Page 651 - 672 **DOI:** *https://doi.org/10.63108/IJLMH.13253*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 6

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Coerced but "Authorised": Allocating Loss in India's Digital Arrest Frauds and the Case for a Statutory Reimbursement Regime

SYED AADIL RIZVI*

ABSTRACT

In a "digital arrest" fraud, callers posing as police, customs or central-agency officers convince a victim over video that she is under investigation and must move her savings into a "verification" account to avoid arrest. The victim makes the transfers herself. That single fact has shaped how Indian law allocates the loss. Because the payment is authenticated by the customer, it falls outside the "unauthorised transaction" framework that has governed bank liability since 2017, and the victim usually bears the whole loss. This paper examines whether that allocation can be defended and what should replace it. It combines doctrinal analysis of the Reserve Bank of India's 2017 Circular, the Responsible Business Conduct Third Amendment Directions, 2026, consumer law and the Supreme Court's continuing suo motu proceedings with analysis of official data placed before Parliament and the Court, and a comparative study of the United Kingdom, the European Union, Singapore and Australia. Reported digital-arrest losses rose from ₹91.14 crore in 2022 to ₹1,935.51 crore in 2024, and the average reported loss per complaint rose from about ₹22,800 to about ₹1.57 lakh. The 2026 Directions bring coerced payments within the definition of a fraudulent transaction, but a coerced customer who took reasonable care falls under none of their liability rules, and their compensation mechanism covers only negligent customers' losses of up to ₹50,000, once in a lifetime, for a single year. The paper argues that coercion is not negligence, that banks are the cheapest avoiders of this loss, and that the bank hosting the mule account should share it. It proposes a statutory Coerced Payment Reimbursement Scheme built on a presumption of reimbursement, an equal split between sending and receiving banks, a meaningful cap and a narrow gross-negligence exception.

Keywords: *Digital Arrest, Authorised Push Payment Fraud, Bank Liability, Consumer Protection, Reimbursement*

* Author is a Student at National University of Study and Research in Law, Ranchi, Jharkhand, India. ORCID: https://orcid.org/0009-0008-0126-3095

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

I. Introduction

Between 3 and 16 September 2025 an elderly couple in Ambala, Haryana, were contacted by people posing as officers of the Central Bureau of Investigation and the Enforcement Directorate and as judicial authorities. Shown forged orders of the Supreme Court and threatened with arrest and the seizure of their property, they were, in the Court's words, "coerced to transfer Rs.1,05,50,000 through multiple bank transactions."[1] Their complaint became a *suo motu* writ petition, *In re Victims of Digital Arrest Related to Forged Documents*.[2] On 29 October 2026 the Court told the Reserve Bank of India (RBI) that the regulatory measures it was preparing must require financial institutions to compensate victims, in an amount not less than the sum lost, where the fraud occurred because the institution failed to exercise due diligence.[3]

Behind that direction lies a question the law has not answered well. When a criminal frightens a customer into instructing her own bank to pay, who should bear the loss? Since 2017 Indian banking regulation has approached the problem by asking whether the transaction was "unauthorised". The RBI's customer-liability framework protects a customer against debits she did not authorise, gives her zero liability where the bank was at fault, or where a third party was at fault and she reported promptly, and puts on the bank the burden of proving that she was to blame.[4] A digital-arrest victim, however, logs in herself, enters her own credentials and approves each transfer. In form the payment is hers. What makes it fraudulent is the reason she made it.

Most Indian writing on digital arrest has examined the criminal law and the investigative response. The allocation of loss between the victim and the banks has received far less attention, although it decides whether a victim ever sees her money again. This paper argues that the authorisation test gives the wrong answer for coercion-based payment fraud, and that the reforms the RBI notified in June 2026, though a real advance, leave the typical digital-arrest victim where she was. It asks how large the problem is and what the distribution of losses implies for compensation, how Indian law allocates the loss from a coerced but authenticated payment before and after 1 January 2027, what other jurisdictions can teach, and what allocation is both principled and workable. It makes three contributions. First, it brings together the official figures placed before Parliament and the Supreme Court and shows that the average reported

[1] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶¶ 1–3 (S.C. Oct. 17, 2025) (order) (India).
[2] *Id.* ¶ 1.
[3] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 4 (S.C. Oct. 29, 2026) (order) (India).
[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, ¶¶ 6, 12 (July 6, 2017), https://www.rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx?Id=11040 [hereinafter 2017 Circular].

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

loss per digital-arrest complaint rose from about ₹22,800 in 2022 to about ₹1.57 lakh in 2024, more than three times the ceiling of the RBI's new compensation mechanism. Second, reading the text of the 2026 Directions, it shows that a coerced customer who took reasonable care falls under none of their liability rules and outside their compensation mechanism, so that the least blameworthy victim is the one most likely to recover nothing. Third, drawing on the United Kingdom's mandatory reimbursement regime and on the economics of loss allocation, it proposes a statutory scheme built around a presumption of reimbursement and shared liability between the sending and receiving banks.

Part 2 sets out the method and Part 3 the data. Parts 4 and 5 examine Indian law and the Supreme Court's intervention, Part 6 the foreign models, Part 7 the case for placing the loss on the payment system, and Part 8 the proposed scheme.

II. Method and sources

The method is doctrinal and comparative, supported by secondary quantitative analysis. The doctrinal sources are the relevant statutes, the RBI's circulars and directions, decisions of the Supreme Court and the High Courts, proceedings before the National Consumer Disputes Redressal Commission (NCDRC), and the orders passed so far in the Supreme Court's *suo motu* case. The data come from written replies of the Ministry of Home Affairs in Parliament, figures recorded in the Supreme Court's order of 4 August 2026, the RBI's Annual Report for 2025-26, and published data of the United Kingdom's Payment Systems Regulator (PSR). Average losses were calculated by dividing the reported amount defrauded in a year by the number of complaints in that year.

Three limitations should be stated plainly. The Indian figures count complaints on the National Cyber Crime Reporting Portal (NCRP), not verified incidents, and the amounts are those reported by complainants. Officially comparable loss figures for 2025 have not been published, so the loss series ends in 2024. And the 2026 Directions take effect only on 1 January 2027; the analysis rests on their text, but the policies that banks must frame under them are not yet available.

