BEYOND ZERO LIABILITY: RE-EXAMINING CUSTOMER PROTECTION AND BANK ACCOUNTABILITY FOR CYBER FRAUD UNDER THE RBI'S 2017 FRAMEWORK AND ITS 2026 REFORMS

Kairavi Jain, Symbiosis Law School, Pune,
Symbiosis International (Deemed University), India

ABSTRACT

India's rapid migration onto digital payment rails has been matched, almost step for step, by the growth of cyber-enabled financial fraud, leaving courts, regulators and consumer forums to work out who bears the loss when a transaction is authenticated by a machine but never truly authorised by the account holder. This paper revisits the liability architecture created by the Reserve Bank of India's circular of 6 July 2017 on Customer Protection - Limited Liability of Customers in Unauthorised Electronic Banking Transactions, and asks whether its promise of tiered, fault-based liability has produced consistent outcomes in practice. Drawing on a doctrinal reading of the Circular alongside the conflicting Single Judge and Division Bench rulings in the Hare Ram Singh litigation, Supreme Court authority restricting consumer fora from adjudicating fraud-tainted claims, and the developing practice of the RBI's Integrated Ombudsman Scheme, the paper identifies a structural mismatch: a regime that formally shifts the evidentiary burden onto banks, operating inside forums that either lack the technical capacity to test that burden or decline jurisdiction the moment fraud is alleged. The paper also situates this doctrinal gap against the Reserve Bank's March 2026 draft revision, which proposes a compensation mechanism for small-value unauthorised transactions, and against parallel institutional measures such as MuleHunter.AI and the newly incorporated Indian Digital Payment Intelligence Corporation. It closes with proposals for a rebuttable presumption of bank liability, a standing technical-assessor mechanism within consumer fora, and mandatory forensic audit trails.

Keywords: Unauthorised electronic transactions, zero liability, RBI Circular 2017, cyber fraud, Banking Ombudsman, Consumer Protection Act, deficiency in service, mule accounts.

I. Introduction

India's decisive shift towards digitally intermediated retail banking is closely associated with the November 2016 demonetisation exercise, after which electronic transaction volumes rose sharply and reshaped the risk profile of a banker-customer relationship that had, until then, been governed largely by contract and the common law duty of care.[1] The speed, distance and relative anonymity of electronic transactions called for a regulatory response distinct from that inherited duty of care, and the Reserve Bank of India supplied one through its circular of 6 July 2017, Customer Protection - Limited Liability of Customers in Unauthorised Electronic Banking Transactions ('the 2017 Circular').[2] Nearly a decade later, the Circular remains the principal instrument for allocating losses arising from phishing, vishing, SIM-cloning, card-skimming and comparable frauds - even as the Reserve Bank has now placed a revised version out for public consultation in response to the scale and sophistication these frauds have since acquired.[3]

This paper argues that while the design of the 2017 Circular was progressive, its real-world efficacy has been diluted by three connected problems: first, the practical difficulty of discharging or rebutting the 'bank negligence' standard in an environment where the relevant evidence sits almost entirely on the bank's own servers; second, the reluctance of consumer fora to exercise jurisdiction once fraud or forgery is alleged; and third, inconsistent judicial treatment, most visibly in the reversal, on intra-court appeal, of a customer-favourable ruling in the *Hare Ram Singh* litigation.[4] The paper proceeds in six parts: an account of the Circular's liability architecture; its judicial reception; its interaction with the Consumer Protection Act, 2019 and the RBI's Integrated Ombudsman Scheme, 2021; an assessment of the 2026 draft revision and allied institutional measures; a critical analysis; and recommendations for reform.

II. The 2017 Circular's Tiered Liability Architecture

Issued under Section 35A of the Banking Regulation Act, 1949,[5] the 2017 Circular superseded

[1] Reserve Bank of India, *Customer Protection-Limited Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, DBR. No. Leg. BC.78/09.07.005/2017-18 (July 6, 2017).
[2] Reserve Bank of India, *Customer Protection-Limited Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, DBR. No. Leg. BC.78/09.07.005/2017-18 (July 6, 2017).
[3] RBI Tightens Rules on Unauthorised Electronic Banking Fraud, *Construction World* (Mar. 26, 2026), https://www.constructionworld.in/policy-updates-and-economic-news/rbi-tightens-rules-on-unauthorised-electronic-banking-fraud/88647.
[4] *Hare Ram Singh v. Reserve Bank of India*, 2024 DHC 8816; *State Bank of India v. Hare Ram Singh*, LPA 52/2025 (Delhi High Ct.).
[5] Banking Regulation Act, 1949, § 35A.

