# CYBER-ENABLED FINANCIAL FRAUD AND DIGITAL ARREST SCAMS: GAPS IN BNS/IT ACT COORDINATION

Abed Husen Sayyad, Symbiosis Law School, Pune, Symbiosis International (Deemed University)

**ABSTRACT**

The growing incidence of "digital arrest" and related types of cyber-enabled financial fraud have revealed a structural gap in India's post-2024 criminal law system: the "join" of the Bharatiya Nyaya Sanhita, 2023 ("BNS") and the Information Technology Act, 2000 ("IT Act"). In this paper, the current state of that coexistence is analysed from the doctrinal and policy perspective. It charts the substantive provisions each statute brings to bear in the fight against impersonation-based cyber fraud, identifies institutional and procedural fault lines that can occur when general criminal law and special cyber legislation are brought to bear in the same first information report, and provides a framework for this analysis within the Supreme Court's current Suo motu case of In re Victims of Digital Arrest Related to Forged Documents. It alleges that the lack of a harmonising agenda among the BNS and the IT Act aggravated by inconsistent definitions of offences as cognizable or bailable, disjointed investigative powers, lack of a provision that enables sharing of real-time information from banks with telecom platforms and absence of a specific offence to tackle the use of impersonation of law-enforcement and judicial authorities for extortion has created an impromptu coordination gap that fraud syndicates, many of whom operate outside India's borders, are exploiting. The paper ends with a list of legislative and institutional recommendations such as a proposed harmonisation schedule, a specific offence for "impersonation of state authority for digital extortion" and statutory timelines for intermediary and telecom cooperation, as well as a victim compensation mechanism on the lines of existing financial-fraud compensation frameworks.

**Keywords:** Digital arrest scam, Bharatiya Nyaya Sanhita, Information Technology Act 2000, cyber fraud, BNS-IT Act coordination, cheating by personation, cybercrime jurisdiction, I4C

## I. INTRODUCTION

A 73-year-old woman in Ambala, Haryana, wrote a letter to the Chief Justice of India on 21st September 2025. She and her husband, the letter said, have been virtually imprisoned for nearly two weeks by those who showed them fake orders with the Supreme Court's seal to extort more than one crore rupees from them[1]. The Supreme Court, took Suo Motu, cognisance of complaint, which it registered as "In re Victims of Digital Arrest Related to Forged Documents", and noted that the making of judicial orders with forged judicial signatures undermined the trust in the rule of law[2]. The Ambala case was nothing out of the ordinary. The government estimates that citizens have lost about Rs. In 2024 alone, the total reported cyber financial fraud cases were around 36.37 lakh and the total cyber financial fraud amount was more than two hundred per cent more than the last year, which is 22,845.73 crore[3].

The "digital arrest" phenomenon is less sensational with regard to the forged court seals, the supposedly real interrogation rooms, the psychological coercion of the elderly victims, than it is with respect to its more muted legal-architectural problem, which it has exposed. Since 1 July 2024, India has enforced cybercrime under two different and overlapping sets of laws, one, the Bharatiya Nyaya Sanhita, 2023 (replacing the Indian Penal Code, 1860) and two, the Information Technology Act, 2000, which remains as India's unique cyber law. The BNS was not written to incorporate the current language of the other statute (or the IT Act was written to refer to the current language of the BNS), as even at the time of the BNS's enactment, the language of the two was constructed around distinct conceptions of computer crime[4]. Neither statute was written with the other's current wording in mind: the BNS is a wholesale recodification of general criminal law that happens to reference cyber-related offences through general terms such as "cheating," "forgery," and "criminal intimidation"; and the IT Act remains embedded in a definitional and technological vocabulary largely frozen in time in 2008. This leaves behind a continuing and growing mismatch in the way charge-sheeting is done, how offences are classified, where the investigation is located, and the ways it is possible to force banks, telecom operators and intermediaries to act in real time.