III. The anatomy and scale of digital arrest fraud

A. How the fraud works

The fraud usually begins with a call that seems routine: a courier company reporting a parcel in the victim's name that contains drugs or forged passports. The call is then "transferred" to a supposed police or central-agency officer, who moves to video, in uniform, before what looks

like a police station. The victim is shown warrants, freezing orders and, in some cases, orders bearing the seal of the Supreme Court. She is told that she is under investigation, that she must stay on camera and that she must tell no one. To prove her innocence she must move her savings into a "verification" or "secure" account, from which the money will be returned once she is cleared. The funds pass within minutes through layers of mule accounts and are withdrawn, often abroad.[5]

Indian law recognises no such thing as an arrest by video call; at a hearing in October 2026 the Chief Justice openly wondered how anyone could believe that a person can be arrested over a mobile phone.[6] The offences committed are many: personating a public servant, extortion, cheating, cheating by personation and organised crime under the new penal code, and identity theft and cheating by personation using a computer resource under the information technology law.[7]

Two features of this pattern matter for what follows. First, the payment is made by the victim through her own authenticated channel; no password is stolen and no account is hacked. Second, the payment is obtained by fear rather than by a false promise. An investment-scam victim wants to invest and is deceived about the investment. A digital-arrest victim does not want to pay at all; she pays because she believes that refusing will lead to her arrest. The law has long treated those two kinds of defective consent differently, and Part 7 argues that loss allocation should do the same.

B. What the numbers show

Table 1 sets out the official figures, and Figure 1 plots them. Complaints of digital arrest on the NCRP rose from 39,925 in 2022 to 60,676 in 2023 and 1,23,672 in 2024, increases of 52 and 104 per cent. The amounts reported as defrauded rose much faster, from ₹91.14 crore to ₹339.03 crore and then ₹1,935.51 crore, a twenty-one-fold rise in two years.[8] Complaints fell to 58,239 in 2025 and stood at 16,377 for the first half of 2026.[9] The decline is welcome, but the losses

[5] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶¶ 1, 3 (S.C. Oct. 17, 2025) (order) (India); *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 6(vi) (S.C. Dec. 1, 2025) (order) (India); Asif Yar Khan, *Don't Fall Prey to 'Digital Arrest'*, TELANGANA TODAY (May 16, 2024), https://telanganatoday.com/dont-fall-prey-to-digital-arrest.

[6] Debby Jain, *'What Kind of People Believe They Can Get Arrested on Mobile?' CJI Expresses Shock at Digital Arrest Scams*, LIVELAW (Oct. 29, 2026), https://www.livelaw.in/top-stories/what-kind-of-people-believe-they-can-get-arrested-on-mobile-cji-expresses-shock-at-digital-arrest-scams-556486.

[7] The Bharatiya Nyaya Sanhita, No. 45 of 2023, INDIA CODE (2023), §§ 111, 204, 308, 318, 319; The Information Technology Act, No. 21 of 2000, INDIA CODE (2000), §§ 66C, 66D.

[8] MINISTRY OF HOME AFFAIRS, Rajya Sabha Unstarred Question No. 1505 (answered Mar. 12, 2025), https://www.data.gov.in/resource/year-wise-number-incidents-digital-arrest-scams-and-related-cyber-crimes-reported-national.

[9] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 3 (S.C. Aug. 4, 2026) (order) (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

that remain are large: at the hearing on 29 October 2026 the Chief Justice observed that about ₹800 crore had been lost to digital arrest in 2026 alone.[10]

Year	Complaints on NCRP	Change in complaints	Amount reported defrauded (₹ crore)	Average reported loss per complaint (₹)
2022	39,925	NA	91.14	22,828
2023	60,676	+52.0%	339.03	55,875
2024	1,23,672	+103.8%	1,935.51	1,56,503
2025	58,239	−52.9%	Not officially reported	NA
2026 (to 30 June)	16,377	NA	About 800 (stated in Court, Oct. 2026)	NA

Table 1: Digital-arrest complaints and reported losses, 2022 to 2026. Sources: Rajya Sabha Unstarred Question No. 1505 (answered Mar. 12, 2025) for 2022 to 2024; Supreme Court order of 4 August 2026 for complaints in 2025 and 2026; the 2026 loss figure was stated at the hearing of 29 October 2026 and is not an official total. Changes and averages calculated by the author.

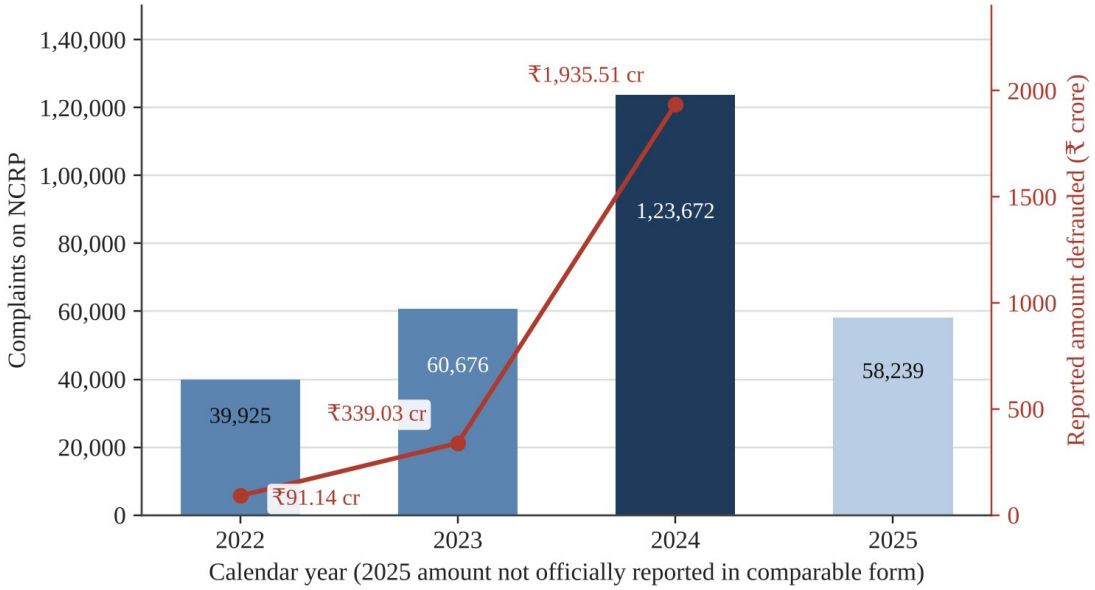


Figure 1: Digital-arrest complaints on the NCRP and reported amounts defrauded, 2022 to 2025. Source: Rajya Sabha Unstarred Question No. 1505 (answered Mar. 12, 2025); Supreme Court order of 4 August 2026 (2025 complaints). Chart by the author.