the Reserve Bank's earlier 2002 directions[6] and applies uniformly to scheduled commercial banks, small finance banks, payment banks and prepaid payment instrument issuers. It structures customer liability into three tiers keyed to fault and to the promptness of reporting: zero liability where the loss flows from contributory fraud, negligence or deficiency in service on the bank's part, or where a genuine third-party breach is reported within three working days; limited liability, capped by account type, where a third-party breach is reported within four to seven working days; and full liability, which persists only until the customer reports the loss, where the loss is attributable solely to the customer's own negligence, such as the voluntary disclosure of credentials.[7]

Tier	Trigger	Reporting Window	Customer's Liability
Zero Liability	Bank fault, contributory negligence, or deficiency in service	Any time, or within 3 working days for a genuine third-party breach	Nil
Limited Liability	Genuine third-party breach	4-7 working days	Lower of the transaction value or ₹5,000 / ₹10,000 / ₹25,000, depending on account type
Full Liability	Customer's own negligence (e.g., voluntary disclosure of credentials)	Until reported	Full amount until reporting; liability shifts to the bank thereafter

The Circular further requires that the disputed amount be provisionally re-credited within ten working days of notification, without awaiting the outcome of any internal investigation or insurance claim, and that the bank record its final determination of liability within ninety days under a policy approved by its board. Its most consequential feature, however, is evidentiary: the burden of proving customer negligence rests on the bank, not the customer - a deliberate reversal of the ordinary presumption, designed to correct the structural information asymmetry between an individual customer and an institution with exclusive access to transaction logs and

[6] Reserve Bank of India, Circular No. DBOD.Leg.BC.86/09.07.007/2001-02 (Apr. 8, 2002).
[7] Reserve Bank of India, *Customer Protection-Limited Liability of Customers in Unauthorised Electronic Banking Transactions*, RBI/2017-18/15, DBR. No. Leg. BC.78/09.07.005/2017-18, cls. 7-9 (July 6, 2017).

server-side data.[8]

III. Judicial Interpretation: Promise and Retreat

The protective intent of the 2017 Circular has received a mixed judicial reception, illustrated starkly by the *Hare Ram Singh* litigation. In a 2024 judgment, a Single Judge of the Delhi High Court held the State Bank of India liable for a ₹2.6 lakh loss suffered in a vishing attack, finding that the bank had breached the RBI's Master Direction on Digital Payment Security Controls and that the transaction fell within the zero-liability clause of the 2017 Circular; the Court was influenced by the petitioner's promptness in reporting the fraud through the Cyber Crime Cell and the Banking Ombudsman, contrasted with the bank's comparatively slow response.[9]

On intra-court appeal, however, a Division Bench reversed this finding.[10] It held that a customer's mere denial of having shared an OTP does not, without more, establish bank liability, and that 'negligence' under the 2017 framework extends beyond credential-sharing to conduct such as clicking a compromising link. The Division Bench also observed that questions of credential compromise and security breach demand technical and forensic examination that writ proceedings are not equipped to undertake. This is a meaningful doctrinal retreat: the zero-liability guarantee, as textually framed in the Circular, collapses into a fact-intensive inquiry that ordinary adjudicatory forums are often institutionally unable to resolve within any reasonable time. A comparable emphasis on the bank's burden of proof appears in the Allahabad High Court's decision in *Suresh Chandra Singh Negi v. Bank of Baroda*, which reiterated that Clause 12 of the 2017 Circular requires the bank, not the customer, to adduce convincing evidence before liability can be shifted.[11]

IV. The Consumer Protection Overlap and Its Limits

Banking services fall within the definition of 'service' under Section 2(42) of the Consumer Protection Act, 2019,[12] allowing customers to approach consumer commissions on grounds of deficiency in service. The Supreme Court's recent decision against Canara Bank, concerning negligent handling of cheques, confirms that ordinary negligence in routine banking operations

[8] *Id.* cl. 6, 10.
[9] *Hare Ram Singh v. Reserve Bank of India*, 2024 DHC 8816.
[10] *State Bank of India v. Hare Ram Singh*, LPA 52/2025 (Delhi High Ct.).
[11] *Suresh Chandra Singh Negi v. Bank of Baroda*, MANU/UP/1956/2025.
[12] Consumer Protection Act, 2019, § 2(42).