The argument consists of six additional parts. Part II discusses the anatomy and size of digital

[1] In re Victims of Digital Arrest Related to Forged Documents, Suo Motu Writ Petition (Crl.) No. 3 of 2025 (S.C., order dated 17 Oct. 2025) (India); see also Aaratrika Bhaumik, Supreme Court Issues Notice to Centre Over 'Digital Arrest' Scam, MediaNama (Oct. 21, 2025), https://www.medianama.com/2025/10/223-supreme-court-notice-centre-digital-arrest-judicial-seals/.

[2] Supreme Court Takes Suo Motu Cognisance of 'Digital Arrest' Scams, Issues Notices to States, UTs, Outlook

arrest fraud, which is a type of cyber facilitated financial fraud. Part III explains how the BNS provisions, which in practice are invoked in a single FIR, are harmonised with the provisions of the IT act and the general law applied to the digital medium and the special law addressed to the medium itself. This is a dual statute which creates six separate coordination gaps, as identified in Part IV. Part V reviews the on-going suo motu proceedings of the Supreme Court as a case study to illustrate these gaps in the context of live litigation and executive action. Part VI reviews the institutional steps announced by the Ministry of Home Affairs and the Reserve Bank of India in response to the directions of the Court, and determines the extent to which the gaps pointed out in Part IV are met. Part VII presents specific legislative and institutional options, while Part VIII is the conclusion.

## II. THE ANATOMY OF DIGITAL ARREST SCAMS AND THEIR MODUS OPRANDI

The word "digital arrest" does not appear in the statute, but rather is a term of art used by investigators and courts to describe a certain series of impersonation-based extortion. The fraud starts with a call from someone pretending to be an official of an investigative agency or a regulatory authority – such as the CBI, the Enforcement Directorate, the Narcotics Control Bureau or, with growing frequency, the judiciary. The victim is informed that there is a package, SIM card or bank account in his/her name that has been used in a serious crime, typically money laundering or narcotics activity. There is a video call which is set up to look like an interrogation room with uniforms, official insignia and in the case of Ambala, fake orders supposedly signed by the Supreme Court in the name of a previous Chief Justice of India[5]. The victim is then told that they are being monitored, that they should not contact their family or police, and that they should move money to certain accounts to "prove" that they are innocent or they must obey the asset-freeze order claimed under the Prevention of Money Laundering Act, 2002.

This is quite different from previous waves of cyber fraud, like lottery fraud or traditional phishing. First, it arms what it calls the "coercive authority" of the State itself, of which the

(Oct. 29, 2025)
https://www.outlookindia.com/national/supreme-court-takes-suo-motu-cognisance-of-digital-arrest-scams-issues-notices-to-states-uts.,

[3] Supreme Court Issues Notice to Centre Over 'Digital Arrest' Scam, supra note 1.

[4] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Preamble (India) (in force 1 July 2024); Information Technology Act, 2000, No. 21 of 2000 (India).

[5] SC Takes Suo Motu Cognisance of 'Digital Arrest' Scams, Issues Notice to Centre, CBI, The Shillong Times (2025), https://theshillongtimes.com/2025/10/17/sc-takes-suo-motu-cognisance-of-digital-arrest-scams-issues-notice-to-centre-cbi/.

visual and documentary grammar of arrest, seizure and judicial process is the medium, to create compliance that ordinary confidence tricks can't. Second, it is carried out by a multi-layered technological stack, including spoofed caller IDs, encrypted messaging apps, fake PDF orders and mule bank accounts, that cuts across multiple regulatory silos: telecommunications, banking and information technology (IT) intermediation. Third and most importantly from the current point of view the wrongs which it inflicts are not novel wrongs, but old wrongs – such as cheating, criminal intimidation, impersonation of a public servant, and forgery – in new forms. This double nature is what makes investigators have to simultaneously rely on the BNS and the IT Act, and it is what gives rise to coordination problems which are analysed in this paper.

The magnitude of the problem has given rise to a constitutional doctrine question. In addition to the aggregate loss statistics, the Ministry of Home Affairs, Government of the Union, told Parliament and the Supreme Court that it has arrested more than 83,000 WhatsApp accounts and almost 4,000 Skype identifiers that were used in digital arrest fraud[6]. The Attorney General (AG) of India, who appeared before the Supreme Court, admitted that a considerable number of these syndicates were located beyond the territorial boundaries of India, including some in Myanmar and Thailand, which would otherwise make the case one of ordinary criminal investigation, but render the issue one of extradition, mutual assistance, and scope of Indian criminal laws[7].