These figures sit inside a much larger problem. Citizens reported losses of ₹22,845.73 crore to cyber fraud in 2024, up from ₹7,465.18 crore in 2023, across 36,37,288 reported incidents of financial fraud.[11] Digital arrest accounted for about 3.4 per cent of those reported incidents in

[10] *Banks to Compensate Digital Arrest Victims? SC Mulls Big Move amid Push for New RBI Cyber Crime Rules*, THE WEEK (Oct. 29, 2026), https://www.theweek.in/news/india/2026/10/29/supreme-court-mulls-new-crackdown-on-digital-arrest-banks-to-compensate-victim-and.html; Jain, *supra* note 6.

[11] MINISTRY OF HOME AFFAIRS, Written Reply in the Lok Sabha (answered July 22, 2025), *reported in* Press Trust of India, *Citizens Lost Over Rs 22,845 Crore to Cyber Criminals in 2024: Govt*, THE WEEK (July 22, 2025), https://www.theweek.in/wire-updates/business/2025/07/22/del23-lsq-cyber-fraud.html.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

2024 but about 8.5 per cent of the money lost, up from 4.5 per cent of losses in 2023 (Figure 2). Its share of losses is far larger than its share of complaints because each case is large.

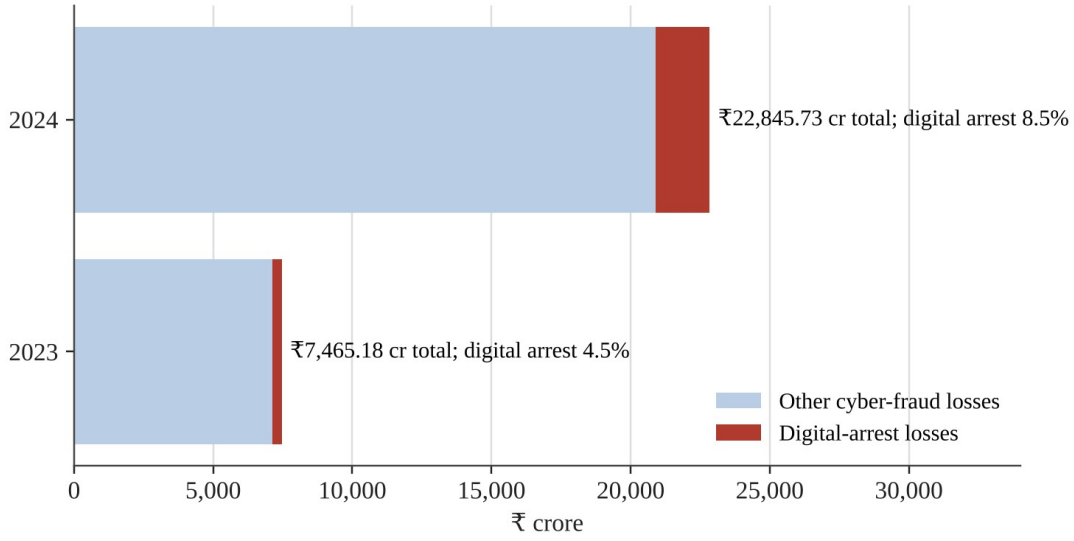


Figure 2: Digital arrest as a share of reported cyber-fraud losses, 2023 and 2024. Source: Ministry of Home Affairs replies in Parliament (Mar. 12, 2025 and July 22, 2025). Chart by the author.

There is also a striking gap between these figures and the RBI's own fraud statistics. Banks and financial institutions reported 28,836 frauds involving cards, internet banking and digital payments in 2023-24, worth ₹1,452 crore, falling to 13,332 cases worth ₹517 crore in 2024-25 and 293 cases worth ₹29 crore in 2025-26.[12] The RBI series covers frauds of ₹1 lakh and above, its amounts do not represent actual losses, and it was not designed to measure customer losses from scams, so the two sets of numbers are not directly comparable. The difference in scale is still telling. The ₹1,935.51 crore lost to digital arrest in 2024 alone exceeds the total value of card, internet and digital-payment frauds that banks reported in either of the two financial years that calendar year straddles. A likely reason is that a payment the customer authorised is not treated as a fraud on the bank at all. Figure 3 sets the two series side by side. The authorisation gap is statistical as well as legal: losses that banks do not bear tend not to appear in banks' fraud returns.

[12] RESERVE BANK OF INDIA, ANNUAL REPORT 2025-26, at 105–06 (2026).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

