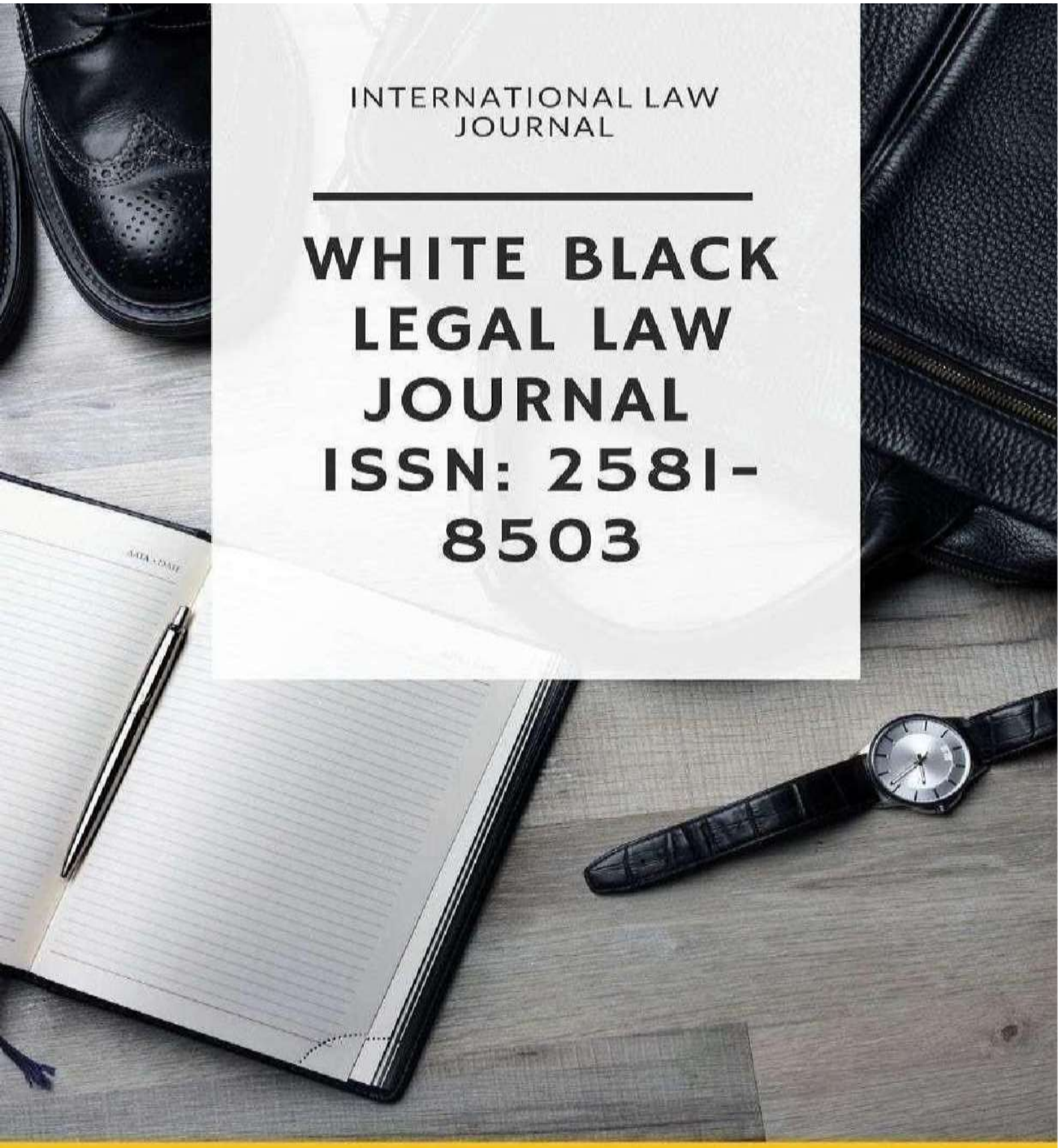

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

FRICTIONLESS TRANSFERS, FETTERED ACCOUNTS: ANALYZING THE LIABILITY OF THIRD-PARTY BENEFICIARIES IN UPI CYBER FRAUDS

AUTHORED BY - VEDIKA VYANKATESH KAMALU
B.A.LLB. 4th year,
Manikchand Pahade Law College, Chh. Sambhajinagar (MAH)