## III. THE DUAL-STATUTE ARCHITECTURE: BNS AND IT ACT IN CYBER FRAUD PROSECUTIONS

### A. Relevant Provisions of the Bharatiya Nyaya Sanhita, 2023

There is no chapter on cybercrime in the BNS. Instead, it is an expansion of a group of general crimes (most of which are direct descendants of the Indian Penal Code which was repealed) that are committed via electronic devices, social media and computer networks. In digital arrest and related fraud cases, there are four clusters of provisions which are frequently invoked.

First, the offence of cheating under Section 318, which is a consolidation of the offences of

[6] Id.
[7] SC Issues Notices to All States, UTs in Suo Moto Case on 'Digital Arrest' Scams, Bilkul Online (2025), https://bilkulonline.com/2025/10/27/sc-issues-notices-to-all-states-uts-in-suo-moto-case-on-digital-arrest-scams/.

cheating, dishonest or fraudulent induction on to a person to part with property, as found in the old Sections 415, 417 and 420 of the Indian Penal Code, carries a stricter punishment as compared to its predecessor, the BNS[8]. This Section 319, which is the successor to Section 416 of the former Code, covers a more serious form of cheat by personation, namely where the person pretends to be a bank manager, an investigating officer or a judicial officer in order to persuade a person to transfer funds[9].

Second, public servants are specifically referred to in their own right. Sections 204 (formerly 170 of the Indian Penal Code) and 205 (formerly 171) are clearly relevant to callers who appear on video in the guise of the C.B.I. or a judge and are actually impersonating an official or wearing garb or carrying a token used by an official with fraudulent intent[10].

Third, the provisions on forgery in Section 336 (which was a consolidation of Sections 463, 465 and 468) renders the making of a fake court order, arrest warrant, and freeze notice as a crime, albeit one that is not clearly defined. Third, under Section 336 (combining the former Sections 463, 465 and 468), the fabrication of false documents is made a crime, and that is an obvious fit for the manufacture of counterfeit court orders, arrest warrants, and freeze notices that gave the Ambala scam its coercive force[11]. Third, Section 351(4) punishes "criminal intimidation by anonymous communication" which includes the threats of arrest and asset seizure that are repeated throughout the course of the scam and that maintain the victim's compliance. The BNS's new organised-crime section, Section 111, also comes into play where the fraud is organised and executed from a State or an international border, as the Ambala case and the Attorney General's submissions suggest, is now standard practice[12].

### B. Relevant Provisions of the Information Technology Act, 2000

The special statutory regime of the IT Act runs parallel to this general law regime. Section 66C is the section which imposes a penalty on identity theft, that is the use of another person's

[8] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 318 (India); see also Cheating Under the Bharatiya Nyaya Sanhita, 2023: A Comprehensive Legal Analysis, Legal Bites (Apr. 23, 2025), https://www.legalbites.in/bharatiya-nyaya-sanhita/cheating-under-the-bharatiya-nyaya-sanhita-2023-a-comprehensive-legal-analysis-1134664.
[9] Bharatiya Nyaya Sanhita, 2023, § 319.
[10] Bharatiya Nyaya Sanhita, 2023, §§ 204–205; Understanding Cyber Frauds, Digital Arrests and How to Protect Yourself, SCC Online Blog (Nov. 5, 2025), https://www.scconline.com/blog/post/2025/11/05/understanding-cyber-frauds-digital-arrests-protection-tips-law-made-easy-scc-times/.
[11] Bharatiya Nyaya Sanhita, 2023, § 336(1)–(3).
[12] Bharatiya Nyaya Sanhita, 2023, §§ 111, 351(4).

electronic signature or password or other unique means of identification, and its more directly related counterpart, Section 66D, imposes a penalty on the cheating by a personation using a computer resource or communication device[13]. The civil-liability provisions of Section 43 of the Act, which penalise unauthorised access to and damage of computer systems, and the criminal provisions of Section 66 of the Act, which penalise dishonest or fraudulent acts covered by Section 43, provide a residual charge for the unauthorised access aspects of mule-account fraud[14]. Section 66F, which relates to cyber-terrorism, is used sparingly, and its conditions of use that a denial of access to authorised persons or an unauthorised access that causes injury to persons or damage to critical infrastructure have been called for in the biggest syndicate cases involving national-security adjacent targets[15].

