

# SHIFTING THE BURDEN: THE LEGAL FEASIBILITY OF A SHARED INTER-BANK LIABILITY MODEL TO COMBAT UPI MULE ACCOUNTS IN INDIA

**AUTHOR – SEJEL\* & DR. VARUN SRIVASTAVA\*\***

\* LL.M. (CORPORATE, BANKING & INSURANCE LAW), AMITY LAW SCHOOL NOIDA, AMITY UNIVERSITY UTTAR PRADESH

\*\* ASSISTANT PROFESSOR AT AMITY LAW SCHOOL NOIDA, AMITY UNIVERSITY UTTAR PRADESH

**BEST CITATION –** SEJEL & DR. VARUN SRIVASTAVA, SHIFTING THE BURDEN: THE LEGAL FEASIBILITY OF A SHARED INTER-BANK LIABILITY MODEL TO COMBAT UPI MULE ACCOUNTS IN INDIA, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (7) OF 2026, PG. 209-217, APIS – 3920 – 0001 & ISSN – 2583-2344.

## ABSTRACT

*The exponential growth of the Unified Payments Interface (UPI) ecosystem in India has democratised digital financial access, yet simultaneously created fertile ground for a sophisticated category of financial crime: the mule account network. These accounts, operated by witting or unwitting intermediaries, serve as conduits through which proceeds of fraud are laundered and dissipated across the banking system before victims can seek redress. The existing legal architecture in India dispersed across the Payment and Settlement Systems Act 2007, the Prevention of Money Laundering Act 2002, the Indian Penal Code 1860 (now partially superseded by the Bharatiya Nyaya Sanhita 2023), and Reserve Bank of India circulars allocates liability in a fragmented and victim-hostile manner. This paper proposes a novel conceptual framework: a Shared Inter-Bank Liability (SIBL) model, wherein financial institutions that onboard or maintain mule accounts bear proportionate civil liability toward defrauded UPI users, irrespective of which bank originated the payment. Drawing upon the doctrines of vicarious liability, contributory negligence, and the emerging international standards of payment fraud reimbursement, this paper analyses the feasibility of such a model within Indian constitutional, statutory, and regulatory law. It argues that SIBL is not only legally defensible but is arguably compelled by the constitutional guarantee of the right to life with dignity under Article 21 and the RBI's mandate to ensure systemic integrity. The paper further examines how such a model could be operationalised through interbank settlement mechanisms, suggests legislative amendments, and confronts the principal objections from the banking sector.*

## 1. Introduction

India's digital payments landscape underwent a tectonic transformation following the launch of UPI in 2016 by the National Payments Corporation of India (NPCI). By the financial year 2024–25, UPI had processed transactions worth tens of trillions of rupees monthly, with over 400 million unique users transacting on the platform.<sup>297</sup> This extraordinary democratisation

of finance, however, has carried with it an equally extraordinary democratisation of financial crime.

Among the most pernicious forms of UPI-related fraud is the deployment of mule accounts bank accounts opened under fictitious, coerced, or purchased identities that serve as relay stations for fraudulent funds. A typical mule account chain involves an initial victim making a UPI payment to a fraudster, after which the amount is rapidly moved through three to six intermediary accounts before being withdrawn

<sup>297</sup> National Payments Corporation of India, 'UPI Product Statistics' (NPCI, 2025) — the platform recorded over 17 billion transactions in March 2025 alone, reflecting consistent year-on-year growth since 2016.

or converted into cryptocurrency, gift vouchers, or commodities. The velocity of UPI transactions near-instantaneous, 24/7, and irrevocable makes recovery nearly impossible once the funds exit the first mule account.<sup>298</sup>

The current legal framework in India offers the defrauded consumer little systemic recourse. Police complaints result in low recovery rates. Civil suits are practically unviable given the anonymity of fraudsters. The Cyber Crime Portal (cybercrime.gov.in) operated by the Ministry of Home Affairs enables complaints, but the response is inconsistent and bank cooperation is selective. Most critically, there exists no statutory mechanism that compels the bank maintaining the mule account the receiving bank, the intermediary bank, or any bank to bear liability toward the defrauded consumer. The burden of loss falls entirely on the victim.

This paper interrogates that allocation of loss and proposes that it is both legally unjustifiable and practically counterproductive. Section 2 maps the existing legal framework. Section 3 articulates the theoretical foundations of the SIBL model. Section 4 analyses its constitutional and statutory feasibility. Section 5 examines operational considerations. Section 6 confronts objections. Section 7 concludes.