ABSTRACT

India's Unified Payments Interface (UPI) was engineered for broad financial democratization, yet its frictionless architecture has inadvertently given rise to a novel legal crisis. What happens when a network built for instant transfers becomes a weapon for unconsented financial complicity? Cybercriminals increasingly exploit this structural vulnerability by scattering illicit funds across random, unconnected UPI IDs. Fraudsters essentially conscript innocent citizens, ranging from university students to local vendors, as unwitting money mules without their knowledge or permission. Turning then to the statutory response, law enforcement agencies routinely rely on the blunt instrument of Section 106 of the Bharatiya Nagarik Suraksha Sanhita (BNSS) to initiate sweeping, blanket debit freezes on any account that merely touched the tainted funds. This brings us to a critical contradiction in the law. A penal framework designed to paralyze criminal syndicates instead paralyzes the livelihoods of legitimate third-party beneficiaries, mirroring the devastating mass account freezes that recently crippled MSMEs across Gujarat and Telangana. Instantly, the burden of proof violently shifts to the unconsenting receiver, forcing them to fight complex jurisdictional and bureaucratic hurdles to reclaim their financial autonomy. Existing scholarship largely fixates on prosecuting the architects of cyber fraud and enforcing intermediary compliance, leaving a profound legislative vacuum regarding the rights of the accidental recipient. Consequently, this paper conducts a doctrinal analysis of current penal statutes and banking regulations to expose the inadequacies of the state's existing approach. By dissecting the mechanics of these forced digital transfers, the article ultimately proposes pragmatic statutory safeguards, advocating for tier-based lien mechanisms and strict "reversal without penalization" protocols to protect unwitting beneficiaries from disproportionate state overreach.

Keywords: *Unified Payments Interface (UPI); Cyber Fraud Liability; Section 106 BNSS; Unwitting Money Mules; Blanket Account Freezes; Digital Jurisprudence; Third-Party Beneficiaries.*

I. INTRODUCTION: THE UNINTENDED MONEY MULES

How does a system designed for absolute financial democratization become a trap for the unwary? India's Unified Payments Interface (UPI) has undeniably revolutionized digital finance by handling billions of transactions with frictionless ease.[1] Yet, beneath a highly celebrated digital architecture lies a profound legislative blind spot. Criminal syndicates have learned to weaponize the very speed and accessibility that make the network so successful. By scattering fractional amounts of illicitly obtained funds across hundreds of unconnected, randomly selected UPI IDs, fraudsters effectively turn innocent citizens into unwitting money mules. A university student paying for coffee or a local merchant accepting a quick settlement suddenly finds themselves at the center of a sprawling cybercrime investigation.

Such a crisis was recently thrust into the national spotlight during parliamentary proceedings, serving as the primary genesis for this research. Rajya Sabha MP Govind Dholakia championed this issue[2] after witnessing its destructive real-world impact, highlighting a terrifying reality regarding our digital payments' ecosystem. He observed that India currently lacks a dedicated statutory framework to dictate liabilities when a person unwillingly receives tainted funds. Lawmakers correctly pointed out that the advent of UPI brought this specific vulnerability, leaving ordinary citizens completely defenceless against unconsented digital receipts. Immediate administrative reflexes to such fraud usually involve initiating a blanket debit freeze on any account that touched the disputed money. Consider the recent sweeping account freezes targeting diamond traders and MSMEs in Surat, Gujarat;[3] thousands of legitimate businesses were financially paralyzed simply because their QR codes received fractional payments linked to a distant cyber scam.

