# ABUSE OF THE CYBER CELL PORTAL: A GROWING THREAT TO JUSTICE AND DUE PROCESS

Owaiz Ahmed Khan Shirani & Thridev Prince, B.Com LL.B., St, Joseph's College of Law, Bangalore

## ABSTRACT

The rapid digitalization of the Indian economy, characterized by the meteoric rise of the Unified Payments Interface (UPI) and the expansion of digital banking, has fundamentally altered the landscape of criminal activity. As financial transactions migrated to the digital sphere, so too did the mechanisms of fraud, prompting the Government of India to establish a robust defensive infrastructure. Central to this defensive posture is the National Cyber Crime Reporting Portal (NCRP), managed by the Indian Cybercrime Coordination Centre (I4C) under the Ministry of Home Affairs. While the portal was envisioned as a sanctuary for victims of digital predation, its operational implementation has increasingly diverged from the established tenets of due process and natural justice. The systemic prioritization of speed in fund recovery has inadvertently created a framework ripe for exploitation, where the state's coercive powers, specifically the ability to freeze bank accounts[1], are being weaponized by individuals to settle personal vendettas, civil disputes, and matrimonial conflicts[2]. The Cyber Cell Portal was established as a crucial mechanism to provide swift redressal for cyber-related offences and to enhance access to justice in the digital era. Designed to assist victims of online fraud, harassment, identity theft, and other cybercrimes, the portal aims to ensure efficiency, transparency, and timely intervention by law enforcement agencies. However, in recent years, the increasing misuse of the Cyber Cell Portal has emerged as a significant concern, posing a serious threat to justice and due process.

This paper critically examines how false, exaggerated, or malicious complaints are being filed through the portal to harass individuals, settle personal disputes, or exert undue pressure, often without adequate preliminary verification. Such abuse not only undermines the credibility of genuine cybercrime victims but also results in unwarranted investigations,

[1] https://lawbeat.in/top-stories/account-frozen-without-notice-plea-in-supreme-court-seeks-nationwide-sop-on-cyber-cell-bank-freezes-1553709

[2] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2

reputational damage, and violation of fundamental rights of the accused, including the right to fair procedure and natural justice. The absence of stringent safeguards, accountability mechanisms, and penalties for false reporting further exacerbates the problem.

The study highlights the legal, social, and procedural consequences of this misuse and emphasizes the urgent need for reforms. It advocates for balanced safeguards that protect genuine complainants while preventing the weaponization of cyber law enforcement tools, thereby preserving the integrity of the justice system.

## INTRODUCTION

### 1. What is a Cyber Crime?

Cybercrime refers to any unlawful activity committed using computers, digital devices, or the internet, where technology is either the primary tool, the target, or both. With the rapid expansion of digital connectivity, cybercrime has evolved into a complex and pervasive threat affecting individuals, organizations, and governments worldwide. These offences include a wide range of illegal acts such as hacking, identity theft, online fraud, phishing, cyber stalking, data breaches, ransomware attacks, dissemination of malware, online defamation, and financial scams. Cybercrimes may be directed against individuals to steal personal information or cause psychological harm, against businesses to gain unauthorized access to confidential data or disrupt operations, or against governments to compromise national security and critical infrastructure.

One of the defining characteristics of cybercrime is the anonymity it offers to offenders, enabling them to operate across geographical boundaries with minimal risk of immediate detection. The borderless nature of the internet complicates investigation and prosecution, as cyber criminals often exploit jurisdictional loopholes and technological sophistication. Moreover, the rapid advancement of technology has given rise to new forms of cybercrime, including crimes involving artificial intelligence, cryptocurrency fraud, and dark web activities. The impact of cybercrime extends beyond financial losses, affecting privacy, reputation, mental well-being, and public trust in digital systems. Consequently, cybercrime poses a significant challenge to legal frameworks and law enforcement agencies, necessitating robust cyber laws, technological expertise, international cooperation, and public awareness to effectively prevent, detect, and address such offences in the digital age.