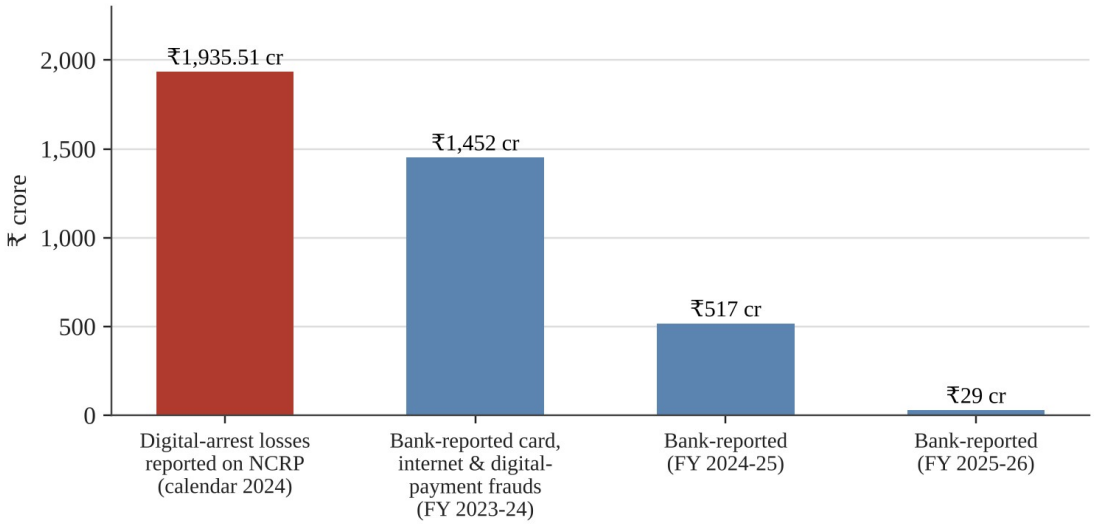


Figure 3: Digital-arrest losses reported by victims compared with card, internet and digital-payment frauds reported by banks. Source: Rajya Sabha Unstarred Question No. 1505 (answered Mar. 12, 2025); RBI Annual Report 2025-26, Table VI.3. The RBI series covers frauds of ₹1 lakh and above and uses financial years; the two series are not strictly comparable. Chart by the author.

C. Why the average matters

Figure 4 shows the average reported loss per complaint. It rose from ₹22,828 in 2022 to ₹55,875 in 2023 and ₹1,56,503 in 2024. Very large cases pull an average upwards, and such cases exist: three complainants before the NCDRC lost ₹10.3 crore, ₹5.85 crore and ₹5.88 crore.[13] The median loss may well be lower than the mean, but the NCRP does not publish it, so the point cannot be tested. Even so, the 2023 average already exceeded ₹50,000, and the 2024 average was more than three times that figure.

This matters because the RBI designed its new compensation mechanism for small frauds. Announcing it in February 2026, the Governor explained that, by number, nearly 65 per cent of fraud cases involve amounts below ₹55,000.[14] That is a sound basis for a scheme aimed at the general run of payment fraud. Digital arrest is different. Its losses are concentrated in fewer and larger cases, and a ceiling set for the typical UPI fraud will exclude most of the money and, on the available averages, a large share of the victims.

[13] *Digital Arrest: Can Customers Hold Banks Responsible for Fraud?*, OUTLOOK MONEY (July 15, 2025), https://www.outlookmoney.com/banking/digital-arrest-can-customers-hold-banks-responsible-for-fraud.

[14] *Hit by Digital Fraud? RBI Proposes Rs 25,000 Compensation for Small-Value Losses*, BUSINESS TODAY (Feb. 6, 2026), https://www.businesstoday.in/personal-finance/news/story/hit-by-digital-fraud-rbi-proposes-rs-25000-compensation-for-small-value-losses-514979-2026-02-06.

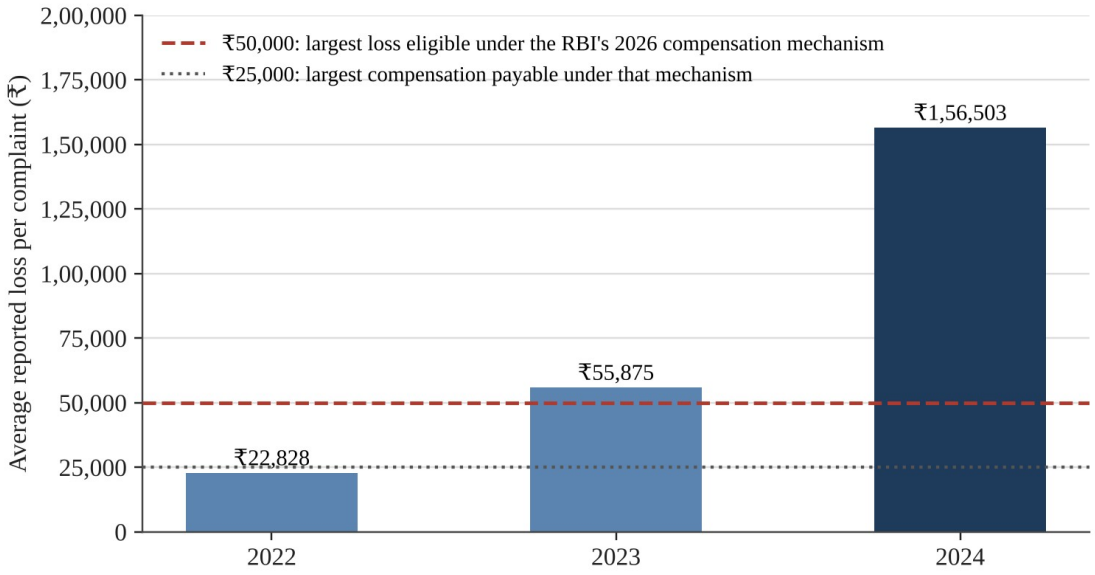


Figure 4: Average reported loss per digital-arrest complaint compared with the RBI's 2026 compensation limits. Source: calculated by the author from Rajya Sabha Unstarred Question No. 1505 (answered Mar. 12, 2025) and the 2026 Directions.

IV. THE EXISTING INDIAN FRAMEWORK

A. Criminal law punishes the fraudster but does not repay the victim

Criminal law supplies offences, not compensation. A prosecution can end in conviction, but restitution depends on tracing and freezing the money before it leaves the system. By July 2025 the government's Citizen Financial Cyber Fraud Reporting and Management System had, since its launch, prevented losses of more than ₹5,489 crore across more than 17.82 lakh complaints,[15] and a Suspect Registry had shared details of 24 lakh first-layer mule accounts with participating institutions.[16] These figures show what prompt reporting can save, but the mule-account figure also shows the size of the network through which unrecovered money flows. Once funds have passed through several layers and across a border, recovery is rare, and the question of who bears the residual loss remains.