This brings us to a critical contradiction in the law. Current penal statutes, specifically Section

[1] National Payments Corporation of India, *UPI Product Statistics* (2024)
[2] *Cyber Fraudsters Misusing UPI; Govt Must Formulate Strict Law to Punish Them: BJP MP in RS*, THE ECON. TIMES (Feb. 9, 2024), https://economictimes.indiatimes.com/news/india/cyber-fraudsters-misusing-upi-govt-must-formulate-strict-law-to-punish-them-bjp-mp-in-rs/articleshow/107555132.cms.
[3] *Surat Traders Face Heat as Bank Accounts Frozen Over Suspicious UPI Transfers*, THE HINDU (Jan. 12, 2024), https://www.thehindu.com/news/national/gujarat/surat-traders-face-heat-as-bank-accounts-frozen.

106 of the Bharatiya Nagarik Suraksha Sanhita (BNSS),[4] grant law enforcement broad powers to seize property suspected to be the proceeds of a crime.[5] Applying such a blunt instrument to the hyper-connected web of digital finance, however, creates a dangerous presumption of guilt. State authorities place the onus entirely on the unwitting receiver to prove they did not solicit the funds, marking a violent shift in the burden of proof that forces a victim to fight through complex bureaucratic hurdles across state lines. Why should an innocent third party bear the punitive weight of an offense they had no part in orchestrating?

Turning then to the jurisprudential aspect, existing literature predominantly focuses on prosecuting the actual cybercriminals and enforcing the compliance obligations of banking intermediaries. Academic scholarship almost completely ignores the collateral damage inflicted on innocent third parties, thereby failing to address the statutory vacuum that leaves unconsenting recipients of tainted funds legally exposed. To understand the mechanics of this legislative failure, the following research relies on a doctrinal analysis of the BNSS, the Information Technology Act,[6] and recent regulatory responses from the Reserve Bank of India.[7] Dissecting the anatomy of unconsented digital transfers will demonstrate how technological efficiency has radically outpaced our legal safeguards. Subsequent sections will ultimately argue for a nuanced, tier-based liability framework that protects the unwitting beneficiary without compromising the broader pursuit of digital justice.

II. THE ANATOMY OF UNCONSENTED TRANSFERS

To grasp the severity of this statutory vacuum, one must first dissect the exact mechanics of modern digital layer-laundering. How does a legitimate local vendor suddenly become an accessory to a multi-state cybercrime? Financial networks engineered for absolute convenience inherently strip away the friction that once served as a natural barrier to fraud. Much like the unprecedented velocity of the GameStop short squeeze[8] or the immediate market tremors following Elon Musk's Twitter and Tesla disclosures,[9] digital financial ecosystems react in milliseconds, often leaving regulatory bodies struggling to catch up. Cyber syndicates exploit

[4] Bharatiya Nagarik Suraksha Sanhita, 2023, § 106
[5] *See* State of Maharashtra v. Tapas D. Neogy, (1999) 7 S.C.C. 685 (India).
[6] Information Technology Act, 2000
[7] *See, e.g.*, Reserve Bank of India, *Master Direction on Digital Payment Security Controls*, RBI/2020-21/74 (Issued Feb. 18, 2021).
[8] Matt Phillips & Taylor Lorenz, *'Dumb Money' Is on GameStop, and It's Beating Wall Street at Its Own Game*, N.Y. TIMES (Jan. 27, 2021), https://www.nytimes.com/2021/01/27/business/gamestop-wall-street-bets.html.
[9] Dave Michaels, *Elon Musk's Tweets Keep Testing the SEC*, WALL ST. J. (Nov. 8, 2021), https://www.wsj.com/articles/elon-musk-tweets-sec-tesla-11636405520.

this exact latency-free environment to execute complex dispersal strategies before authorities can even register a formal complaint.