Cybercrimes in India are governed primarily by the Information Technology Act, 2000**,** which specifically addresses offences committed through electronic means, and are supplemented by the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaces the Indian Penal Code and provides general criminal liability applicable to cyber-related offences.

The Information Technology Act, 2000, lays down the core framework for cyber offences. Section 43 provides for civil liability in cases of unauthorized access, data theft, damage to computer systems, or introduction of malware. Section 65 criminalizes tampering with computer source documents, while Section 66 prescribes punishment for computer-related offences involving dishonest or fraudulent intent. Sections 66B, 66C, and 66D deal with offences such as receiving stolen computer resources, identity theft, and cheating by personation using computer resources respectively. Section 66E safeguards individual privacy by penalizing the capturing or transmission of private images without consent. Sections 67, 67A, and 67B prohibit the publication or transmission of obscene content, sexually explicit material, and child sexual abuse material in electronic form.

In addition to the IT Act, the Bharatiya Nyaya Sanhita, 2023, applies to cybercrimes where digital means are used to commit conventional offences. Provisions relating to cheating, criminal intimidation, defamation, forgery, stalking, sexual harassment, and threats under the BNS are invoked when such acts are carried out through electronic platforms. The BNS thus ensures that offences committed in cyberspace are punished on par with their physical-world counterparts.

Together, the IT Act, 2000, and the Bharatiya Nyaya Sanhita, 2023, form a comprehensive legal framework to address cybercrime, ensure digital security, and uphold justice in the rapidly evolving technological landscape.

The National Cyber Crime Reporting Portal (https://cybercrime.gov.in) serves as the primary intake point for citizens to report a spectrum of digital offenses, ranging from financial fraud to crimes against women and children. Launched to empower victims who might otherwise be deterred by the complexities of traditional police stations, the portal facilitates a streamlined reporting process that bypasses initial jurisdictional hurdles. Supporting this portal is the national helpline number 1930, which operates as part of the Citizen Financial Cyber Fraud Reporting and Management System (CFCFRMS).

The operational efficiency of the system is predicated on the "Golden Hour" principle, the immediate period following a fraud when funds remain within the domestic banking system and are susceptible to interception. To maximize the probability of recovery, the I4C has integrated the NCRP with the banking sector and payment gateways, enabling the instantaneous issuance of "debit freeze" or "lien" instructions once a transaction is flagged. However, this focus on velocity has come at the expense of verification. The portal allows users to register complaints by providing basic incident details, bank transaction IDs, and national ID proofs, which are then used to trigger account freezes across multiple layers of the banking chain.

The statistical successes of this framework are undeniable. By 2024, the I4C reported that over ₹4,386 crore had been saved in more than 13.36 lakh complaints[3]. As of early 2025, over 9.42 lakh SIM cards and 2.63 lakh IMEI numbers linked to fraudulent activities had been blocked. Yet, these numbers tell only half the story. The very mechanism that saves thousands of crores also facilitates the freezing of legitimate funds, often involving amounts that bear no rational proportion to the alleged crime.

The Cyber Cell Portal was introduced as a progressive initiative to facilitate the reporting of cyber offences and to provide swift access to law enforcement authorities in an increasingly digital society. Its primary objective is to protect victims of cyber fraud, online harassment, identity theft, and other technology-enabled crimes by enabling quick registration of complaints and prompt investigation. However, the ease of access and minimal preliminary scrutiny associated with the portal have led to its increasing misuse, thereby undermining the principles of justice and due process.

One of the most concerning forms of abuse involves the filing of false, exaggerated, or malicious complaints to harass individuals, settle personal vendettas, or exert pressure in civil, matrimonial, or commercial disputes. In many cases, complaints are registered without adequate verification of facts, resulting in the initiation of coercive investigative measures such as repeated summons, device seizure, account freezing, and informal intimidation. These actions often occur even before any prima facie evidence of a cyber-offence is established, causing irreparable harm to the reputation, mental health, and professional standing of the

[3] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112244&reg=3&lang=2

accused.