## 2. The Existing Legal Framework: A Fragmented Architecture

### 2.1 The Payment and Settlement Systems Act, 2007

The Payment and Settlement Systems Act 2007 (PSSA) is the primary statute governing payment systems in India. Section 4 of the PSSA vests authority in the Reserve Bank of India to authorise and regulate payment systems. Section 18 empowers the RBI to issue directions to system participants.<sup>299</sup> Crucially, however, the PSSA contains no provision that creates direct civil liability between banks participating in a

payment system and end consumers who suffer fraud losses within that system. The Act is fundamentally regulatory in character it governs the *architecture* of payment systems but does not address the *allocation of losses* arising from fraud within those systems.

This legislative silence is not accidental; it reflects the original design assumption that fraud losses would be individualised and exceptional. In an era where UPI fraud has become systemic and industrial in scale, this assumption no longer holds.

### 2.2 The Prevention of Money Laundering Act, 2002

The Prevention of Money Laundering Act 2002 (PMLA) is relevant because mule accounts are instruments of money laundering they are used to layer and integrate the proceeds of predicate offences including cheating (under the Bharatiya Nyaya Sanhita 2023) and criminal breach of trust.<sup>300</sup> Under Section 3 of the PMLA, the offence of money laundering is committed by any person who directly or indirectly is involved in the process or activity connected with the proceeds of crime. The term 'person' under Section 2(1)(s) includes companies and, by extension, juristic entities such as banks.

The critical question is whether a bank that negligently onboards a mule account operator failing to conduct adequate Know Your Customer (KYC) verification or failing to act on red flags in transaction patterns is 'connected with' the proceeds of crime within the meaning of Section 3. No Indian court has definitively answered this question, but a purposive reading of the PMLA, consistent with the Financial Action Task Force (FATF) recommendations that India has committed to implementing, suggests that passive facilitation through wilful blindness or gross negligence is not immunised by the statute.<sup>301</sup>

<sup>298</sup> Ministry of Home Affairs, 'Annual Report of the Indian Cyber Crime Coordination Centre 2023–24' — the Report notes that funds in mule account chains are typically dissipated within 24 to 72 hours of initial deposit, making recovery through bank freezing orders practically very difficult  
<sup>299</sup> Payment and Settlement Systems Act 2007, ss 4 and 18.

<sup>300</sup> Prevention of Money Laundering Act 2002, ss 2(1)(u), 3. The definition of 'scheduled offence' in the Schedule to the PMLA includes cheating under IPC s 420 (now substantially replicated in BNS s 316) and organised crime under BNS s 111 (introduced by the 2023 codification).

<sup>301</sup> Financial Action Task Force, 'Guidance on Risk-Based Approach for the Banking Sector' (FATF, 2014) para 49 — the FATF guidance explicitly states

### 2.3 The Bharatiya Nyaya Sanhita, 2023 and the Former IPC Framework

The Bharatiya Nyaya Sanhita 2023 (BNS), which replaced the Indian Penal Code 1860 from 1 July 2024, retains and expands offences relevant to financial fraud. Section 316 of the BNS (corresponding broadly to Section 420 IPC) addresses cheating and dishonestly inducing delivery of property. Section 111 introduces the concept of organised crime, defined to include economic offences committed by a syndicate a definition that plainly captures large-scale mule account operations.<sup>302</sup>

However, criminal law in India is victim-distant in its remedial architecture. Conviction results in punishment of the accused but does not automatically result in compensation to the victim. Section 396 of the Bharatiya Nagarik Suraksha Sanhita 2023 (the procedural code) permits courts to order compensation, but this is discretionary and practically ineffective where accused persons are anonymous, insolvent, or untraced.

### 2.4 RBI Circulars and the Limited Consumer Protection Framework

The RBI has issued several circulars addressing unauthorised electronic transactions and consumer liability. The Master Circular on Customer Protection Limiting Liability of Customers in Unauthorised Electronic Payment Transactions (2017) establishes a framework under which banks must credit customers for unauthorised debit transactions, with liability limits depending on the contributory negligence of the customer.<sup>303</sup> However, this framework is designed for situations where a customer's own account is debited without authorisation. It does not address the situation where a customer voluntarily initiates a UPI payment to an

that wilful blindness to red flags in account management can constitute participation in money laundering within the meaning of FATF Recommendation 3.