Consider the mechanical reality of a standard UPI transfer. Pushing funds requires nothing more than a ten-digit mobile number or a hastily scanned QR code, entirely bypassing any requirement for the recipient to actively consent to the inbound credit.[10] Criminals have aggressively weaponized this structural design flaw. Upon executing a successful phishing attack or social engineering scam,[11] the perpetrators rarely retain the stolen capital in a single, easily traceable repository. Keeping the proceeds centralized would be a catastrophic operational failure on their part. Instead, they deploy automated networks to fracture the primary sum into dozens, sometimes hundreds, of micro-transactions.[12]

Why would a criminal enterprise send stolen money to a complete stranger? The objective is deliberate obfuscation through overwhelming volume. Shifting focus to the practical execution of these frauds, syndicates intentionally pollute the money trail by injecting illicit funds into the legitimate financial streams of everyday citizens. A university student might discover a random, unexplained credit of ₹800 in their account, likely shrugging it off as a mistaken transfer from an acquaintance. A neighbourhood grocery store might receive a fractional payment via their merchant QR code during a busy evening rush, completely unaware of its origin. These individuals possess absolutely no *mens rea* or knowledge of the underlying offense.[13] Yet, their personal bank accounts now sit squarely in the chain of custody of stolen assets.

Diving deeper into the anatomy of the operation, the syndicates eventually consolidate these fractured funds. They might utilize secondary layers of actual, complicit money mules to funnel the cash into cash withdrawals or unregulated crypto-exchanges.[14] However, the initial wave of unconsented transfers serves a highly specific, tactical purpose: exhausting law enforcement resources by creating a smokescreen of innocent actors. When a victim finally reports the

[10] National Payments Corporation of India, *Unified Payments Interface (UPI) Procedural Guidelines* § 4.2 (2022).
[11] Reserve Bank of India, *Booklet on Modus Operandi of Financial Fraudsters* 12–14 (2022).
[12] Financial Action Task Force [FATF], *Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems* 22 (June 18, 2008).
[13] K.D. GAUR, CRIMINAL LAW: CASES AND MATERIALS 45–48 (8th ed. 2015).
[14] *See* Chainalysis, *The 2023 Crypto Crime Report* 45 (2023).

original cybercrime to the National Cyber Crime Reporting Portal (NCRP),[15] the investigating officer faces an immediate labyrinth of interconnected transactions spanning multiple states and jurisdictions.

Faced with this sprawling web of digital ledgers, police cyber cells rely on automated tracing protocols that flag every single account touched by the tainted money.[16] The tracing algorithm makes absolutely no legal distinction between the mastermind orchestrating the fraud and the innocent student who unwittingly received a fragmented deposit. Consequently, the state treats the unconsenting recipient exactly the same as the active co-conspirator. The sheer speed of the UPI architecture, widely celebrated for driving India's economic modernization, thus becomes the exact mechanism that ensnares the innocent, setting the stage for the draconian statutory overreach we see today.

III. STATUTORY OVERREACH: THE BLANKET FREEZE PROTOCOL

How does law enforcement respond to the instantaneous, multi-layered dispersal of stolen funds? Faced with overwhelming transaction volumes, investigating agencies instinctively turn to the broadest legal tool at their disposal. Section 106 of the Bharatiya Nagarik Suraksha Sanhita (BNSS), which continues the legacy of Section 102 of the Criminal Procedure Code[17], empowers police officers to seize any property suspected of being stolen or found under circumstances that create suspicion of the commission of an offense. Drafted long before the advent of instantaneous digital ledgers, this provision was originally intended for physical contraband or distinctly identifiable stolen assets. Applying such a blunt, analogue statute to the hyper-connected web of UPI micro-transactions creates immediate legal friction. State cyber cells routinely interpret a fractional digital credit from a tainted source as sufficient grounds to classify the recipient's entire bank account as suspicious property.[18]

Shifting focus to the operational reality, the crisis unfolds rapidly once a primary victim registers a complaint on the National Cyber Crime Reporting Portal (NCRP). Investigating authorities do not pause to differentiate between the criminal mastermind and the unwitting recipient downstream. They issue sweeping notices under the BNSS to banking intermediaries,