## 2. The Legal Landscape and the Power to Freeze

The authority to freeze bank accounts in the context of cybercrime is primarily derived from Section 102 of the Code of Criminal Procedure (CrPC), which has been superseded by Section 106 of the Bharatiya Nagarik Suraksha Sanhita (BNSS). These provisions empower police officers to seize any property that is suspected of being stolen or linked to an offense. In the landmark case of *State of Maharashtra v. Tapas D. Neogy*[4], the judiciary definitively held that a bank account constitutes "property" under this section, thereby permitting investigating agencies to issue "debit freeze" instructions to banks during an investigation.

The Information Technology (IT) Act, 2000, provides the substantive framework for defining cyber offenses. Sections 66, 66C (identity theft), and 66D (cheating by personation) are the most frequently invoked provisions in financial fraud cases. Furthermore, the Bharatiya Nyaya Sanhita (BNS) modernizes these offenses, incorporating provisions against organized crime and the misuse of electronic modes.

However, the procedural application of these laws reveals a significant due process deficit. Under Section 102(3) of the CrPC (now BNSS 106(3)), any seizure or freezing of property must be reported "forthwith" to the jurisdictional Magistrate. This mandatory safeguard is designed to ensure judicial oversight and prevent executive overreach. In practice, this reporting is frequently neglected. Account holders often discover their funds are frozen only when a transaction fails at a point of sale or a cheque is dishonored, leading to what many describe as "complete financial paralysis".

| Statute | Section | Legal Function | Point of abuse |
|---|---|---|---|
| BNSS | 106 (formerly 102 CrPC) | Power to seize property suspected of being stolen | Arbitrary freezes without Magistrate notification[5] |

[4] *State of Maharashtra v. Tapas D. Neogy*
[5] https://legal.economictimes.indiatimes.com/news/litigation/bombay-high-court-rules-against-freezing-bank-accounts-in-cyber-fraud-cases/125491922

| | | | |
|---|---|---|---|
| IT Act | 66D | Punishment for cheating by personation | Filing false personation claims in P2P trades |
| BNS | 356 | Provisions against cyber defamation | Weaponized in matrimonial and personal disputes |
| IPC | 211 | Punishment for filing false charges with intent to injure | Rarely invoked against portal abusers |
| PMLA | 5 | Provisional attachment of proceeds of crime | Used to justify prolonged freezes in minor cases |

The absence of strict accountability mechanisms and penalties for false reporting further aggravates the problem. While genuine victims of cybercrime deserve immediate protection, unchecked misuse of the portal dilutes law enforcement resources and diverts attention from legitimate cases. Moreover, such abuse directly violates the fundamental principles of natural justice, particularly the presumption of innocence and the right to fair procedure.

Individuals accused through frivolous complaints are often subjected to procedural harassment without timely remedies or safeguards.

Additionally, the misuse of the Cyber Cell Portal raises serious concerns regarding data privacy and misuse of state power. Arbitrary access to personal devices and digital information without judicial oversight erodes public trust in cyber law enforcement institutions. If left unaddressed, the growing abuse of the Cyber Cell Portal risks transforming a protective legal mechanism into a tool of oppression, thereby threatening the credibility of the justice system and the rule of law itself. Effective reforms, procedural safeguards, and strict action against false complainants are essential to restore balance and ensure that the portal serves its intended purpose of justice rather than harassment.

## 3. Anatomy of Portal Abuse

The abuse of the cyber cell portal is not a monolith but a multifaceted phenomenon that

manifests differently across various sectors of the digital economy. The ease of filing a complaint, requiring only a basic description and an identity proof has turned the portal into a tool for extrajudicial coercion.