B. The 2017 Circular and the "unauthorised" trigger

The RBI issued its circular on limiting customer liability in July 2017, when the main risks were card skimming, data breaches and stolen credentials, and its structure reflects that world. A customer has zero liability where the loss arises from contributory fraud, negligence or deficiency on the part of the bank, whether or not she reports it, and also where a third-party

[15] MINISTRY OF HOME AFFAIRS, Written Reply in the Lok Sabha, *supra* note 11; *Indians Lost INR 22,845 Cr to Cyber Fraud in 2024: Govt*, INC42 (July 22, 2025), https://inc42.com/buzz/indians-lost-inr-22845-cr-to-cyber-fraud-in-2024-govt.

[16] MINISTRY OF HOME AFFAIRS, Written Reply in the Lok Sabha, *supra* note 11; *Cyber Fraud Costs Indians ₹22,845 Crore in 2024: Government*, ANGEL ONE (July 23, 2025), https://www.angelone.in/news/cyber-fraud-costs-indians-22-845-crore-in-2024-government.

breach is to blame and she reports within three working days of the bank's alert.[17] Where the loss is due to her own negligence, as where she has shared her payment credentials, she bears the entire loss until she reports it.[18] The bank must credit the disputed amount within ten working days of notification, must resolve the complaint within ninety days and bears the burden of proving customer liability.[19]

Each of these rules assumes that the question is whether the customer authorised the debit. The digital-arrest victim did. She did not share her credentials with the fraudster; she used them herself. When victims have complained, banks have argued exactly this: that a transaction made by the customer, whether under coercion or not, is not their responsibility, that the RBI's rules cover unauthorised rather than coerced transactions, and that their systems were neither breached nor negligent.[20] Under the 2017 framework the coerced victim is not even classified as negligent. She is simply outside the scheme, and she bears the whole loss.

C. *Pallabh Bhowmick* and the limits of judicial generosity

Courts have read the 2017 Circular in customers' favour where they can. In *State Bank of India v. Pallabh Bhowmick*, a customer lost ₹94,204 in three online transactions after a caller posing as a retailer's customer-care manager persuaded him to download a mobile application in order to receive a refund.[21] The Gauhati High Court held the transactions to be unauthorised and fraudulent, found that the bank had established no negligence on his part, and applied the circular so that he bore no liability.[22] The Supreme Court dismissed the bank's petition, observing that the bank must remain vigilant and has access to current technology to detect and prevent fraud,[23] while adding that account holders must not share one-time passwords and may, on suitable facts, be held negligent.[24]

The decision is important for credential-theft cases. It cannot reach digital arrest, because its reasoning depends on the finding that the transactions were unauthorised. Where the customer herself made the transfers that premise fails, and the judicial route back to the 2017 Circular is closed.

---

[17] 2017 Circular ¶ 6.
[18] *Id.* ¶ 7.
[19] *Id.* ¶¶ 9, 10, 12.
[20] *Digital Arrest: Can Customers Hold Banks Responsible for Fraud?*, *supra* note 13.
[21] *State Bank of India v. Pallabh Bhowmick*, W.A. No. 364 of 2022, ¶ 3 (Gau. H.C. Sept. 13, 2024) (India).
[22] *Id.* ¶ 42.
[23] *State Bank of India v. Pallabh Bhowmick*, Special Leave to Appeal (C) No. 30677 of 2024, ¶ 3 (S.C. Jan. 3, 2025) (order) (India).
[24] *Id.* ¶ 5.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

D. Consumer law and the NCDRC

The Consumer Protection Act, 2019 offers a second route. Banking is a "service", and "deficiency" includes any act of negligence or omission that causes loss to the consumer.[25] In January 2025 three digital-arrest victims filed complaints before the NCDRC alleging deficiency in service by the banks through which their money had passed. Admitting them on 3 March 2025, the Commission observed that customer diligence had been "clearly compromised" and that RBI guidelines had been "blatantly violated", and it issued notice to every bank in the chain, including the beneficiary banks.[26] That is a meaningful step, but the route has limits. Each claim must prove a specific failure by a specific bank, using information about monitoring systems and account opening that only the banks hold. Months after admission, the Commission was still considering whether the complaints were maintainable and within its pecuniary jurisdiction.[27] Litigation of this kind is slow and costly for someone who has just lost her savings, and its outcome turns on the facts of each case.

E. The 2026 Directions: a wider door, a narrow room

On 24 June 2026 the RBI issued, under section 35A of the Banking Regulation Act, 1949, a set of amendment directions, the principal one being the Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026. They apply to electronic banking transactions undertaken on or after 1 January 2027.[28] Their most important change is conceptual. The trigger is no longer an "unauthorised" transaction but a "fraudulent" one, defined as a transaction "executed by a third-party using the credentials obtained from the customer through fraudulent means or executed by the customer by granting approval under coercion or duress from the third-party, and / or an unauthorised EBT".[29] The middle limb describes digital arrest exactly. For the first time, coerced payments sit inside the RBI's customer-protection framework.

Inclusion in the definition does not decide who pays, and on this the text leaves a gap. The liability rules turn on three categories. Where the fraud occurs through negligence by the bank, which includes failing to put mandated systems in place, failing to send required alerts and

---

[25] The Consumer Protection Act, No. 35 of 2019, INDIA CODE (2019), § 2(11), (42).
[26] Dhvani Rajyagor, *Digital Arrests Have Reached the Doorstep of the National Consumer Commission*, THE MAINSTREAM (July 14, 2025), https://themainstream.co.in/?p=86644; *Digital Arrest: Can Customers Hold Banks Responsible for Fraud?*, *supra* note 13.
[27] Rajyagor, *supra* note 26.
[28] *Reserve Bank of India (Commercial Banks – Responsible Business Conduct) Third Amendment Directions, 2026*, RBI/2026-27/167, DOR.MCS.REC.No.130/01-01-032/2026-27, ¶¶ 2–3 (June 24, 2026) [hereinafter 2026 Directions]; RESERVE BANK OF INDIA, Press Release No. 2026-2027/533, *RBI Issues Amendment Directions on 'Review of Framework of Limiting Customer Liability in Digital Transactions'* (June 24, 2026).
[29] 2026 Directions ¶ 4(15A).