[15] *National Cyber Crime Reporting Portal*, MINISTRY OF HOME AFF., www.cybercrime.gov.in (last visited Mar. 14, 2026).
[16] *See generally* Pavan Duggal, CYBERLAW - THE INDIAN PERSPECTIVE 210 - 12 (2018).
[17] Code of Criminal Procedure, 1973, § 102
[18] *see* Swaran Sabharwal v. Comm'r of Police, 1987 (13) D.R.J. 294 (India).

demanding immediate debit freezes on every single account appearing in the transaction chain. Can a local merchant realistically be expected to conduct a forensic financial audit on every hundred-rupee scan-and-pay settlement they receive during peak business hours? Holding an innocent third party strictly liable for the origin of inbound digital funds fundamentally contradicts the basic tenets of criminal jurisprudence, which heavily rely on establishing *mens rea* or guilty intent.[19] Yet, the current police mechanism operates on an automated, algorithmic presumption of guilt by association.[20]

Examining the punitive nature of these administrative actions reveals a glaring lack of proportionality. When an investigating officer flags a specific UPI transaction, banks rarely restrict the lien exclusively to the disputed amount. Financial institutions almost universally execute a blanket debit freeze to ensure total compliance, completely paralyzing the account holder's entire life savings over what might be a negligible tainted deposit. A university student holding fifty thousand rupees for upcoming tuition payments suddenly finds their funds entirely inaccessible because they unknowingly received an unprompted five-hundred-rupee credit from a compromised ID. Such draconian enforcement destroys livelihoods and shatters public trust in the digital banking ecosystem.[21] The state essentially sacrifices the financial autonomy of the innocent merely to secure a fragmented piece of evidence.

Moving toward the jurisprudential vacuum, courts have struggled to reconcile these aggressive police action with the fundamental rights of bona fide third parties. While higher judiciary bodies have occasionally intervened to unfreeze accounts upon establishing the clear lack of complicity,[22] these rulings remain reactive, localized, and financially exhausting to obtain. India lacks a binding, uniform statutory directive that explicitly protects the unconsenting recipient[23] from these arbitrary seizures. The burden of initiating litigation falls heavily on the victimized account holder, who must often travel across state lines to appear before the specific cyber cell that issued the original freeze order. This geographical and bureaucratic nightmare essentially operates as a severe punishment for a crime the individual never committed, highlighting the urgent need for a modernized legal framework.

[19] RATANLAL & DHIRAJLAL, THE INDIAN PENAL CODE 142 (36th ed. 2019)
[20] Apar Gupta, *Automated Policing and its Discontents*, 51 ECON. & POL. WKLY. 14, 16 (2016).
[21] *Cyber Cells Freezing Bank Accounts of Innocent People, Allege Traders*, THE HINDU (Oct. 12, 2023), https://www.thehindu.com/news/cities/Hyderabad/cyber-cells-freezing-bank-accounts-of-innocent-people-allege-traders/article67411649.ece.
[22] *See, e.g.*, Mukesh v. State of Gujarat, (2023) 3 G.L.R. 2101 (India).
[23] R.K. Singh, *Digital Frauds and Statutory Voids*, 45 J. INDIAN L. INST. 312, 318 (2022).

IV. THE BURDEN OF PROOF AND THE INNOCENT BENEFICIARY

How does a citizen successfully prove a negative? Under the traditional tenets of criminal jurisprudence, the state bears the absolute responsibility of establishing a suspect's guilt beyond a reasonable doubt.[24] The digital payments ecosystem, however, operates under a violently inverted reality. When a cyber cell initiates a blanket account freeze under the BNSS, the procedural friction acts as an immediate, pre-trial financial conviction. Law enforcement freezes the assets first and asks questions later, entirely shifting the evidentiary burden onto the shoulders of the unwitting recipient.

