



INTERNATIONAL JOURNAL OF HUMAN RIGHTS LAW REVIEW

An International Open Access Double Blind Peer Reviewed, Referred Journal

Volume 5 | Issue 5 | 2026

Art. 19

Authorised but Not Autonomous: Loss Allocation in India's Coerced Push Payment Frauds

Eshan Garg

*Law Student, 3rd Year, BA.LL.B.,
Jindal Global Law School, O.P. Jindal Global University*

Recommended Citation

Eshan Garg, *Authorised but Not Autonomous: Loss Allocation in India's Coerced Push Payment Frauds*, 5 IJHRLR 209-218 (2026).
Available at www.ijhrlr.in/current-issues/.

This Article is brought to you for free and open access by the International Journal of Human Rights Law Review by an authorized Lex Assisto & Co. administrator.

For more information,
please contact submission.ijhrlr@gmail.com

Authorised but Not Autonomous: Loss Allocation in India's Coerced Push Payment Frauds

ABSTRACT

India allocates loss from electronic banking fraud through a Reserve Bank circular of 6 July 2017, which distributes liability across three tiers, each presupposing that the disputed transaction was unauthorised. The fastest-growing category of Indian payment fraud does not fit that premise. In frauds described as "digital arrest", the victim is persuaded by impersonators of the police or the judiciary that criminal process has been initiated against her, and transfers the money herself using her own credentials and authentication. The transaction is authorised in every technical sense, the framework therefore does not reach it, and the victim bears the whole loss by default rather than by any considered allocation. This article asks how loss should be distributed when a payment instruction is genuine but the consent behind it was procured by fraud. It argues that the circular asks who authenticated the transfer when it should ask whether consent was free, and that contract law cannot close the gap, the Indian Contract Act locating vitiated consent between victim and fraudster rather than between victim and bank. The study is doctrinal and functionally comparative, drawing on Reserve Bank instruments, decisions of the Delhi and Allahabad High Courts, orders of the Supreme Court in its suo motu digital arrest proceedings, and data placed before Parliament by the Ministry of Home Affairs. It finds that India has built substantial capacity to intercept fraudulent funds in transit while restoring close to two per cent of reported losses, and that High Courts have had to improvise the distinction between coercion and self-dealing case by case, the regulator having left the question open. It recommends a third liability category for fraudulently induced authorised transactions, with loss shared between remitting and beneficiary institutions.

KEYWORDS

Authorised push payment, Consumer protection, Digital arrest, Liability allocation, Payment regulation.

I. INTRODUCTION

In October 2025 the Supreme Court took suo motu cognisance of a complaint from a seventy-three-year-old woman in Ambala, who had

been confined in what her captors called a 'digital arrest' through forged orders of the Court itself and induced to part with more than one crore rupees.¹ Over the months that followed the Court issued directions to the Reserve Bank, the Ministry of Home Affairs and the Department of Telecommunications, recording that upwards of fifty-two thousand crore rupees had been siphoned through such frauds between April 2021 and November 2025, describing the conduct as robbery and dacoity.² On 9 February 2026 it directed the Reserve Bank and other authorities to meet and develop a framework for compensating victims.³

That direction is an admission of something the regulatory record states plainly. A compensation framework needs to be created because the existing one does not reach these losses. Liability for fraudulent electronic banking transactions in India is governed by a Reserve Bank circular of 6 July 2017, which allocates loss across three tiers according to whether the fault lay with the bank, a third party, or the customer.⁴ Every tier rests on a premise stated in the circular's own title: the transaction must have been unauthorised. A victim who transfers money under a fabricated threat of arrest has authenticated the transfer personally. No credential was compromised, no system failed, and nothing about the instruction was irregular.

The scale is not marginal. Reported digital arrest incidents rose from 39,925, involving about 91 crore rupees, in 2022 to 1,23,672, involving about 1,935 crore rupees, in 2024.⁵ In comparison, the restitution to victims remains negligible. The gap has attracted a substantial criminological and enforcement literature and almost no attention to the question this article addresses: who should bear a loss that no existing rule assigns. The objectives are to establish the exclusion as a matter of construction, to explain why private law cannot close it, to evaluate two jurisdictions that have allocated this loss deliberately, and to propose a design for the framework the Court has now called for.