failing to act on a customer's notification, the customer has zero liability whether or not she reports it.[30] Where there is a third-party breach, meaning a deficiency "elsewhere in the system" such as at a payment aggregator or telecom operator, she has zero liability if she reports "the unauthorised fraudulent EBT" within five calendar days.[31] Where she is negligent, she bears the loss until she reports it, subject to the compensation mechanism.[32] Customer negligence includes careless handling of credentials and "not paying attention to specific, directed and clear warnings from the bank that a prospective transaction is likely a scam".[33]

Now consider a digital-arrest victim whose bank did everything the Directions mandate and who received no specific warning. She was not negligent within the definition, and neither was the bank. The third-party-breach rule is framed around an unauthorised transaction, which a payment she approved herself is not. The coerced but careful customer therefore falls under none of the three rules. Her position is left to the bank's own policy, which must define customers' rights "in specified scenarios" but is given no rule for this one.[34] Because the compensation mechanism is confined to negligence cases, she is outside that too.[35] Her best argument is that a bank which let a pensioner's savings leave in a burst of unusual transfers failed to maintain the "robust and dynamic fraud detection and prevention mechanism" the Directions require, and was therefore negligent.[36] That argument may well succeed, but it must be won case by case.

The compensation mechanism, summarised in Table 2, is available to a *bona fide* individual victim whose gross loss from negligence-based fraud is up to ₹50,000. It pays 85 per cent of the net loss or ₹25,000, whichever is less, once in a lifetime, and only if the victim reported the fraud to the cyber-crime portal or helpline and to her bank within five calendar days. In domestic cases the RBI bears 65 per cent of the net loss in smaller cases and the customer's bank and the "beneficiary bank", which holds the account where the money was first credited, bear 10 per cent each. The mechanism covers only frauds occurring within one year of 1 January 2027.[37]

Element	Rule
Eligible claimant	Bona fide individual victim, including a sole proprietor (¶ 76T(1))

[30] *Id.* ¶¶ 4(20B), 76L.
[31] *Id.* ¶¶ 4(26.1A), 76M.
[32] *Id.* ¶ 76N.
[33] *Id.* ¶ 4(20C).
[34] *Id.* ¶ 76A(2).
[35] *Id.* ¶ 76T(1).
[36] *Id.* ¶ 76B(2).
[37] *Id.* ¶¶ 76T–76U.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Element	Rule
Eligible loss	Gross loss of up to ₹50,000 from fraudulent transactions caused by customer negligence (¶¶ 76N, 76T(1))
Amount	85% of the net loss after recoveries, or ₹25,000, whichever is less
Frequency	Once in a lifetime; one holder per joint account
Reporting condition	Report to the NCRP or helpline 1930 and to the bank within 5 calendar days of the fraud
Payment	Within 5 calendar days of the customer's application (¶ 76T(5))
Cost sharing, domestic (loss below ₹29,412)	RBI 65%; customer's bank 10%; beneficiary bank 10%; customer bears 15%
Cost sharing, domestic (₹29,412 to ₹50,000)	Flat ₹25,000: RBI ₹19,118; customer's bank ₹2,941; beneficiary bank ₹2,941
Cost sharing, cross-border	RBI 65%; customer's bank 20% (or ₹19,118 and ₹5,882 in the higher band)
Duration	Frauds occurring up to one year from 1 January 2027 (¶ 76U)

Table 2: The compensation mechanism under the 2026 Directions. Source: 2026 Directions ¶¶ 76N, 76T and 76U, compiled by the author.

Even setting aside the gap just described, three features of the mechanism shut out the typical digital-arrest victim. The ₹50,000 ceiling sits below the average reported loss in every year since 2023 (Figure 4). The five-day reporting window assumes a victim who knows she has been defrauded, whereas a digital-arrest victim is kept isolated, often for days, and told that the money will come back; the Ambala couple were defrauded over fourteen days. And the one-year sunset means that even the small-loss victim is protected only for frauds committed in 2027.

Table 3 applies the Directions to four scenarios. Its message is uncomfortable because the customer who was coerced, and whose conduct is least blameworthy, is the one most likely to recover nothing. Two features of the Directions nonetheless deserve credit. They bring coercion into the definition of fraud, which is the conceptual move this paper argues for. And they make the beneficiary bank contribute to compensation, the first time Indian regulation has accepted that the bank which hosts the receiving account should share the cost of fraud.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Scenario	2017 Circular	2026 Directions (from 1 January 2027)	Likely outcome
A. Digital arrest. After a video "interrogation", a 68-year-old transfers ₹3 lakh by net banking in four payments to a new payee. Alerts were sent; no specific scam warning was given. She reports on day 6.	Authorised; outside the Circular	"Fraudulent" (coercion limb, ¶ 4(15A)). No bank negligence (¶ 76L), no unauthorised third-party breach (¶ 76M), no customer negligence (¶ 76N). No express rule; left to bank policy. Compensation unavailable.	Victim likely bears the full loss
B. As in A, but the bank's systems did not flag the four transfers, made in one day to a payee account opened a few weeks earlier and unlike anything in her history.	Authorised; possible deficiency claim before a consumer forum	Arguable bank negligence for want of a "robust and dynamic fraud detection" mechanism (¶ 76B(2)), giving zero liability (¶ 76L)	Zero liability if the argument succeeds; uncertain
C. Credential fraud. A caller posing as the bank obtains an OTP and transfers ₹40,000. The customer reports on day 2.	Customer negligence (shared credentials); bears loss until reporting	"Fraudulent" (credential limb). Customer negligence (¶ 4(20C)(i)). Compensation available (¶ 76T).	Recovers ₹25,000 once (85% of ₹40,000, capped)
D. SIM swap by a telecom insider; account debited. The customer reports on day 1.	Third-party breach reported within 3 working days	Third-party breach involving a telecom provider, reported within 5 calendar days (¶¶ 4(26.1A), 76M)	Zero liability; full reversal

Table 3: Liability under the 2017 Circular and the 2026 Directions in four scenarios. Source: author's analysis of the 2017 Circular and the 2026 Directions.