<sup>302</sup> Bharatiya Nyaya Sanhita 2023, s 111 — defines 'organised crime' to include a 'continuing unlawful activity' carried out by a syndicate, which encompasses systematic mule account networks established for the purpose of laundering proceeds of fraud.

<sup>303</sup> Reserve Bank of India, 'Master Circular — Customer Protection' (n 1) — the framework distinguishes liability based on reporting timeline and contributory negligence but does not address authorised push payment fraud.

account that turns out to be a mule a fraud-induced authorised push payment. The distinction between unauthorised transactions and authorised-but-fraudulently-induced push payments is a critical lacuna in Indian consumer financial protection law.

### 2.5 The Lacuna: Authorised Push Payment Fraud

Authorised Push Payment (APP) fraud where a victim is deceived into authorising a payment is the dominant form of UPI fraud in India. Unlike unauthorised debit fraud, where the bank's duty to the customer is well-established, APP fraud occupies a doctrinal grey zone. The customer did press 'pay'; the bank processed a technically legitimate instruction. Under the current framework, the bank owes no duty to the customer beyond executing the payment accurately. The receiving bank which holds the mule account bears no liability whatsoever toward the defrauded sender. This allocation of loss is the central injustice that the SIBL model seeks to correct.

## 3. The Shared Inter-Bank Liability Model: Theoretical Foundations

### 3.1 Conceptual Architecture

The SIBL model proposed in this paper rests on a simple but powerful premise: where fraud occurs within a shared payment ecosystem, all institutional participants who benefit from that ecosystem and whose negligence contributes to the fraud should bear proportionate liability. Applied to UPI mule account fraud, this translates into a framework where:

(a) The *receiving bank* (the bank maintaining the mule account) bears primary liability if it failed to conduct adequate KYC at account opening or failed to flag anomalous transaction patterns consistent with mule activity;

(b) The *sending bank* bears secondary liability if it failed to deploy adequate fraud detection alerts before processing a high-risk transaction;

(c) The *NPCI* as system operator bears residual liability if it failed to implement or enforce

system-level velocity checks and mule account detection mechanisms; and

(d) These liabilities are apportioned in a predetermined ratio and subject to reimbursement from a *Shared Fraud Compensation Pool* (SFCP) maintained by participating banks under RBI supervision.

The SIBL model does not eliminate individual criminal liability of the mule account operator or the masterfraud syndicate. It creates a parallel civil liability track that ensures the defrauded consumer receives swift compensation while the institutional backstop system conducts its own investigation and recovery.

### 3.2 Doctrinal Foundations in Indian Law

#### 3.2.1 Contributory Negligence and Proportionate Fault

The doctrine of contributory negligence recognised in Indian tort law through a series of High Court and Supreme Court decisions permits apportionment of loss where multiple parties share fault.<sup>304</sup> In the context of UPI mule fraud, the receiving bank's failure to conduct adequate due diligence during account opening or to act on transaction monitoring alerts is a form of contributory negligence. The bank's negligence does not cause the fraud in a direct sense, but it facilitates the fraud by providing the fraudster's instrumentality: the account itself. Under Indian negligence law, as crystallised in *Jacob Mathew v State of Punjab*,<sup>305</sup> liability attaches where there is a duty of care, breach of that duty, causation, and damage. Each of these elements can be established against a receiving bank that maintains a mule account with inadequate oversight.

<sup>304</sup> See for instance *Municipal Corporation of Delhi v Subbagnvanti* AIR 1966 SC 1750 — the Supreme Court applied principles of proportionate fault allocation in tort claims involving multiple parties.

<sup>305</sup> *Jacob Mathew v State of Punjab* (2005) 6 SCC 1 [48] — the Court articulated the classic negligence elements applicable in Indian tort law: duty, breach, causation, and damage.

#### 3.2.2 The Banker's Duty of Care and Fiduciary Obligations

Indian banking law recognises that the banker-customer relationship is not merely contractual but also carries dimensions of a fiduciary duty in specific contexts.<sup>306</sup> The Supreme Court in *Canara Bank v United India Insurance Co Ltd*<sup>307</sup> held that banks owe duties of care that extend beyond their immediate contractual obligations in circumstances where third-party reliance on their conduct is foreseeable. A bank that onboards a mule account operator creates a foreseeable risk of loss to all future UPI senders who are deceived into transacting with that account. The foreseeability requirement is satisfied: mule account fraud is a well-documented, statistically significant, and institutionally known risk.