¹ In *Re: Digital Arrest Scams*, Suo Motu proceedings, Supreme Court of India, cognisance taken on Oct. 17, 2025. See "SC Takes Strong Note of Rising Digital Arrest Scams, Seeks Centre and CBI Response", *News on AIR*, Oct. 17, 2025, available at: <https://www.newsonair.gov.in> (Last visited on Sept. 4, 2026).

² "Digital fraud like 'robbery': Supreme Court asks Centre to frame SOPs", *Business Standard*, Feb. 9, 2026, available at: <https://www.business-standard.com> (Last visited on Sept. 5, 2026).

³ *Id.*

⁴ Reserve Bank of India, "Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions", RBI/2017-18/15, DBR.No.Leg.BC.78/09.07.005/2017-18, dated July 6, 2017, available at: <https://www.rbi.org.in> (Last visited on Sept. 4, 2026).

⁵ "How India's Cyber Crime Incidence Is Rising", *IndiaSpend*, Dec. 6, 2025, available at: <https://www.indiaspend.com> (Last visited on Sept. 4, 2026). Figures are drawn from the National Cybercrime Reporting Portal as placed before Parliament.

II. LITERATURE REVIEW

Three strands of writing bear on the problem and none engages it directly. The first is criminological and geopolitical, examining the transnational scam compounds in Cambodia, Myanmar and Laos from which a large share of these operations is run, and treating the response as a problem of interdiction and extradition. The second assesses institutional capacity, measuring the reach of the National Cybercrime Reporting Portal and the Citizen Financial Cyber Fraud Reporting and Management System against the volume of complaints, and concluding that response capacity is outpaced by fraud growth.⁶ Both strands measure the state's effort against the criminal rather than its allocation of loss between innocent parties.

The third strand is doctrinal and reads the 2017 circular as a consumer-protective instrument, tracing its application by High Courts and consumer fora under the label of the zero-liability principle. That writing assumes throughout that the disputed transaction was unauthorised, which is the case the circular was drafted for. Comparative scholarship on authorised push payment fraud is well developed but overwhelmingly British and has not been brought to bear on a system of India's transaction volumes or on a fraud typology built around impersonation of the State. The gap this article occupies is narrow: not the absence of writing on digital arrest, which is plentiful, but the absence of any treatment of coerced authorisation as a distinct category for allocating loss.

III. RESEARCH METHODOLOGY

The design is doctrinal, supported by secondary quantitative material and functional comparison. Primary sources are the Reserve Bank circulars, the Indian Contract Act, 1872, the Consumer Protection Act, 2019, decisions of the Delhi and Allahabad High Courts, and orders of the Supreme Court in the suo motu digital arrest proceedings. Quantitative material is drawn from answers given by the Ministry of Home Affairs in Parliament and from status reports of the Indian Cyber Crime Coordination Centre. The scope is confined to retail electronic transfers initiated by individual customers, excluding card-present and corporate mandate fraud. Two limitations qualify the findings: parliamentary answers use varying reference periods and category definitions, so the series are indicative rather than strictly comparable, and no primary survey of victims was conducted. Allocation rules are assessed against whether they track free consent, whether they price each

⁶ CyberPeace Foundation, "India's Cybercrime Surge Signals a Growing Digital Security Challenge: An Assessment Based on Rajya Sabha Proceedings and MHA Data" (2026), available at: <https://cyberpeace.org> (Last visited on Sept. 3, 2026).

party's capacity to prevent the loss, and whether they are administrable at scale.