Section 79 has a unique structure. It provides intermediaries (social media platforms, payment gateways, etc. and messaging services linked to telecom) with a "safe harbour" from liability for third party content and transactions, provided they take "reasonable measures" and follow lawful government instructions, such as the Intermediary Guidelines and Digital Media Ethics Code Rules issued under the Act in 2021[16]. Since this safe harbour is based on cooperation and not predicated on any particular time limit for assistance in the ongoing fraud investigation, it becomes as Part IV. The point of the disagreement between D and the BNS is the coordination gap between the general criminal process and the special regulatory process in the IT Act, which D contends.

### C. The Doctrinal Rationale for Coexistence, and Its Practical Costs

A combination of general and special criminal law is not any unnatural or undesirable arrangement. General offences are regularly used in the context of data protection, telecommunications or securities law, which is subject of a separate regulation by a special statute. The BNS provides the architecture (mental element, harm) and the vocabulary (intermediary, computer resource, unique identification feature); the IT Act includes the regulation (Controller of Certifying Authorities, safe-harbour, blocking mechanisms) and the

[13] Information Technology Act, 2000, No. 21 of 2000, §§ 66C–66D (India); see also Section 66C and 67D of the IT Act Explained, Legal Bihar (Nov. 12, 2025), https://legal.bihar.in/section-66c-and-67d-of-the-it-act-explained-key-case-laws/.
[14] Information Technology Act, 2000, §§ 43, 66.
[15] Information Technology Act, 2000, § 66F.
[16] Information Technology Act, 2000, § 79; Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; see The Information Technology Act, 2000, LawBhoomi (Mar. 28, 2026), https://lawbhoomi.com/the-information-technology-act-2000/.

technologically specific vocabulary. Investigators, in most reported cyber fraud matters, therefore enter both of these provisions into one first information report, which is recognized and accepted as not "special" in case commentaries explored above[17].

But the practical costs of this arrangement are not trivial and are not often discussed in the literature on cyber fraud, which has generally been more engaged in a catalogue of the provisions of each statute as they apply to the specific frauds of interest than in exploring the friction created by their concurrent operation. It is to this coordination friction, the subject of this paper's title, that the focus turns in the analysis.

## IV. MAPPING THE COORDINATION GAPS

### A. Jurisdictional Fragmentation and Cross-Border Enforcement

They are the type of arrest syndicate which is digital; usually operates in jurisdictions other than the police station where the victim lives, and often outside India. The Attorney General's description of a number of such syndicates operating in Myanmar and Thailand highlights a jurisdictional issue which either the BNS or the IT Act, alone, is not particularly well suited to address[18]. The IT Act also extends its jurisdiction to any offence that is committed with respect to a computer resource located in India, regardless of the nationality of the offender or their location, but these treaties and Interpol channels are time-consuming and involve months of time, while the money sent in a digital arrest scam can be mulled and drawn within hours[19]. Because the BNS is entirely inward looking, it has no parallel to the extraterritorial mechanism found in the countries of origin of the Convention; its territorial bases are the place of the offence and the residence of the accused, which are poorly suited to the offence with several bases in different countries.