#### 3.2.3 Unjust Enrichment

There is also a residual claim grounded in the principle against unjust enrichment. Under Section 70 of the Indian Contract Act 1872, where a person lawfully does something for another person or delivers anything, and the other person enjoys the benefit, the latter is bound to compensate the former or restore the thing. A bank that receives fraudulent deposits into a mule account, earns float income on those deposits, and charges transaction fees for onward transfers has, in a juristic sense, received a benefit from the fraud. The unjust enrichment argument does not require proof of the bank's bad faith; it requires only proof that the bank received and retained a benefit attributable to the fraudulent transaction chain.

#### 3.3 International Analogues

The United Kingdom's Contingent Reimbursement Model (CRM) Code, introduced in 2019 and subsequently given statutory force under the Payment Systems Regulator's mandatory APP fraud reimbursement rules

<sup>306</sup> See PN Varshney, *Banking Law and Practice* (22nd edn, Sultan Chand 2022) ch 4 — discusses the hybrid contractual-fiduciary character of the banker-customer relationship in Indian law.

<sup>307</sup> *Canara Bank v United India Insurance Co Ltd* AIR 1993 SC 2884 — the Court held that banks owe extended duties of care where third-party reliance is foreseeable.

effective October 2024, provides the closest international parallel.<sup>308</sup> Under the UK model, sending and receiving Payment Service Providers (PSPs) share the cost of reimbursing APP fraud victims equally 50:50 unless the victim acted with gross negligence. The Financial Conduct Authority's equivalent rules have created a powerful incentive for banks to invest in fraud prevention, since their liability exposure is now directly linked to their fraud management performance. The Indian SIBL model draws inspiration from this architecture but adapts it to the distinctive features of the UPI ecosystem, including the multilateral settlement structure, the role of NPCI as a quasi-regulatory operator, and the specific vulnerabilities of India's customer base.

#### 4. Constitutional and Statutory Feasibility

##### 4.1 Article 21 and the Right to Financial Dignity

The Supreme Court of India has progressively expanded the scope of Article 21 of the Constitution the right to life and personal liberty to encompass dimensions of human dignity, livelihood, and economic security. In *Olga Tellis v Bombay Municipal Corporation*,<sup>309</sup> the Court held that the right to livelihood is integral to the right to life. In *Consumer Education and Research Centre v Union of India*,<sup>310</sup> the Court held that the right to life includes the right to protection against economic exploitation.

The proliferation of UPI fraud represents, for millions of Indians particularly those in the economically vulnerable segments who have recently entered the digital banking system a direct threat to economic security and livelihood. Where the State, through its licensed banking institutions, creates and operates a payment infrastructure that systematically exposes citizens to uncompensated fraud loss, a credible argument arises that the failure to

impose liability on negligent institutional participants constitutes a violation of the positive dimension of Article 21. The SIBL model, if enacted by legislation, would be a fulfilment of this positive constitutional obligation.

##### 4.2 Feasibility Under the Banking Regulation Act, 1949

The Banking Regulation Act 1949 (BRA) governs the conduct of banking companies in India. Section 35A empowers the RBI to issue directions to banking companies in the public interest or in the interest of banking policy or to prevent the affairs of any banking company from being conducted in a manner detrimental to the interests of depositors. The language of Section 35A is broad enough to support an RBI direction requiring banks to participate in a Shared Fraud Compensation Pool. The requirement to maintain a proportionate contribution to such a pool is analogous to the requirement to maintain a statutory liquidity ratio or capital adequacy a prudential requirement justified by systemic risk management.<sup>311</sup>

Further, Section 36 of the BRA empowers the RBI to caution or prohibit banking companies from entering into any particular transaction or class of transactions. Read together, Sections 35A and 36 provide a robust statutory foundation for RBI directions that could give operational form to the SIBL model without requiring primary legislation, though primary legislation would be preferable for reasons of legal certainty and democratic legitimacy.