### 3.1 The P2P Cryptocurrency Trading Crisis

The most pervasive area of abuse is found in Peer-to-Peer (P2P) cryptocurrency trading on global exchanges. Fraudsters often employ "triangular scams" to illicitly gain funds. In this model, a scammer tricks a victim into sending money directly to the bank account of a legitimate P2P crypto seller. The scammer then receives the cryptocurrency from the seller and disappears. When the victim realizes they have been defrauded, they report the transaction to the 1930 helpline.

The system automatically flags the seller's account as the "beneficiary" of fraudulent funds, leading to an immediate debit freeze[6]. Because money moves rapidly through the banking system, this freeze often cascades through multiple layers (Layer 1, Layer 2, Layer 3 accounts), affecting hundreds of innocent secondary and tertiary account holders who have no knowledge of the original fraud. These account holders, many of whom are small business owners or freelancers, find their entire working capital frozen over a small suspicious credit, sometimes as low as ₹150.[7]

### 3.2 Weaponization in Civil and Commercial Disputes

The portal is increasingly used as a "short-cut" for debt recovery in civil and contractual disputes. Instead of following the lengthy process of a civil suit, an aggrieved party may file a complaint on the NCRP alleging "online fraud" or "hacking" to freeze the counterparty's bank account. This tactic is particularly effective in harassing Micro, Small, and Medium Enterprises (MSMEs) whose liquidity is essential for daily operations.

The impact is exacerbated by the "blanket freeze" methodology. Investigating agencies often direct banks to freeze the entire account balance rather than marking a lien on the specific disputed amount. This is done even when the disputed sum is negligible compared to the total

[6] https://www.taxmann.com/research/company-and-sebi/top-story/10501000000026755/safeguarding-rights-in-the-age-of-digital-fraud-legal-challenges-to-arbitrary-account-freezes-experts-opinion
[7] https://www.binance.com/en-IN/square/post/9471115057850

balance. For example, the Delhi High Court noted a case where an account with a withdrawable balance of over ₹93 crore was frozen in its entirety over a suspicious transaction of just ₹200.[8]

### 3.3 Matrimonial Sabotage and Personal Vendettas

The categories of "Crimes Against Women and Children" and "Other Cybercrimes" on the portal are susceptible to weaponization in matrimonial litigation. Estranged spouses may file complaints of cyberstalking, defamation, or "unauthorized access" to social media accounts to gain leverage in divorce or child custody battles. The National Crime Records Bureau compiled data showing a significant rise in cybercrime cases against women, totaling 14,409 in 2022[9]. While many are legitimate cases of sextortion or harassment, the portal's lack of a pre-verification mechanism allows for the filing of frivolous reports to settle personal scores.

## 4. Structural Vulnerabilities and Procedural Flaws

The systemic abuse of the NCRP is facilitated by several structural flaws in the reporting and investigative process. These vulnerabilities range from technical routing issues in the 1930 helpline to the institutional culture of the Indian police.

### 4.1 The 1930 Helpline and the Jurisdictional Roadblock

A critical flaw exists in the national helpline 1930, which routes calls based on the physical location of the caller rather than the location of the bank or the victim's residence. In a mobile society where people travel across state lines for work or tourism, this location-based routing creates significant delays. For example, a victim from Hyderabad who is scammed while on a trip to Vijayawada will have their call routed to the Andhra Pradesh cyber cell. Because the bank account is in Telangana, the AP police may refuse to act or claim they lack the jurisdiction to freeze the account, forcing the victim to wait until they return home to report the crime. This geographic tethering often costs the victim the "Golden Hour," [10]during which the funds could have been successfully intercepted.