Jurisdictional fragmentation is also experienced within India at the State level. The same conduct leads to multiple complaints being lodged by the various cyber cells of the State, leading to investigations being conducted in parallel, as in the case of multiple FIRs in Haryana in the Ambala proceedings in the Supreme Court[20]. The Supreme Court's recommendation for

[17] Offences Against Cybercrime under the Bharatiya Nyaya Sanhita, 2023, Your Law Article (Feb. 20, 2026), https://www.yourlawarticle.com/post/offences-against-cybercrime-under-the-bharatiya-nyaya-sanhita-2023-bns.
[18] SC Issues Notices to All States, UTs in Suo Moto Case, supra note 8.
[19] The Information Technology Act, 2000: A Comprehensive Guide, Airacle Labs (Jul. 21, 2025), https://airacle.in/blog/it-act-2000/.
[20] SC Issues Notices to All States, UTs in Suo Moto Case, supra note 8 (noting multiple FIRs registered by

a central inquiry into cyber fraud under the CBI was an ad hoc judicial impropriety, without any statutory tools or provisions to coordinate investigations across States as found in the Bharatiya Nagarik Suraksha Sanhita (BNS) or the IT Act[21].

**B. Inconsistent Classification: Cognizability, Bailability, and Charge-Sheeting Practice**

A second difference comes from the different classificatory logic for the two statutes. The classifications of cognizability and bailability are given in the First Schedule of the Bharatiya Nagarik Suraksha Sanhita, which is based on the sentencing provisions in the BNS. Offences under the IT Act have their own, separately drafted classifications in Section 77 and the IT Act's schedule, based on sentencing under the IT Act. If the same transaction is covered by both Section 318/319 BNS as well as Section 66D IT Act, the investigators as well as courts have to cross-validate two classificatory regimes which were not prepared taking into account each other. In practice this means that bail practice varies from station to station and on occasion from State to State; and that the more 'generous' of the two classifications can be pressed by the defence regardless of which is the better to reflect the gravity of the fraud.

This is exacerbated by the lack of any statutory provision clarifying the sentencing issue between the general and special offence, both of which are based on the same facts. There are some broad principles against double jeopardy and a general principle of a saving and harmonisation clause that are helpful in providing guidance, but these principles are not explicitly set out in the BNS or the IT Act. There is no section 81 of the erstwhile IT Act (prior to the amendment) similar to that of the IT Act and other enactments. What this means is that the practice of charge-sheeting is different among investigating officers and different from jurisdiction to jurisdiction and the predictable results for which the codification exercise was intended were not realized.

**C. Absence of a Dedicated Offence for State-Impersonation Digital Extortion**

The most conceptually important lacuna is definitional, in that the BNS and the IT Act do not have an offence specifically tailored to the hallmark of the digital arrest scam: the impersonation, via live video, of a judicial or law-enforcement figure, backed by fake judicial

Ambala's Cyber Crime Branch and directing other States to furnish similar details).

[21] Digital Arrests | MHA Proposes SOP Before Supreme Court, LiveLaw (Feb. 10, 2026), https://www.livelaw.in/amp/top-stories/supreme-court-digital-arrest-scam-suo-motu-mha-status-report-sop-rbi-cbi-dot-meity-victim-compensation-liability-framework-522549.

or law-enforcement paperwork, to the end of extortion. Existing charges need to be collated from provisions which were drafted for more narrow or more generic wrongs: personation under Section 319 BNS, impersonation of a public servant under Sections 204 – 205 BNS, forgery under Section 336 BNS, and cheating by personation under Section 66D IT Act[22]. None of these provisions reflects the aggravated nature of the offence at its totality, or the abuse of judicial power as a tool of coercion, which the Supreme Court itself called the 'very essence of public confidence in the rule of law[23]. A prosecutor is then left with the task of obtaining the aggregate sentence from a series of charges and not from one offence which bears the maximum sentence that Parliament, if it were asked, would attach to this conduct. This is a gap in the legislation in the strict sense: It is not about what is interpreted or how it will be enforced, but because there is no offence in the BNS and no offence in the IT Act.

**D. Intermediary and Telecom Cooperation: The Section 79 Safe-Harbour Problem**

The digital arrest scams are based on a series of intermediated services used: VoIP and messaging applications for the impersonation call, e-mail or file-sharing services for the documents used as forgery, banking channels for fundraising and layering of funds. Section 79 of the IT Act imposes a due diligence requirement on the intermediary and its compliance with lawful government directions, but neither the IT Act nor the rules made under it provide for a specific time frame within which the intermediary must cooperate during an active fraud investigation, of the nature at issue in these proceedings. The 2018 intermediary guidelines do set a 72-hour response period, and a 24/7 nodal contact for cybersecurity requests, but that period is for security and cybersecurity coordination in general, not for the time it takes to intercept a fraudulently induced transfer of funds before they are withdrawn via a mule account which is often minutes[24]. BNS, on its side, does not provide any statutory anchor to compel intermediary cooperation, that is left to the IT Act and executive directions given under it – without any cross-reference harmonising between the two.