IV. DISCUSSION AND ANALYSIS

A. The authorisation premise

The 2017 circular establishes a graded scheme. A customer bears no liability where the loss arises from a deficiency on the part of the bank, or from a third-party breach where the deficiency lies with neither bank nor customer and the customer notifies the bank within three working days. Liability is capped at a figure fixed by account type where the loss arises from the customer's own negligence in sharing credentials, or where notification is delayed by four to seven working days. Beyond that, liability is governed by the bank's board-approved policy. Critically, the burden of establishing customer negligence rests on the bank, and complaints must be resolved within ninety days.⁷

The scheme is a reasonable allocation of the two risks it envisions: that the bank's systems fail, and that a third party obtains and misuses the customer's credentials. The coerced transfer is neither. The fraudster never touches the credentials; the customer supplies them herself, having been convinced that compliance is a legal obligation. There is no unauthorised transaction to which any tier can attach. The consequence is not that she is assigned liability under the second tier, which would at least cap her exposure, but that the circular does not apply at all and her exposure is unlimited. An instrument built to protect customers therefore leaves the fastest-growing class of retail payment loss outside its reach as a matter of construction rather than of policy choice.

B. What contract law supplies and what it cannot

Indian law is not short of the relevant concept. Consent is free only when it is not caused by coercion, undue influence, fraud, misrepresentation or mistake, and an agreement whose consent was caused by fraud is voidable at the option of the party deceived.⁸ A transfer made under a fabricated threat of arrest, supported by forged process, is a textbook instance of consent procured by fraud. The difficulty is one of parties. The corrupting conduct is that of the fraudster and the agreement it vitiates is the one between the victim and the fraudster. Between the victim and her bank there is a different relationship, that of mandate: the customer instructed and the bank executed a properly authenticated instruction. Nothing in these provisions displaces that mandate, and on the current state of the law the bank's answer, that it performed the mandate it was given, is good.

⁷ *Supra* note 4, cl. 12 (burden of proof on the bank).

⁸ Indian Contract Act, 1872, ss. 14, 17 and 19.

India accordingly possesses the doctrine of vitiated consent without any mechanism for translating it into an allocation of loss, because the doctrine sits in the wrong bilateral relationship. The general consumer remedy fares no better. A claim of deficiency in service⁹ requires a standard against which the bank's conduct can be measured, and no instrument identified in this study specifies when a payment service provider must interrupt an anomalous transaction, what an effective warning consists of, or how a pattern deviation should be treated. Consumer fora asked to find deficiency are asked to invent the duty first. Regulatory vacancy thus disables the residual remedy as well as the specific one, which is the strongest argument for locating the reform in the Reserve Bank rather than in litigation.

C. Judicial improvisation and the evidence of vacancy

The courts have been left to improvise. The Delhi High Court in *Hare Ram Singh* held a bank liable notwithstanding that the disputed transactions had been authenticated by a one-time password, reasoning that customer diligence must be assessed in the light of contemporary social engineering techniques.¹⁰ A Division Bench of the Allahabad High Court in *Suresh Chandra Singh Negi* marked the limit of that protection, holding on evidence that the transfers came from the account holder's own device and IP address that the circular is a shield for customers and not a sword by which personal transactions may be recast as cyber fraud.¹¹ Neither case concerned a coerced authorisation, and that is the difficulty: courts are drawing the line between genuine deception and self-dealing on the facts of individual disputes, with no provision telling them where it falls. The improvisation is a symptom of regulatory silence rather than of judicial error.

The empirical record shows where the State has invested. Interception capacity is considerable. The Citizen Financial Cyber Fraud Reporting and Management System had saved more than 8,189 crore rupees across 23.61 lakh complaints by 31 December 2025,¹² and the Suspect Registry, drawing on 21.65 lakh identifiers and 26.48 lakh first-layer mule accounts shared by banks, had caused transactions worth 9,055.27 crore rupees to be declined.¹³ Restoration to victims is of a different order: the status report placed before the Supreme Court recorded money restored in

⁹ Consumer Protection Act, 2019, s. 2(11).

¹⁰ *Hare Ram Singh v. Reserve Bank of India*, W.P. (C) No. 13497 of 2022, Delhi High Court.

¹¹ *Suresh Chandra Singh Negi v. Bank of Baroda*, Writ (C) No. 24192 of 2022, Allahabad High Court, decided on July 17, 2025 (Saraf and Giri, JJ.).