Stepping into the procedural labyrinth of unfreezing an account reveals a system engineered for administrative convenience rather than justice. Once a lien is marked, the bank immediately washes its hands of the dispute, directing the bewildered customer to contact the specific investigating officer who issued the order. Geography instantly becomes a weapon against the innocent. A street vendor in Assam might discover that their life savings have been frozen by a local cyber police station in Kerala over a fractional ₹200 transaction. Navigating this interstate jurisdictional nightmare requires resources that ordinary citizens simply do not possess. They must somehow communicate with distant authorities, often overcoming severe language barriers, to secure a "No Objection Certificate" (NOC) to regain access to their own money.[25]

Consider the sheer evidentiary impossibility placed upon the account holder. The state requires the individual to prove that they had no prior association with the cybercriminal. Yet, the architectural design of UPI deliberately obscures the sender's identity, displaying only a virtual payment address (VPA) or a phone number. Does the law genuinely expect a busy merchant to conduct a background check on every customer who scans their QR code? The innocent beneficiary is forced to produce invoices, chat logs, or CCTV footage for transactions they likely did not even register as significant. For the average university student or daily wage earner, assembling this level of documentary defence is practically impossible.

Beneath the surface of this bureaucratic exhaustion lies a profound constitutional crisis. Article 300A of the Indian Constitution[26] strictly mandates that no person shall be deprived of their

[24] RATANLAL & DHIRAJLAL, THE LAW OF EVIDENCE 415 (27th ed. 2019).
[25] *See* Ministry of Home Affairs, *Standard Operating Procedure for Investigating Cyber Crimes* (2021).
[26] INDIA CONST. art. 300A.

property save by authority of law. A bank account represents the digital extension of a citizen's livelihood, inextricably linked to their Right to Life under Article 21.[27] Paralyzing an individual's entire financial existence over a negligible, unconsented digital deposit fundamentally violates the doctrine of proportionality.[28] The state essentially sacrifices the fundamental rights of the third-party beneficiary at the altar of investigative expediency.

Compounding this judicial hurdle is the harsh economic reality of legal intervention. When police refuse to lift a blanket freeze, the only remaining recourse is to approach the judiciary. Why must a legitimate business owner hire a high court advocate to access funds they legally earned? The cost of retaining legal counsel, filing a writ petition, and fighting a multi-state jurisdictional battle almost always exceeds the actual amount of the tainted deposit. Consequently, thousands of innocent citizens abandon their frozen accounts, surrendering their hard-earned money to a broken regulatory framework. They become collateral damage in a digital war they never chose to participate in.

V. PROPOSED REGULATORY AND TECHNOLOGICAL SAFEGUARDS

Critiquing the current application of the Bharatiya Nagarik Suraksha Sanhita is legally necessary but insufficient without proposing pragmatic alternatives. How do we actually balance the aggressive pursuit of cyber syndicates with the financial liberty of the everyday citizen? The answer lies in replacing blunt statutory instruments with surgical, technology-driven regulations. Law enforcement cannot be expected to abandon their investigations, but their methods must strictly adhere to the constitutional doctrine of proportionality.

Addressing the immediate financial paralysis of victims requires a radical overhaul of how banks execute police orders. Currently, a disputed transaction of a few hundred rupees triggers a catastrophic total debit freeze. The Reserve Bank of India (RBI) must mandate a strict 'amount-specific' lien protocol across all banking intermediaries.[29] If an investigating officer flags a specific UPI credit of ₹2,000, the bank should legally be permitted to freeze only that exact sum. The remainder of the citizen's life savings must remain entirely accessible. Enforcing such a granular approach immediately neutralizes the unconstitutional deprivation of property, allowing a merchant to buy inventory or a family to cover medical expenses while

[27] INDIA CONST. art. 21.
[28] K.S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1, 312 (India).
[29] *See* B.R. Enterprises v. State of Telangana, 2022 S.C.C. OnLine T.S. 1894 (India).

the tainted ₹2,000 remains securely locked pending investigation.