This deficiency is also acknowledged and evident in the responses of the regulatory bodies in recent times. Twenty-six banks have deployed an AI monitoring application called

[22] Bharatiya Nyaya Sanhita, 2023, §§ 204–205, 319, 336; Information Technology Act, 2000, § 66D.
[23] SC Takes Suo Motu Cognisance of 'Digital Arrest' Scams, Issues Notice to Centre, CBI, supra note 4.
[24] Information Technology Act, 2000, § 79; see In this situation the government proposed stringent changes to Section 79 of the IT Act, IIPRD (Jun. 4, 2024), https://www.iiprd.com/section-66a-of-it-act2000/ (discussing the 2018 intermediary rules' 72-hour response obligation for security and cybersecurity requests, and the requirement of a 24×7 nodal officer).

"MuleHunter.ai" and the Supreme Court directed the SIM-binding and session-duration limits for the telecommunication identifier user entities, such as WhatsApp, Telegram, Signal and Arattai, have been given by the Ministry of Home Affairs, through a High-level Inter-Departmental Committee set up according to its directions[25]. While welcome, these measures have come in the form of executive directions that are subject to ongoing judicial oversight, and not as a statutory obligation under the IT Act, so that the durability and enforceability of these measures depends on judicial oversight a thin reed on which to rest what should be a permanent part of the regulatory landscape.

### E. Institutional Overlap: I4C, CERT-In, RBI, and State Cyber Cells

Another coordination split is at the institutional design level, not on the statute book. The Indian Cyber Crime Coordination Centre (I4C), under the Ministry of Home Affairs, collects complaint information and coordinates the National Cyber Crime Reporting Portal, CERT-In under Section 70B of the IT Act regulates response of banking sector on mule account and fraudulent transactions, and State cyber cells conduct the actual criminal investigation under the BNS and the IT Act. Only I4C has its coordinating mandate from an executive order, CERT-In from the IT Act, and RBI from banking and payment system legislation that is completely separate from the BNS or the IT Act[26]. Under the Prevention of Money Laundering Act, 2002, Section 12AA, which was the subject of this consultation, does not mandate that any one agency make such a determination as it is a measure that could be invoked alongside other laws and regulations[27].

### F. Victim Compensation and Asset-Freezing Gaps

There is no such scheme under the BNS and IT Act that specifically provides for compensation to the victims of cyber-crime like cyber fraud, with special emphasis on the recovery of the underlying money which is often not possible till the time the FIR is filed in the case of layered and cross border arrest frauds in the digital world. This is itself a recognition of the need, as evidenced in the Ministry of Home Affairs' statement before the Supreme Court that it was

[25] Digital Arrests | MHA Proposes SOP Before Supreme Court, RBI to Consider Staff Accountability & Liability Framework, LiveLaw (Feb. 10, 2026), https://www.livelaw.in/amp/top-stories/supreme-court-digital-arrest-scam-suo-motu-mha-status-report-sop-rbi-cbi-dot-meity-victim-compensation-liability-framework-522549.
[26] Information Technology Act, 2000, § 70B (establishing CERT-In); IT Act 2000, Understand UPSC (Jan. 28, 2026), https://www.understandupsc.com/information-technology-act-2000/.
[27] Digital Arrests | MHA Proposes SOP Before Supreme Court, supra note 20.

looking into the possibility of having a separate framework for compensation of victims in coordination with the other stakeholders while simultaneously reviewing gaps in bulk and corporate SIM cards issuance that enables the supply chain of mule accounts and spoofer numbers. The fact that this examination is happening well over a year and a half post the BNS and more than twenty-five years after the IT Act became law demonstrates that victim compensation was never envisioned as a coherent part of the BNS/IT Act framework, but rather is being piecemeal and added as a judicial afterthought[28].