V. The Supreme Court's intervention

The *suo motu* proceedings have moved quickly. Taking cognisance on 17 October 2025, the Court described the forging of its orders as "a direct assault on the dignity and majesty of this institution".[38] On 1 December 2025 it made the Central Bureau of Investigation the primary agency for digital-arrest cases.[39] It gave the agency a free hand to investigate bankers under the Prevention of Corruption Act, 1988 wherever they had been involved in opening mule accounts, and impleaded the RBI to explain why artificial-intelligence or machine-learning tools should not be used to identify such accounts and freeze the proceeds of crime.[40] The Court also noted that senior citizens were most often the targets.[41] At a hearing in December 2025 the *amicus*

[38] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 4 (S.C. Oct. 17, 2025) (order) (India).
[39] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 5 (S.C. Dec. 1, 2025) (order) (India).
[40] *Id.* ¶ 6(i)–(ii).
[41] *Id.* ¶ 3; Debayan Roy, *Supreme Court Orders CBI Probe into Digital Arrest Scams*, MONEYLIFE (Dec. 1, 2025), https://www.moneylife.in/article/supreme-court-orders-cbi-probe-into-digital-arrest-scams/78995.html.

curiae, Senior Advocate N.S. Nappinai, urged a victim-compensation mechanism on the lines of the United Kingdom's scheme for authorised push payment (APP) fraud, and the Union agreed to convene a meeting of stakeholders.[42]

On 4 August 2026 the Court directed the RBI to adopt, within four weeks, a standard operating procedure for temporary debit holds on amounts linked to mule accounts and cyber-enabled fraud, and asked the Inter-Departmental Committee to discuss a "shared-liability and victim-compensation framework".[43] The RBI released draft amendments to its Know Your Customer directions for consultation on 11 September 2026.[44] Then, on 29 October 2026, a bench of the Chief Justice and Justices Joymalya Bagchi and V. Mohana decided to examine, in the first instance, the Reserve Bank of India (Know Your Customer) Amendment Directions, 2026, due to be notified by 30 November and operationalised by 31 December 2026.[45] It said that the RBI's measures "must mandate and incorporate suitable provisions" requiring financial institutions to indemnify victims of digital arrest and other cyber frauds with compensation not less than the amount lost, where the fraud occurred because the institution failed "to exercise due diligence in preventing or reporting the act/incident".[46] It listed possible safeguards, among them temporarily suspending transactions inconsistent with an account's history, informing the nearest police station and verifying such transactions physically.[47] At the hearing the Attorney General argued that bank liability was a matter for the regulator, and Justice Bagchi observed that the Court could impose strict liability on financial institutions.[48] The matter is next listed on 23 November 2026.[49]

The October direction goes well beyond the 2026 Directions: it contemplates full compensation and is not confined to small frauds. But it keeps fault at the centre. A victim must still prove a failure of due diligence inside systems to which only the bank has access. The Court's readiness to consider strict liability points in the right direction. This paper's argument is that such a rule is better made by Parliament or the regulator, with caps, exceptions and a cost-sharing formula,

---

[42] *Supreme Court Suggests Reimbursement Framework for Digital Arrest Scam Victims*, MONEYLIFE (Dec. 17, 2025), https://moneylife.in/article/supreme-court-suggests-reimbursement-framework-for-digital-arrest-scam-victims/79144.html.

[43] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 7(i), (viii) (S.C. Aug. 4, 2026) (order) (India).

[44] RESERVE BANK OF INDIA, Press Release No. 2026-2027/1109, *Draft Reserve Bank of India (Know Your Customer) Amendment Directions, 2026* (Sept. 11, 2026).

[45] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 3 (S.C. Oct. 29, 2026) (order) (India).

[46] *Id.* ¶ 4.

[47] *Id.* ¶ 5.

[48] Jain, *supra* note 6.

[49] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 9 (S.C. Oct. 29, 2026) (order) (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

than built up order by order in a writ proceeding, and that the Court's directions supply the occasion for doing so.

VI. COMPARATIVE PERSPECTIVES

A. The United Kingdom: from *Philipp* to mandatory reimbursement

The closest foreign analogue is a case on almost exactly the facts of a digital arrest. In *Philipp v. Barclays Bank UK plc*, fraudsters posing as an officer of the Financial Conduct Authority working with the National Crime Agency persuaded Mrs Philipp and her husband to transfer £700,000 to accounts in the United Arab Emirates.[50] She argued that her bank owed her a duty to refuse or delay instructions it had reason to believe were the product of fraud, relying on the line of authority that began with *Barclays Bank plc v. Quincecare Ltd.*[51] The UK Supreme Court rejected the claim. Lord Leggatt held that where the customer has authorised and instructed the bank to make a payment, the bank must carry out the instruction promptly, and that "[i]t is not for the bank to concern itself with the wisdom or risks of its customer's payment decisions."[52] The *Quincecare* duty guards against an agent who misuses his authority; it has no application where the customer is herself the victim of APP fraud.[53]

The common law thus gave the same answer as the RBI's 2017 Circular. Parliament then changed it. Section 72 of the Financial Services and Markets Act 2023 required the PSR to impose a reimbursement requirement for APP scam payments made over the Faster Payments system.[54] The regime came into force on 7 October 2024. Payment firms must reimburse victims up to £85,000 per claim, generally within five business days, and the cost is shared equally between the sending firm and the firm that received the payment. Gross negligence by the consumer remains an exception, as does first-party fraud.[55]

---

[50] *Philipp v. Barclays Bank UK plc* [2023] UKSC 25, [1], [10]; U.K. SUPREME COURT, Case Summary, *Philipp v. Barclays Bank UK plc*, UKSC/2022/0075, https://supremecourt.uk/cases/uksc-2022-0075.

[51] *Barclays Bank plc v. Quincecare Ltd.* [1992] 4 All ER 363 (QB).

[52] *Philipp v. Barclays Bank UK plc* [2023] UKSC 25 [3].

[53] *Id.* [100].

[54] Financial Services and Markets Act 2023, c. 29, § 72 (U.K.); PAYMENT SYS. REGULATOR, *Specific Direction 20: Faster Payments APP Scam Reimbursement Requirement* ¶ 2.4 (Dec. 2023, amended July 2024), https://psr.org.uk/media/rqrpnb0w/amended-specific-direction-20-july-2024.pdf.