- wrongful dishonour, delayed processing and the like - attracts consumer liability and compensation once deficiency is established.[13]

That remedy narrows considerably, though, once fraud enters the facts. In *Sant Rohidas Leather Industries v. Vijaya Bank*, the Supreme Court held that a consumer forum, exercising summary jurisdiction, could not adjudicate a dispute involving serious allegations of fraud or forgery - there, a contested FDR pledge - reiterating its earlier view in *Chairman & Managing Director, City Union Bank Ltd. v. R. Chandramohan* that consumer commissions are unsuited to matters involving criminality.[14][15] The National Consumer Disputes Redressal Commission has applied the same logic to digital fraud, holding summary proceedings inappropriate where a customer's hacked email had triggered a simultaneous Cyber Crime Branch investigation.[16]

This produces a troubling paradox: the very customers most in need of a swift remedy - victims of fraud, by definition - are the ones most likely to find their consumer complaints rejected as unsuited to summary adjudication, since the bulk of unauthorised electronic transactions involve an allegation of fraud, whether by a third party or by way of an allegedly compromised bank system. Such customers are pushed instead towards a slower, costlier civil suit, or towards the Banking Ombudsman.

V. The Ombudsman Route: A Partial Corrective

The Reserve Bank - Integrated Ombudsman Scheme, 2021, notified under Section 35A of the Banking Regulation Act, 1949 and introduced under Section 45L of the RBI Act, 1934 and Section 18 of the Payment and Settlement Systems Act, 2007, merged three earlier ombudsman schemes into a single 'One Nation, One Ombudsman' structure and replaced a closed list of complaint grounds with a broad definition of 'deficiency in service'.[17] Complaints relating to digital payments have consistently been the single largest category received by the Ombudsman, accounting for more than 42 per cent of the total in the most recent reporting year.[18] The Scheme offers a cost-free, quasi-judicial award mechanism of up to ₹20 lakh,

[13] *Canara Bank v. Kavita Chowdhary*, 2026 INSC 363, Civil Appeal No. 2587 of 2025 (S.C. Apr. 15, 2026).
[14] *Sant Rohidas Leather Indus. & Charmakar Dev. Corp. Ltd. v. Vijaya Bank*, 2026 INSC 264, Civil Appeal No. 4841 of 2023 (S.C. Mar. 19, 2026).
[15] *Chairman & Managing Dir., City Union Bank Ltd. v. R. Chandramohan*, (2023) 7 SCC 775.
[16] *Neil E. Lobo v. Bank of Baroda*, F.A. No. 1662 of 2018 (Goa State Consumer Disputes Redressal Comm'n).
[17] Reserve Bank of India, *Reserve Bank-Integrated Ombudsman Scheme, 2021*, notified under Banking Regulation Act, 1949, § 35A; Reserve Bank of India Act, 1934, § 45L; Payment and Settlement Systems Act, 2007, § 18.
[18] Digital Payment Complaints Highest in RBI's Integrated Ombudsman Scheme, *Business Standard*.

excluding the disputed amount, plus up to ₹1 lakh for mental agony.[19] It remains, however, ill-suited to disputes requiring detailed documentary or forensic analysis, so the most technically complex - and often most valuable - cyber-fraud cases are routinely pushed back to the civil courts, precisely the trajectory the *Hare Ram Singh* appeal itself followed.

VI. Recent Regulatory Developments: The 2026 Draft Revision and Institutional Responses

On 6 March 2026, the Reserve Bank placed for public comment a revised customer-liability framework that, notably, proposes a standing compensation mechanism for small-value unauthorised transactions, rather than requiring every customer to be routed through the full three-tier structure irrespective of the amount involved. The Reserve Bank has framed the exercise as a review made necessary by the pace of technology adoption in banking and payments, intended to rebalance customer protection against banks' operational resilience.[20]

The draft revision sits alongside a cluster of preventive and detection-focused measures. MuleHunter.AI, an artificial-intelligence and machine-learning solution developed by the Reserve Bank Innovation Hub to identify mule accounts used to launder fraud proceeds, has moved from a two-bank pilot to live deployment across more than thirty banks, with further scaling planned; banks have correspondingly been advised to strengthen real-time transaction monitoring, deploy network analytics to trace mule networks, and tighten controls against the diversion and layering of funds.[21] On the institutional side, the Indian Digital Payment Intelligence Corporation was incorporated as a Section 8 company on 16 October 2025 specifically to detect, prevent and analyse fraud across the digital payments ecosystem in real time using artificial intelligence, machine learning and big-data analytics.[22]

Reporting infrastructure has also been overhauled: the SACHET portal, the centralised channel for reporting financial misconduct, was relaunched in June 2026 with a redesigned interface,