##### 4.3 Feasibility Under the Payment and Settlement Systems Act, 2007

As noted above, the PSSA confers broad regulatory powers on the RBI over payment systems. Section 18 of the PSSA allows the RBI to issue directions to a 'system participant' defined under Section 2(1)(p) to include banks, financial institutions, and payment intermediaries regarding the conduct of

<sup>308</sup> Payment Systems Regulator (UK), 'APP Scams: Mandatory Reimbursement' (PS23/3, December 2023) — established the 50:50 liability split between sending and receiving PSPs, effective October 2024.

<sup>309</sup> *Olga Tellis v Bombay Municipal Corporation* (1985) 3 SCC 545 [32] — the Court held that the right to livelihood is an essential component of Article 21.

<sup>310</sup> *Consumer Education and Research Centre v Union of India* (1995) 3 SCC 42 [24] — the Court extended Article 21 protection to cover the right against economic exploitation in the context of organised consumer harm.

<sup>311</sup> Banking Regulation Act 1949, s 35A — the breadth of this provision has been upheld in numerous decisions, including *All India Bank Officers' Confederation v Union of India* (2005) 2 SCC 1.

payment systems. An RBI direction under Section 18 could require system participants to:

- (a) Implement enhanced due diligence protocols for account opening in high-risk categories;
- (b) Maintain real-time transaction monitoring for mule account indicators;
- (c) Contribute to a centralised SFCP administered by NPCI; and
- (d) Report to a central fraud data repository to enable cross-bank identification of mule networks.

The constitutionality of such directions under the PSSA would be assessed under Article 19(6) of the Constitution, which permits reasonable restrictions on the right to carry on any trade or profession in the interests of the general public. Given the demonstrably enormous scale of UPI mule fraud and its disproportionate impact on economically vulnerable consumers, a proportionality analysis would likely sustain such restrictions as reasonable.

#### 4.4 Proposed Legislative Amendments

For the SIBL model to operate with full legal certainty, this paper proposes the following legislative insertions:

**Amendment to PSSA 2007:** Insert a new Section 23A titled 'Liability of system participants in cases of payment fraud,' providing that where a payment is made through an authorised payment system pursuant to fraudulent inducement, and the receiving account is subsequently identified as a mule account, the system participant maintaining such account shall be primarily liable to the aggrieved payer for reimbursement, subject to defences of due diligence and absence of negligence, and the quantum of such liability shall be determined by regulations made under Section 38.

**Amendment to Banking Regulation Act 1949:** Insert a new sub-section to Section 35A providing that the RBI may, by directions, require banking companies to contribute to a Shared Fraud Compensation Pool and may specify the

conditions under which disbursements from such pool shall be made to aggrieved customers.

**Amendment to Information Technology Act 2000:** Insert a new Section 66F (replacing the existing provision) to specifically criminalise the knowing or reckless provision of one's bank account for use as a mule account, with enhanced penalties where a financial institution's KYC failure is found to have enabled the criminal use.

### 5. Operationalising the SIBL Model

#### 5.1 The Shared Fraud Compensation Pool

The operational heart of the SIBL model is the Shared Fraud Compensation Pool (SFCP). This pool would function as follows. Each bank participating in the UPI ecosystem would contribute to the SFCP at a rate proportionate to its UPI transaction volume and its historical mule account incidence rate creating a direct financial incentive for banks to reduce their mule account exposure. The pool would be administered by NPCI, which already operates the technical infrastructure of UPI and has access to real-time transaction data. Disbursements from the pool to defrauded consumers would be made within a prescribed period proposed as 10 working days upon submission of a fraud complaint to the originating bank, subject to a preliminary threshold assessment.<sup>312</sup>

The SFCP model draws upon the existing structure of the Deposit Insurance and Credit Guarantee Corporation (DICGC), which provides insurance to depositors of insured banks through a pooled fund mechanism under the Deposit Insurance and Credit Guarantee Corporation Act 1961. The legal architecture for mandatory pooled bank contributions for consumer protection already exists in Indian law; the SIBL model extends this architecture to the fraud compensation context.

<sup>312</sup> The 10-working-day disbursement period is proposed by analogy with the RBI's existing mandate for provisional credit in unauthorised debit cases under the 2017 Master Circular (n 7), adapted for the APP fraud context.