[8] https://www.scconline.com/blog/post/2025/03/01/delhi-high-court-freezing-bank-accounts-cyber-crime-policy-reform-legal-news/
[9] https://recordoflaw.in/the-matrimonial-cyber-fraud-in-india-legal-framework-and-emerging-trends-2/
[10] https://timesofindia.indiatimes.com/business/cybersecurity/jurisdiction-flaw-in-1930-helpline-costs-cyber-fraud-victim-crucial-response-time/articleshow/121391891.cms

### 4.2 Verification Gaps and the "Shoot First" Approach

The NCRP does not require a First Information Report (FIR) to be registered before an account freeze is initiated. A simple "petition" or "complaint" on the portal is sufficient to trigger a debit freeze[11]. This "pre-FIR" freeze is intended to prevent the dissipation of funds, but it operates on a standard of "suspicion" that is far lower than the standard of evidence required for other forms of seizure. Furthermore, the lack of transparency means that the affected account holder is rarely informed of the reason for the freeze or the specific complaint number.

### 4.3 The Burden on Law Enforcement and Institutional Stress

The Indian police force faces immense pressure to resolve cybercrime cases in an environment where criminals often have a technological edge. There is just one civil police officer for every 1,037 residents in India[12], significantly below the global average. This overstretching, combined with a lack of specialized training in digital forensics and cyber law, leads many officers to take "short-cuts". Refusing to register complaints to keep crime statistics low, or automatically freezing any account linked to a transaction trail without investigation, are common responses to the systemic stress of the investigative process.

## 5. Judicial Response and the Push for Reform

The increasing frequency of arbitrary account freezes has triggered a significant wave of litigation, forcing the Indian judiciary to intervene and uphold constitutional protections. The central theme of recent judicial pronouncements is that the state’s power to freeze must be exercised proportionately and within the bounds of due process.

### Landmark Cases: Vivek Varshney and Neelkanth Pharma

The Supreme Court of India recently agreed to examine a petition seeking a uniform Standard Operating Procedure (SOP) for the freezing and de-freezing of bank accounts in cybercrime cases. The case, *Vivek Varshney v. Union of India (2026)*,[13] was filed by a petitioner whose

[11] https://lawbeat.in/top-stories/account-frozen-without-notice-plea-in-supreme-court-seeks-nationwide-sop-on-cyber-cell-bank-freezes-1553709
[12] https://www.hrw.org/report/2009/08/04/broken-system/dysfunction-abuse-and-impunity-indian-police
[13] *Vivek Varshney v. Union of India (2026)*

accounts were frozen by the Tamil Nadu Cyber Cell without notice or judicial approval, resulting in what the plea described as "financial paralysis". The petition emphasizes that the lack of time limits and oversight mechanisms has led to "rampant misuse of freezing powers" and violates fundamental rights under Articles 19(1)(g) and 21.

The Delhi High Court, in *Neelkanth Pharma Logistics Pvt Ltd v. UOI*,[14] strongly condemned the "indiscriminate freezing" of bank accounts, particularly when based on minuscule transactions. The court held that unless an account holder is proven to be complicit in a crime, their entire account should not be restricted. It recommended that the Ministry of Home Affairs formulate an SOP where marking a lien on the specific disputed amount should be the "first and foremost option".

## 6. Personally Faced Incident

A particularly alarming consequence of such misuse is reflected in my own experience, where my bank accounts were frozen pursuant to a wrongful and baseless complaint lodged through the Cyber Cell Portal bearing acknowledgment no.21609250041622. The freezing of my accounts was carried out without proper verification, prior notice, or an opportunity to be heard, amounting to a gross violation of my **fundamental right to life and personal liberty under Article 21 of the Constitution of India**, which includes the right to livelihood and dignity. As a result, I have been rendered incapable of carrying out basic banking transactions, including meeting daily expenses, professional commitments, and financial obligations. This arbitrary action has caused significant monetary losses, disrupted my livelihood, and subjected me to severe mental stress, anxiety, and trauma. The indiscriminate freezing of bank accounts based solely on an unverified complaint reflects a serious procedural lapse and misuse of state power, highlighting how the Cyber Cell Portal, when abused, can inflict disproportionate harm on innocent individuals and undermine the principles of due process and natural justice.