[19] Reserve Bank of India, *Reserve Bank-Integrated Ombudsman Scheme, 2021*, cl. 15.
[20] RBI Tightens Rules on Unauthorised Electronic Banking Fraud, *Construction World* (Mar. 26, 2026), https://www.constructionworld.in/policy-updates-and-economic-news/rbi-tightens-rules-on-unauthorised-electronic-banking-fraud/88647.
[21] RBI Unveils Revised Framework to Combat Digital Banking Fraud with AI Tools, *CAclubindia* (Mar. 25, 2026), https://www.caclubindia.com/news/rbi-unveils-revised-framework-to-combat-digital-banking-fraud-with-ai-tools-26353.asp; RBI's AI Fraud System Combats Mule Accounts Across 31 Banks, *News4Hackers* (Sept. 2026), https://www.news4hackers.com/rbis-ai-fraud-system-combats-mule-accounts-across-31-banks/.
[22] RBI Tightens Rules on Unauthorised Electronic Banking Fraud, *Construction World* (Mar. 26, 2026) (recording the incorporation of the Indian Digital Payment Intelligence Corporation as a Section 8 company on Oct. 16, 2025).

multilingual support across thirteen Indian languages, and accessibility improvements aimed at widening its reach.[23] These sit alongside longer-running preventive efforts, including the Centre for Financial Literacy project - which had established 2,421 centres by 31 March 2025 - the annual Financial Literacy Week held since 2016, and the multilingual public-awareness campaign RBI Kehta Hai.[24]

Read together, these measures are overwhelmingly ex ante: they aim to detect fraud before it consummates (MuleHunter.AI, the IDPIC), or to make reporting easier once it has occurred (SACHET), or to prevent it through awareness (RBI Kehta Hai, the Financial Literacy Week). The March 2026 draft's proposed compensation mechanism is the first initiative in this cluster to address the ex post evidentiary bottleneck identified in Parts III and IV directly - but as a consultation draft, its interaction with the existing tiered structure, its value thresholds, and its relationship to the consumer-fora fraud exception have not yet been settled, and merit close attention once the framework is finalised.

VII. Critical Analysis

This analysis identifies four connected weaknesses in the present structure.

First, the burden-shifting rule in the 2017 Circular is not genuinely symmetrical in operation: customers rarely have access to the forensic server-log and Indicator-of-Compromise analysis needed either to discharge or to rebut a finding of negligence, since that evidence is generated and held entirely within the bank's own systems.

Second, the fragmentation of available forums - writ courts, consumer commissions, and the Banking Ombudsman, each of which tends to decline the cases of greatest factual complexity - creates an incentive to forum-shop and produces inconsistent outcomes for factually similar frauds.

Third, the typology of 'fault' embedded in the 2017 framework is increasingly strained by the sophistication of contemporary attacks, including SIM-swapping and AI-assisted vishing; the Division Bench in *Hare Ram Singh* itself acknowledged this by treating link-clicking as a

[23] RBI's AI Fraud System Combats Mule Accounts Across 31 Banks, *News4Hackers* (Sept. 2026), https://www.news4hackers.com/rbis-ai-fraud-system-combats-mule-accounts-across-31-banks/.
[24] RBI Tightens Rules on Unauthorised Electronic Banking Fraud, *Construction World* (Mar. 26, 2026) (noting the Centre for Financial Literacy project's 2,421 centres as of Mar. 31, 2025, and the annual Financial Literacy Week held since 2016).

distinct species of fault separate from OTP-sharing.

Fourth, the 2026 reform cluster, welcome as it is, is concentrated on detection and prevention rather than on the adjudicatory bottleneck: none of MuleHunter.AI, the IDPIC or the SACHET relaunch resolves the question of which forum is competent to decide a contested fraud claim, or on what evidentiary footing. Absent express integration, a faster reporting channel and a smarter detection system may simply feed a larger volume of disputes into the same fragmented and reluctant adjudicatory pipeline.

VIII. Recommendations and Conclusion

To address these gaps, this paper proposes three reforms.

(i) A rebuttable presumption of bank responsibility, triggered by the timely fact of a customer's report, which can be displaced only by a technical assessment from an independent forum empanelled by the Reserve Bank, with forensic findings recognised across writ courts, consumer commissions and the Ombudsman alike.

(ii) A standing 'technical assessor' mechanism within consumer commissions, to whom the narrow factual question of the origin of a fraud can be referred without the commission losing jurisdiction over the ultimate question of liability - achievable either through an amendment to the Consumer Protection Act, 2019 or through a new RBI Master Direction.

(iii) A statutory requirement that, within the Ombudsman Scheme's existing ninety-day window, the technical assessor's findings be placed before the consumer commission and expressly considered - though not treated as binding - before it reaches a final decision on liability.

The 2017 Circular remains, on paper, a well-designed regime; its 'zero liability' promise nonetheless depends on an enforcement environment that has been more reactive than the digital frauds it is meant to address. The Reserve Bank's own March 2026 consultation on a compensation mechanism for small-value fraud suggests the regulator is alive to this gap, and offers a live opportunity to embed the adjudicatory reforms proposed here directly into the revised framework, rather than leaving substantive protection to outrun institutional capacity once again.