## 5.2 Fraud Intelligence Sharing and the Central Mule Account Registry

A functional SIBL model requires an informational infrastructure that does not yet exist in India in adequate form. This paper proposes the creation of a Central Mule Account Registry (CMAR) a shared database maintained by NPCI and accessible to all participating banks that would flag accounts exhibiting mule account indicators in real time. These indicators would include: unusually high transaction velocity shortly after account opening; multiple inward and immediate outward transfers without corresponding credit activity; geographic mismatches between account registration and transaction location; and accounts linked to mobile numbers or devices associated with known fraud complaints.<sup>313</sup>

The legal basis for such data sharing would require careful navigation of the Digital Personal Data Protection Act 2023 (DPDPA). Under Section 7 of the DPDPA, processing of personal data for a legitimate purpose is permissible, and Section 7(b) permits processing necessary for compliance with a legal obligation under Indian law. A statutory or regulatory requirement to contribute account data to the CMAR for fraud prevention purposes would satisfy the legitimate purpose and legal obligation gateways, provided appropriate data minimisation and access control safeguards are in place.

## 5.3 Liability Apportionment Formula

Under the proposed SIBL model, liability would be apportioned between the receiving bank (which maintained the mule account), the sending bank (which processed the payment), and NPCI (in its capacity as system operator) in the following baseline proportions: 60:25:15. This apportionment reflects the relative causal proximity of each participant to the fraud. The receiving bank, which created the instrument of

fraud through negligent onboarding, bears the primary burden. The sending bank, which could have deployed stronger pre-transaction fraud alerts, bears a secondary burden. NPCI, as the system-level operator responsible for setting and enforcing fraud prevention standards, bears a residual systemic contribution.

These proportions would be subject to adjustment where a bank demonstrates that it complied fully with all prescribed due diligence standards reducing its liability share or where a bank is found to have had actual knowledge of mule activity increasing its liability share up to 100% in cases of wilful facilitation.

## 5.4 Subrogation and Recovery Rights

Upon compensating the defrauded consumer from the SFCP, the Pool would be subrogated to the consumer's rights against the fraudster, the mule account operator, and any other parties. This creates a well-resourced institutional plaintiff NPCI or the SFCP administrator with both the legal standing and the financial incentive to pursue recovery actions, including applications under the PMLA for attachment of proceeds of crime. The subrogation mechanism transforms what are currently scattered and ineffective individual recovery attempts into a coordinated institutional enforcement effort.

## 6. Principal Objections and Responses

### 6.1 The Moral Hazard Objection

The primary objection anticipated from the banking sector is moral hazard: if banks are required to compensate victims of fraud regardless of fault, they will have reduced incentives to invest in fraud prevention. This objection mischaracterises the SIBL model. The model explicitly ties liability exposure to the receiving bank's due diligence performance a bank that maintains rigorous KYC and real-time monitoring, and can demonstrate compliance with prescribed standards, benefits from a reduced liability share or a due diligence defence that can eliminate its liability entirely. The incentive structure is therefore fraud-prevention positive, not neutral. The analogy to

<sup>313</sup> These indicators are derived from the RBI's 'Report of the Committee on Digital Payments' (January 2019) and the Financial Intelligence Unit's typologies on mule account-based money laundering.

motor insurance is instructive: mandatory third-party insurance does not reduce drivers' incentives to drive safely; the combination of no-claims bonuses, excess provisions, and premium risk pricing creates a financial incentive structure that rewards safe behaviour.

### 6.2 The Definitional Uncertainty Objection

A second objection concerns the difficulty of definitively identifying a 'mule account.' Fraud syndicates are adaptive; they continuously evolve account behaviours to evade detection. This objection has merit as a practical challenge but does not defeat the SIBL model as a legal proposition. The liability framework does not require proof that an account is a mule account in a criminal law sense; it requires proof, on the civil standard of balance of probabilities, that the bank's onboarding and monitoring of the account fell below the prescribed due diligence standard. The causal link is to the bank's negligence, not to the account's formal classification.

### 6.3 The Constitutional Validity of Compelled Pool Contribution

A third objection is that compelling banks to contribute to a compensation pool constitutes an unreasonable restriction on their right to carry on business under Article 19(1)(g) of the Constitution. As noted in Section 4.3, such restrictions must satisfy the proportionality test under Article 19(6). Given the scale of UPI fraud estimated at thousands of crores of rupees annually and the documented failure of existing voluntary and fragmented approaches, a compelled contribution mechanism serving the public interest in consumer financial protection would satisfy the proportionality standard.<sup>314</sup> The Supreme Court's decision in *Cellular Operators Association of India v Telecom Regulatory Authority of India*<sup>315</sup>

confirms that regulatory impositions on commercially significant participants in licensed industries are subject to a relatively deferential proportionality review where the regulatory objective is consumer protection.