## 7. Criticism of the Misuse of the Cyber Cell Portal

### 1. Violation of Fundamental Rights

One of the most significant criticisms of the misuse of the Cyber Cell Portal is the infringement of fundamental rights guaranteed under the Constitution of India. In cases

[14] *Neelkanth Pharma Logistics Pvt Ltd v. UOI*,

like mine, where bank accounts were frozen based on a wrongful complaint, there was a direct violation of **Article 21**, which protects the right to life, liberty, and livelihood. The arbitrary freezing of accounts deprived me of the ability to access my earnings and maintain daily necessities. Such actions, taken without verification or due process, also breach **Article 14**, which ensures equality before the law and equal protection of the law, as innocent individuals are treated punitively without proper cause.

2. **Lack of Verification and Preliminary Scrutiny**

The Cyber Cell Portal allows complaints to be lodged with minimal verification, creating an environment where false or malicious complaints can be filed easily. This systemic weakness enables misuse by individuals seeking personal revenge, financial gain, or harassment. In my case, the wrongful complaint resulted in immediate freezing of bank accounts, demonstrating a lack of preliminary assessment or validation, which is essential to ensure that only genuine complaints are acted upon.

3. **Disproportionate Administrative Measures**

The portal empowers authorities to take immediate action against alleged offenders, such as freezing bank accounts, seizing digital devices, or suspending online accounts. While intended to prevent further harm, these measures can become excessively punitive when the complaint is unverified or malicious. In my instance, the freezing of accounts caused severe financial disruption, hindered professional obligations, and prevented even routine banking transactions. Such disproportionate measures illustrate how the system can inflict harm far beyond the scope of the alleged offence.

4. **Procedural Lapses and Lack of Opportunity to be Heard**

Another critical issue is the absence of a mechanism for accused individuals to respond before punitive actions are taken. Due process requires that every individual be given a fair chance to explain, rebut, or clarify allegations. The immediate freezing of my accounts without prior notice or hearing violated this principle and demonstrates a significant procedural lapse, undermining the credibility of cyber law enforcement practices.

5. **Mental and Emotional Trauma**

Misuse of the portal does not merely cause financial or procedural harm; it also has profound psychological consequences. Being subjected to harassment through false complaints induces stress, anxiety, and mental trauma. In my experience, the wrongful complaint and subsequent freezing of my bank accounts led to intense emotional strain, affecting both personal well-being and professional productivity. The portal, when abused, becomes a tool of intimidation and coercion rather than protection.

6. **Resource Diversion and Systemic Inefficiency**

False or malicious complaints consume significant law enforcement resources that could otherwise be dedicated to investigating genuine cybercrimes. Misuse of the portal therefore not only harms the accused but also undermines the overall efficiency of the cybercrime detection system. The authorities' attention is diverted, slowing down legitimate investigations and reducing public trust in digital crime reporting mechanisms.

7. **Absence of Accountability for False Complaints**

Currently, the Cyber Cell Portal lacks strict safeguards and penalties for filing false complaints. Individuals can misuse the system with minimal consequences, as demonstrated by my case. Without accountability, the portal inadvertently incentivizes harassment, threatening innocent citizens' rights while failing to deter malicious actors.

8. **Breach of Public Trust in Digital Law Enforcement**

The improper use of the portal undermines public confidence in government digital services. When innocent individuals, like myself, experience undue punitive actions, the perception arises that cyber law enforcement tools can be weaponized. This erodes trust in the legal system and discourages people from relying on official digital mechanisms for justice.

## 8. High Court Criticism: Bank Account Freeze Without Due Process

In a recent case before the Guwahati High Court, a micro enterprise's current bank account with over ₹12 lakh was abruptly frozen following a complaint lodged through the National Cyber Crime Reporting Portal. The account had been operational lawfully since October 2024,

but in January 2025, all debit transactions were stopped without notice or preliminary inquiry, simply because a cybercrime complaint linked to suspected fraud had been filed. The account holder argued that the freeze was imposed without adequate verification or opportunity to be heard, causing severe prejudice to the business. The High Court noted that while cyber fraud investigations are necessary, they must be balanced with the rights of innocent account holders and cannot be sustained in the absence of proper legal safeguards.