## V. THE SUPREME COURT'S INTERVENTION AS A CASE STUDY IN COORDINATION FAILURE

The issues raised in In re Victims of Digital Arrest Related to Forged Documents are noteworthy precisely because they are played out in real time in litigation. The Bench, which included the Chief Justice of India and Justices Surya Kant, Joymalya Bagchi and (subsequently) N.V. Anjaria, refrained from focusing merely on the individual Ambala FIRs and had exhorted all States and Union Territories to provide particulars of other similar FIRs, which had been filed in their jurisdictions, noting, "we are not in a position to give substantive directions, but we are giving notice to ensure that there is a uniform investigation."[29] In essence, the Court concluded that a uniform investigation of a manifestly pan-Indian and cross-border criminal enterprise was lacking for which it saw no need to send any litigant to an extant coordination provision in the BNS or the IT Act.

It can be noted that the Ministry of Home Affairs has subsequently established a High-level Inter-Departmental Committee and the successive reports of this Committee to the Court establishes a pattern. The Committee's own draft of the Standard Operating Procedure for the debit hold on suspicious accounts, the evaluation of Section 12AA of the Prevention of Money Laundering Act, notification of the Telecommunications (User Identification) Rules, 2025, and directions regarding SIM-binding appear more like an ad hoc creation of a legislative blueprint, as demanded by the judiciary[30]. The Attorney General said that the CBI would have to separately seek consent under Section 6 of the Delhi Special Police Establishment Act, 1946 to investigate such cases which have been identified as loss of Rs. One more interesting

[28] Id. (noting further actions to examine the feasibility of a victim compensation framework in coordination with stakeholders and to review gaps in bulk and corporate SIM issuance).
[29] SC Issues Notices to All States, UTs in Suo Moto Case, supra note 8.
[30] Digital Arrests | MHA Proposes SOP Before Supreme Court, supra note 20.

example is 10 crore or above: even the centralisation of investigation of the very same syndicates whose cross-border nature the Attorney General himself highlighted is carried out under a statute that is completely different from both the BNS and the IT Act, and has no text whatsoever[31].

So, nothing about being unwelcome or ineffective; rather, the Supreme Court has brought about more concrete institutional movement within a span of few months than the previous period of the BNS operating alone. It is not a coordinated statutory regime if it requires an ongoing judicial surveillance to operate. Instead, it's evidence of the very thing that this paper was meant to chart.

## VI. INSTITUTIONAL RESPONSES AND THEIR LIMITS

The actions taken by the Ministry of Home Affairs and allied agencies and brought to the Supreme Court can be broadly divided into three categories, all of which aim at filling any of the identified gaps in Part IV but not to provide a comprehensive solution in the form of new legislation.

The first is technological, with MuleHunter.ai deployed by 26 financial institutions, and other financial institutions using their own artificial-intelligence and machine-learning systems to identify patterns that might be linked to mules transactions[32]. This is only part of the solution to the detection dimension of the problem, and is insufficient on its own to fill the gaps of classification or jurisdiction as described in Parts IV. A and IV. Even if the transaction is flagged for investigation, it still gives rise to two non-coordinated statutes.

The second type is regulatory procedural: the draft Standard Operating Procedure for temporary debit holds, the telecom sector's continued legal review of Section 12AA of the Prevention of Money Laundering Act for blocking of money laundering activities and the notification of the Telecommunications (User Identification) Rules, 2025 and the SIM-binding directions issued to messaging service providers. These measures directly address the intermediary/telecom cooperation gap outlined in Part IV.D, and are the most significant developments so far[33]. However, none of these has been enacted as an amendment to the IT

[31] Id.
[32] Digital Arrests | MHA Proposes SOP Before Supreme Court, supra note 20.
[33] Id.

Act itself, thereby not altering the core statute, and each is a delegated enactment or executive directive, making the underlying statute as unclear as before and the safe-harbour conditions in Section 79 as vague and broad as ever.