Turning then to the legislative vacuum surrounding the recipient's intent, India desperately needs a statutory "Safe Harbor" provision for unconsenting beneficiaries. What happens when a person actively realizes they have received suspicious funds? Under the current regime, attempting to return the funds can further implicate them in the money trail, creating a false digital footprint of association. The National Payments Corporation of India (NPCI) should develop a standardized "reversal without penalization" protocol within the UPI architecture. If an individual receives an unverified, unprompted transfer, they should be able to flag the transaction and return the funds to a centralized, bank-managed suspense account. Executing this specific action would legally sever their liability. Such a mechanism acts as a digital shield, automatically establishing the absence of *mens rea* and explicitly protecting the citizen from subsequent police notices.

Looking strictly at the technological framework, perhaps the payment ecosystem has become entirely too frictionless for its own good. While rapid micro-dispersals are the hallmark of these cyber frauds, the network currently lacks automated circuit breakers to detect and halt them in real time. NPCI could introduce algorithmic velocity limits specifically tailored to unknown payees.[30] Imagine a scenario where a compromised account suddenly attempts to push fifty fractional payments to unconnected mobile numbers within three minutes. The system should automatically quarantine those outbound transfers. Furthermore, introducing an optional "consent to receive" toggle for transactions originating from unverified senders would drastically reduce the volume of unwitting money mules.

Re-evaluating the integration of the National Cyber Crime Reporting Portal (NCRP) is equally paramount. The platform currently functions as a blind force multiplier for state police, automatically generating freeze mandates for every single account in the ledger. It must be upgraded to categorize primary suspects versus mere transactional conduits. Refining tracing algorithms to identify terminal nodes, where syndicates withdraw or launder cash, would enable law enforcement to target the perpetrators rather than wasting resources penalizing innocent citizens who occupy intermediary branches.

[30] *See* National Payments Corporation of India, *Circular on Risk Management and Fraud Monitoring*, NPCI/UPI/OC-114/2021-22 (2021).

VI. CONCLUSION

Stepping back to view the broader ecosystem of India's digital economy, the sheer velocity of the Unified Payments Interface has fundamentally outpaced the evolution of our penal statutes. How much collateral damage is a democratic society willing to tolerate in the blind pursuit of digital security? The current legislative and administrative framework effectively answers that question by sacrificing the financial liberty of the unwitting bystander. We have engineered a payment infrastructure that celebrates absolute frictionlessness, yet we police it with the archaic, blunt force of Section 106 of the Bharatiya Nagarik Suraksha Sanhita.[31]

Moving beyond mere investigative convenience, law enforcement cannot continue treating an unconsented digital receipt as a concrete presumption of active criminal complicity. The devastating mass account freezes witnessed recently are not a sign of successful cyber policing;[32] rather, they expose a profound failure to distinguish between the architect of a fraud and their accidental money mule. Why should a legitimate local merchant or a student be forced to litigate across state lines, spending more than the disputed amount itself, simply to reclaim their own untainted funds?

Rectifying this systemic failure demands immediate statutory intervention rather than relying on piecemeal, localized judicial relief. The state must urgently replace blanket debit freezes with strict, amount-specific liens that respect the constitutional mandate of proportionality under Article 300A.[33] Furthermore, regulatory bodies like the Reserve Bank of India and NPCI must implement technological safe harbours, specifically a seamless "reversal without penalization" protocol,[34] to allow citizens to instantly sever their liability when targeted by random micro-deposits.

Ultimately, a digital economy cannot genuinely thrive if its participants live in constant fear of arbitrary financial paralysis. Protecting the innocent third-party beneficiary does not weaken the fight against cyber syndicates. It simply ensures that the heavy sword of the state strikes the actual perpetrators, rather than endlessly wounding the very citizens it was built to protect.

[31] Bharatiya Nagarik Suraksha Sanhita, *supra* note 4, at § 106.
[32] *See generally* Rahul Deodhar, *Cybercrimes and Blanket Freezing of Bank Accounts: A Call for Proportionality*, 58 ECON. & POL. WKLY. 22, 24 (2023)
[33] INDIA CONST. art. 300A. *See also* K.S. Puttaswamy v. Union of India, *supra* note 28, at 312
[34] *See* Reserve Bank of India, *Report of the Working Group on Digital Lending* 85–87 (2021)