing is not judicial insight but legislative or executive consolidation into a single, binding instrument that applies these principles uniformly across states and cyber cells, rather than requiring each aggrieved account holder to independently litigate the same set of arguments before a different High Court.

CONCLUSION

The digital financial ecosystem cannot function under conditions of continuous legal uncertainty in which innocent citizens face economic paralysis as a side effect of automation. The need to combat cybercrime is a legitimate and pressing public interest, but the current practice of automatic, disproportionate account freezing under Section 106 of the BNSS has, in a significant number of documented cases, moved well beyond legitimate investigative caution into what several High Courts have not hesitated to describe as arbitrary deprivation of property.

The convergence of judicial opinion across the Supreme Court and at least five High Courts between 2024 and 2026, on the seizure–attachment distinction, on the requirement of proportionality, and on the primacy of magisterial oversight represents a significant corrective moment for Indian banking and criminal procedure law. What remains is to translate that judicial consensus into codified, uniformly enforced practice. The pending petition in *Vivek Varshney v Union of India*, read together with the Ministry of Home Affairs' 2026 Standard Operating Procedure, offers a genuine opportunity to do so: to require immediate liens confined to the disputed amount, to impose clear and enforceable notification timelines on investigating agencies and banks alike, and to provide affected account holders with a straightforward and rapid avenue for relief.

A financial system that allows the state to preserve the proceeds of crime while protecting the economic dignity of the ordinary citizen is not a contradiction in terms; it is simply a matter of designing the mechanism correctly. Until that design work is completed and enforced, the burden of an automated, blunt-edged system will continue to fall disproportionately on the very citizens, such as street vendors, freelancers, small businesses and salaried employees, who are least equipped to bear it.