The third is institutional, in the form of the High level Inter-Departmental Committee, which involves the Department of Financial Services, the Reserve Bank of India, I4C, the Ministry of Home Affairs and the Department of Telecommunications. This body directly responds to the gap in the institutional-overlap discussed in Part IV.It does not have any independent statutory power under either the BNS or the IT Act, quite the contrary, its existence is dependent on the life of the case which gave rise to it and under the supervision of the Supreme Court in a pending suo motu case.

These responses in aggregate demonstrate a government that is reacting, effectively and at pace to issues that a more purposefully harmonised BNS/IT Act regime would have foreseen at the time the BNS was drafted. They are not yet the kind of coordinated mechanism that is now recommended in Part VII in the form of a codified coordination mechanism.

## VII. RECOMMENDATIONS

The five reforms listed below would fill the gaps identified above without the need to re-legislate either statute.

First, Parliament should consider making a specific offence against the BNS or the IT Act, and if that is not possible, as an amendment to the IT Act criminal offences for the impersonation of a law enforcement or judicial body using ‘electronic or digital means’ for the purpose of extortion, and the sentencing band reflect the harm of the abuse of state authority – as a crime – rather than as an aggravated incident of ordinary cheating or forgery. This would fill the definitional void mentioned in part IV. Move to a single, focused charge, rather than a collection of “borrowed” provisions, from C and give prosecutors that one charge.

Second, it is important to append a harmonisation schedule to the BNS, the Bharatiya Nagarik Suraksha Sanhita, and the IT Act that specifies one reconciled classification of cognizability, bailability and applicable sentencing ceiling, for the most commonly charged together offences, Sections 318/319 BNS and Sections 66/66C/66D of the IT Act. This would eliminate the anomaly mentioned above in Part IV.B and make the prediction as it was supposed to be.

Third, the obligations on intermediaries and telecoms currently found in the Rules made under Section 79 of the IT Act should be consolidated and updated, and a statutorily fixed, short response time imposed in minutes – and the current safe harbour should be expressly contingent on compliance with that response time – for verified and time-critical requests for information which are to be directed to I4C or an equivalent notified authority for the purpose of dealing with fraud.

Fourth, the ad hoc Inter-Departmental Committee set up under the supervision of the Supreme Court ought to be made permanent in a statutory manner and members of I4C, CERT-In, RBI and DoT should be assigned a standing interlocutory coordination body with specific instructions and powers to issue binding directions on mule account freezing and cooperation between platforms; instead of having I4C in existence on the basis of a pending writ petition.

The gap in Part IV could be filled by introducing a mechanism for victims of cyber fraud to be compensated, either as part of the BNSS victim compensation system, or as a stand-alone cyber-fraud compensation fund, and financed in part by penalties recovered from convicted fraud syndicates and mule-account operators. F and putting flesh on the bones of the Ministry of Home Affairs' admission that such a framework is now being considered.

None of these five reforms calls for the wholesale re-opening of the BNS or the IT Act as complete codes; each can be tackled via focused amendment. They share an understanding that the failure to coordinate is not a necessary result of having two statutes that cover some of the same conduct, or that both statutes are incorrect. It is simply the outcome of two statutes, one passed twenty-five years before the other, without a mechanism to ensure that the statutes coordinate.

## VIII. CONCLUSION

In many ways, digital arrest scams are not new; the offences of cheating by personation, forgery and criminal intimidation have been committed since the Indian Penal Code of 1860, and prior to that, under English common law. What is new is the magnitude of the misdoing syndicates operating across borders, on mule-account networks and VoIP systems, and through forged judiciary documents which harvest crores of rupees with impunity every year, and not just through deliberate design within the framework of a statute. The gaps have surfaced and the Supreme Court, in a matter of months, has brought them into focus and caused an institutional

reaction more than the "natural functioning" of the BNS and the IT Act. But a permanent solution cannot be left languishing on the benchmark of the Supreme Court. It demands that Parliament view the need for coordination between general criminal law and specific cyber laws as a first order legislative issue that necessitates a dedicated offence, a harmonisation schedule, statutory timelines for cooperation, a standing coordination body and a compensation mechanism, as opposed to being a series of loose ends that can be tied up one by one as each new scandal lands on the Chief Justice's desk.