¹² Ministry of Home Affairs, Rajya Sabha Unstarred Question No. 1349, answered on Feb. 11, 2026, available at: <https://www.mha.gov.in> (Last visited on Sept. 7, 2026).

¹³ Ministry of Home Affairs, Rajya Sabha Unstarred Question No. 1338, answered on Feb. 11, 2026, available at: <https://www.mha.gov.in> (Last visited on Sept. 6, 2026).

36,290 cases aggregating approximately 18.05 crore rupees.¹⁴ Independent analysis of the parliamentary series places victim restitution at about 2.18 per cent of reported losses.¹⁵

The disparity between funds frozen in transit and funds returned to victims is not evidence of official indifference. It is the predictable output of a rule that assigns residual loss to whoever authenticated the transfer. Freezing is an operational function the State can perform without deciding who ultimately bears the loss; restitution requires that decision, and no instrument makes it. The negligence framing also fails on its own terms. These frauds work by invoking the authority of the State under manufactured urgency and enforced isolation, and compliance with apparent legal command is not autonomous economic choice. That reported victims include physicians, retired professors and serving officers indicates that the losses do not track digital literacy in the way the negligence tier assumes.¹⁶

D. Two Jurisdictions that allocated the loss deliberately

The United Kingdom faced the same construction problem and resolved it by rule. Since 7 October 2024 payment service providers must reimburse consumers who fall victim to authorised push payment fraud on the Faster Payments system, with the cost divided equally between the sending and the receiving firm.¹⁷ The design carries three features worth transplanting. Reimbursement is presumptive and refusable only where the consumer's conduct fell below a published standard of caution through gross negligence, which replaces an open-ended negligence inquiry with a defined test. The cap was set at a level aligned with deposit insurance after smaller firms raised prudential objections, and a modest excess applies to ordinary consumers but not to vulnerable ones.¹⁸ Most importantly, the equal split gives the receiving institution, which hosts the mule account and alone observes its behaviour, a financial reason to police it.

The predicted consequences did not materialise. An evaluation published in July 2026 found that annual losses to this category of fraud fell by roughly seventy-three million pounds following the reform,

¹⁴ "Supreme Court issues directions to curb digital arrest scams, asks RBI to frame SOP on mule accounts", *Bar and Bench*, Aug. 4, 2026, available at: <https://www.barandbench.com> (Last visited on Sept. 5, 2026).

¹⁵ *Supra* note 6.

¹⁶ *Supra* note 5.

¹⁷ Payment Systems Regulator, *Fighting Authorised Push Payment Scams: Final Decision*, PS23/4 (Dec. 19, 2023); the Faster Payments reimbursement requirement took effect on Oct. 7, 2024, available at: <https://www.psr.org.uk> (Last visited on Sept. 6, 2026).

¹⁸ The maximum reimbursement was reduced from GBP 415,000 to GBP 85,000 after consultation in September 2024, aligning the cap with the deposit insurance limit. An excess of up to GBP 100 may be levied, but not on vulnerable consumers.

which meets the moral hazard objection with evidence rather than assertion.¹⁹ Singapore supplies the second element India needs. Its Shared Responsibility Framework, operative from December 2024, allocates loss down a waterfall in which banks bear it where they breached their duties, telecommunications operators bear it where the banks did not, and the consumer bears it only where both discharged their obligations.²⁰ The telecommunications limb matters in India because these frauds are executed over spoofed calls and fraudulently obtained connections, and because the Department of Telecommunications is already a party before the Supreme Court in the same proceedings.²¹

Two features should not be copied. A cap drawn from British deposit insurance has no application to an Indian loss distribution in which a single elderly victim may lose several crore rupees, and its claims infrastructure presupposes far fewer providers than India's retail systems carry. What transfers is the allocation principle, not the numbers.

V. FINDINGS

First, coerced authorised transfers fall outside the 2017 circular as a matter of construction. The victim bears the whole loss not because a rule assigns it to her but because no rule assigns it at all.