### 6.4 The NPCI Liability Objection

NPCI may object that imposing systemic liability on it as a payment system operator a non-profit entity operating under the regulatory aegis of the RBI is neither legally supportable nor practically viable. This paper's response is that NPCI's liability contribution under the SIBL model is modest (15%) and is specifically tied to its failure to perform *system-level* fraud prevention functions rather than individual transaction monitoring. NPCI's institutional position as the operator of India's most critical payment infrastructure places it in a relationship of proximity to the harms caused by mule account fraud that is sufficient to ground a duty of care in tort. This is consistent with the principle articulated by the Supreme Court in *M.C. Mehta v Union of India*<sup>316</sup> that entities which operate activities with high potential for public harm bear elevated duties of care.

### 7. Conclusion

The proliferation of UPI mule accounts represents one of the most consequential and under-examined structural failures of India's digital financial ecosystem. The existing legal framework built upon statutes designed for a pre-digital financial order and circulars that are consumer-protective in form but practically ineffective in their current scope leaves the burden of fraud loss almost entirely on those least equipped to bear it: the individual defrauded consumer.

The Shared Inter-Bank Liability model proposed in this paper offers a legally grounded, practically operationalisable, and

<sup>314</sup> The precise scale of UPI fraud losses in India is not definitively published in a single official source; estimates from the RBI Annual Report 2023–24 and MHA cybercrime statistics suggest aggregate losses in the thousands of crores annually, though underreporting means actual losses are likely substantially higher.

<sup>315</sup> *Cellular Operators Association of India v Telecom Regulatory Authority of India* (2016) 7 SCC 703 [60]–[70] — the Court applied a deferential proportionality

standard to regulatory impositions on licensed telecom operators serving consumer protection objectives.

<sup>316</sup> *M C Mehta v Union of India* (1987) 1 SCC 395 [10] — in the context of the absolute liability rule, the Court held that enterprises engaged in activities with high potential for public harm bear duties commensurate with that risk.

constitutionally consistent mechanism for redistributing that burden. By harnessing the existing doctrines of contributory negligence, the statutory powers of the RBI under the PSSA and the Banking Regulation Act, the constitutional imperative of Article 21, and the international precedent of APP fraud reimbursement regimes, the SIBL model creates a framework in which the negligence of institutional participants in the UPI ecosystem is internalised rather than externalised onto victims.

This paper does not claim that SIBL will eliminate UPI mule fraud. Fraud is adaptive and institutional measures will always face the challenge of adversarial evolution. What SIBL can achieve is the transformation of the incentive structure within the banking system making fraud prevention a direct financial priority rather than a compliance formality and the provision of meaningful, swift recourse to consumers who suffer fraud losses through no fault of their own. In a country where digital payments have been positioned as an instrument of financial inclusion and economic empowerment, the credibility of that promise depends upon the existence of meaningful legal protection when the system is abused. The SIBL model is a step toward making that protection real.

Payment and Settlement Systems Act 2007

Prevention of Money Laundering Act 2002

#### Cases

*Canara Bank v United India Insurance Co Ltd*  
AIR 1993 SC 2884

*Cellular Operators Association of India v Telecom Regulatory Authority of India* (2016) 7 SCC 703

*Consumer Education and Research Centre v Union of India* (1995) 3 SCC 42

*Jacob Mathew v State of Punjab* (2005) 6 SCC 1

*M C Mehta v Union of India* (1987) 1 SCC 395

*Olga Tellis v Bombay Municipal Corporation* (1985) 3 SCC 545

#### Regulatory Instruments

Reserve Bank of India, 'Master Circular Customer Protection Limiting Liability of Customers in Unauthorised Electronic Payment Transactions' (RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18, 6 July 2017)

Reserve Bank of India, 'Master Direction Know Your Customer Direction 2016' (as updated)

#### BIBLIOGRAPHY

##### Primary Sources

##### Legislation

Banking Regulation Act 1949

Bharatiya Nagarik Suraksha Sanhita 2023

Bharatiya Nyaya Sanhita 2023

Constitution of India 1950

Deposit Insurance and Credit Guarantee Corporation Act 1961

Digital Personal Data Protection Act 2023

Indian Contract Act 1872

Information Technology Act 2000