This case is significant because it highlights several key concerns central to the debate on cyber complaint misuse:

- No Prior Notice or Hearing: The account was frozen without giving the account holder a chance to respond, violating basic principles of natural justice.
- Lack of Preliminary Scrutiny: Authorities acted on the complaint without verifying whether the account was genuinely involved in wrongdoing.
- Economic Harm: The freeze disrupted business operations, illustrating how cyber enforcement can inadvertently harm innocent parties.
- Judicial Scrutiny: The High Court's intervention underscores that such actions can and should be re-evaluated to protect fundamental rights.

This instance aligns closely with broader reports of innocent individuals having accounts frozen after being unknowingly linked to cyber fraud transactions, sometimes without responsive follow-up from cyber cells, a pattern emerging in multiple regions across India.

## 9. The Road to Reform: Actionable Policy Recommendations

The National Cyber Crime Reporting Portal is a vital instrument for public safety, but its current implementation is a growing threat to due process. The shift from protection to weaponization requires a comprehensive policy response that reinstates the primacy of the rule of law.

### 9.1 Mandatory Lien-Marking as the Default Measure

Investigating agencies must be directed to abandon the practice of blanket debit freezes for small suspicious transactions. A uniform policy should be adopted across all states where the

marking of a "lien" on the specific disputed amount is the default first step. This ensures that the state's interest in the potential proceeds of crime is secured without destroying the financial life of the account holder.

### 9.2 Implementation of a Uniform SOP with Judicial Oversight

The Ministry of Home Affairs, in consultation with the Reserve Bank of India, must frame a nationwide SOP that mandates:

- Automatic notification to the account holder within 24 hours of a freeze.
- Mandatory digital reporting of the freeze to the jurisdictional Magistrate within the same window.
- A time-bound limit on administrative freezes, after which a formal court order is required for extension.

### 9.3 Decoupling the 1930 Helpline from Geographical Routing

The technical configuration of the 1930 helpline must be updated to route calls based on the bank's jurisdiction or the victim's residence rather than their real-time GPS coordinates. A truly centralized national response system should be able to issue freeze instructions to any bank in India, regardless of where the call originates, to effectively utilize the "Golden Hour".

### 9.4 Accountability for Malicious and False Complaints

The abuse of the portal to settle civil debts or personal vendettas must be met with strict legal consequences. Law enforcement should be trained to identify red flags of civil disputes masquerading as cybercrime. When a complaint is found to be false or malicious, the provisions of Section 211 IPC (or BNS equivalent) must be vigorously invoked to deter future portal abuse.

### 9.5 Provision for Essential Living Expenses

Drawing inspiration from Singapore's framework, the Indian system should include a provision allowing account holders to withdraw a specified minimum amount for "daily living expenses"

or medical emergencies while an investigation is pending. This would mitigate the human rights violations inherent in total financial paralysis.

**Conclusion**:

The misuse of the Cyber Cell Portal has exposed a critical flaw in our digital justice system, where tools designed to protect citizens from cybercrime are increasingly being weaponized against the innocent. Cases like wrongful freezing of bank accounts without verification, notice, or an opportunity to be heard highlight how such practices violate fundamental rights, disrupt livelihoods, and cause severe mental and financial trauma. The system, in its current form, fails to balance the need for swift cybercrime intervention with the principles of natural justice and due process. This is a clarion call to reform the portal: establish rigorous verification protocols, implement strict accountability for false complaints, and ensure safeguards to protect the rights of innocent individuals. The Cyber Cell Portal must serve as a mechanism of protection, not harassment. Without immediate corrective action, it risks undermining public trust in law enforcement and the very integrity of justice.