Second, private law cannot close the gap. The Indian Contract Act supplies the concept of vitiated consent but locates it between victim and fraudster, and a deficiency claim under the Consumer Protection Act fails, on the instruments examined here, for want of any regulatory standard of intervention against which a bank's conduct can be measured.²²

Third, neither of the leading High Court decisions on the circular concerned a coerced authorisation. Courts are separating genuine deception from self-dealing case by case, because no provision tells them where the line falls.

Fourth, India has invested heavily in interception and negligibly in allocation. Thousands of crores are frozen in transit each year while

¹⁹ Zennon Kapron, "Britain Made Banks Refund Scam Victims. The Sky Did Not Fall.", *Forbes*, July 24, 2026, available at: <https://www.forbes.com> (Last visited on Sept. 7, 2026), reporting an evaluation by Frontier Economics published on July 1, 2026.

²⁰ Monetary Authority of Singapore and Infocomm Media Development Authority, *Shared Responsibility Framework*, operative from December 2024, available at: <https://www.mas.gov.sg> (Last visited on Sept. 7, 2026).

²¹ Observer Research Foundation, "Digital Arrest Scams and the Limits of Domestic Enforcement", July 18, 2026, available at: <https://www.orfonline.org> (Last visited on Sept. 8, 2026).

²² Consumer Protection Act, 2019, s. 2(47).

restitution runs at roughly two per cent of reported losses, a ratio that follows from the design of the liability rule.

Fifth, the reform question is no longer whether but how. The Supreme Court has directed the Reserve Bank to adopt and circulate a standard operating procedure and has asked an inter-departmental committee to examine a framework of shared liability and compensation.²³ What is missing is a design.

VI. RECOMMENDATIONS

The Reserve Bank should amend the 2017 circular to insert a third category of fraudulently induced authorised transactions, covering transfers where the customer's instruction was procured by impersonation of a public authority or comparable deception. The power exists and has already been used for this instrument: section 35A of the Banking Regulation Act, 1949 and section 18 of the Payment and Settlement Systems Act, 2007 permit directions in the public interest.²⁴ Since the existing tiers were created by circular under those powers rather than by statute, a fourth requires no primary legislation, which makes the proposal implementable within the timelines the Court has set.

Within that category, loss should be shared equally between the remitting and the beneficiary institution, subject to a cap fixed by the Reserve Bank. The justification is not that either bank is at fault but that the beneficiary institution alone can observe mule account behaviour, and equal sharing prices that capacity. A cap answers the prudential objection raised by smaller providers.

Reimbursement should be presumptive, rebuttable where the institution demonstrates that the transaction was consistent with the customer's established pattern or that an effective intervention was made and disregarded. This shifts the inquiry from the customer's state of mind, which is unknowable after the fact, to the institution's monitoring conduct, which is documented. It also preserves the allocation of the burden of proof already made by the 2017 circular.²⁵

Two supporting measures follow. Since the reported victim profile is concentrated among senior citizens, no excess should be levied on customers above a prescribed age. The Reserve Bank should also require institution-level publication of fraud incidence and reimbursement rates, because without comparative disclosure no depositor can distinguish between institutions and shared liability operates weakly. Both can be

²³ *Supra* note 14.

²⁴ Banking Regulation Act, 1949, s. 35A; Payment and Settlement Systems Act, 2007, s. 18.

²⁵ *Supra* note 4, cl. 12.

carried in the standard operating procedure the Court has directed the Reserve Bank to circulate, provided it is framed as a binding direction rather than as advisory practice.

VII. CONCLUSION

India's payment fraud framework was drafted for a world in which the question worth asking was whether the customer authorised the transaction. That question no longer separates the cases that matter. The most damaging frauds now operate by procuring authorisation rather than by circumventing it, and a rule organised around authentication answers a question the facts have stopped posing. The Supreme Court has recognised as much and has asked the executive to build what the regulator has not.²⁶ The design is available, tested in two jurisdictions, and within the Reserve Bank's existing powers. What it requires is the decision that the risk of fraudulently procured consent belongs with the institutions that operate the payment system rather than with the individuals who use it.

²⁶ *Supra* note 2.