[55] Rob Bratby, *APP Fraud Reimbursement: The Evidence After One Year*, BRATBY LAW (July 6, 2026), https://bratby.law/app-fraud-reimbursement-evaluation/; FRESHFIELDS BRUCKHAUS DERINGER, *Authorised Push Payment Fraud: A New Mandatory Reimbursement Regime for UK PSPs* (Sept. 30, 2024), https://www.freshfields.com/en/our-thinking/briefings/2024/09/authorised-push-payment-fraud-a-new-mandatory-reimbursement-regime-for-uk-psps.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Figure 5 summarises the results. Eighteen months into the regime, the PSR reported that 88 per cent of the money lost to in-scope APP scams, some £316 million, had been reimbursed, against a reimbursement rate of 61 per cent reported by UK Finance for 2024, although the PSR cautions that the two figures differ in scope. Eighty-two per cent of claims were closed within five business days, and only 3 per cent were rejected because the customer had not taken enough care.[56] The regulator also found "no indication of people being significantly less cautious."[57] An independent evaluation by Frontier Economics found that, in the regime's first year, reimbursement of confirmed APP losses rose from 54 to 65 per cent by value, and that in-scope losses fell by about 21 per cent, roughly £73 million a year.[58] The fall in losses matters most. Making firms pay gave both sending and receiving firms a reason to invest in prevention.

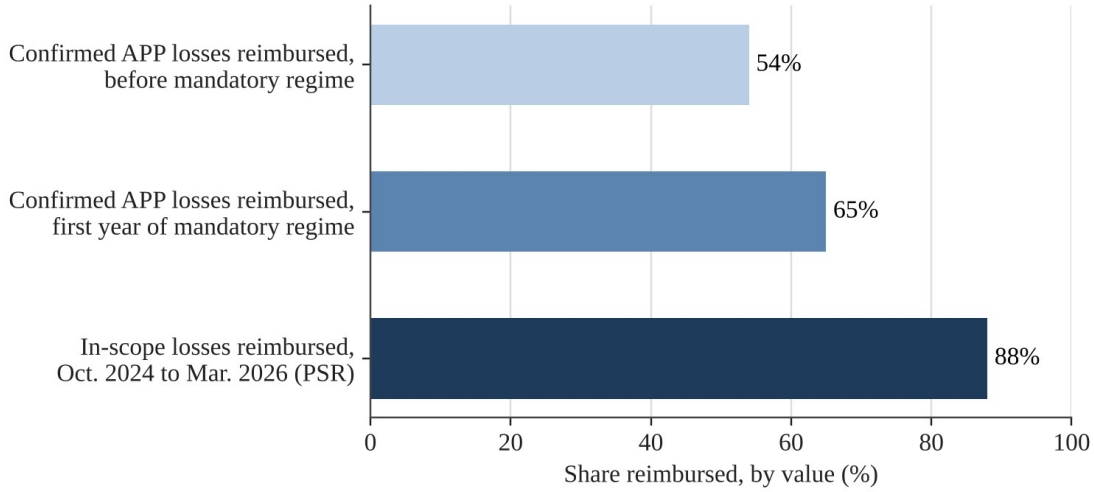


Figure 5: Reimbursement of APP scam losses in the United Kingdom before and after mandatory reimbursement. Source: Frontier Economics evaluation for the PSR, as reported (July 1, 2026); PSR, APP scams reimbursement dashboard for Q1 2026 (updated July 30, 2026). Chart by the author.

B. The European Union

The EU has taken a narrower path. Under the political agreement on a new Payment Services Regulation reached on 27 November 2025, a payment service provider must refund the full amount where a fraudster poses as one of its employees and tricks the customer into approving a payment, provided the customer reports the fraud to the police and informs the provider.[59] The

[56] PAYMENT SYS. REGULATOR, *APP Scams Reimbursement Dashboard for Q1 2026* (updated July 30, 2026), https://www.psr.org.uk/information-for-consumers/app-scams-reimbursement-dashboard/.
[57] *Id.*
[58] Simon Lovegrove & Charlotte Carnegie, *Payment Fraud Falls by £73m Following PSR Reimbursement Scheme*, GLOBAL REGULATION TOMORROW (July 1, 2026), https://www.regulationtomorrow.com/2026/07/payment-fraud-falls-by-73m-following-psr-reimbursement-scheme/; Bratby, *supra* note 55.
[59] Press Release, EUR. PARL., *Payment Services Deal: More Protection from Online Fraud and Hidden Fees* (Nov. 27, 2025), https://www.europarl.europa.eu/news/en/press-room/20251121IPR31540/payment-services-deal-more-protection-from-online-fraud-and-hidden-fees.

Council adopted its first-reading position on 28 October 2026.[60] The right is a genuine no-fault refund, but it is tied to impersonation of the bank. A digital-arrest victim, deceived by someone posing as the police, would fall outside it.

C. Singapore

Singapore's Shared Responsibility Framework, in force since 16 December 2024, assigns duties to financial institutions and telecom operators and allocates losses among them on a "waterfall" basis. It covers phishing scams with a digital link that lead to unauthorised transactions and expressly excludes authorised transactions.[61] A digital-arrest victim would recover nothing under it. Singapore, like India in 2017, chose to draw the line at the compromise of credentials.

D. Australia

Australia's Scams Prevention Framework Act 2025 inserted a new Part IVF into the Competition and Consumer Act 2010 and applies to banks, telecom providers and digital platforms once their sectors are designated.[62] It imposes duties to prevent, detect, report, disrupt and respond to scams, backed by penalties the government has described as reaching A$50 million, but it does not require businesses to compensate victims. Compensation runs through internal and external dispute resolution where a regulated business has failed to meet its obligations.[63] The first designations are expected to take effect on 31 March 2027.[64]

E. Lessons

Table 4 places the regimes side by side. Singapore protects only against unauthorised transactions, Australia relies on duties and fault-based redress, and the EU grants a no-fault refund for one kind of impersonation. The UK alone reimburses victims of authorised payment fraud generally, subject to a cap and narrow exceptions. India's 2026 Directions recognise coerced payments in their definition but compensate only small, negligence-based losses. Only the British model would repay a typical digital-arrest victim.

---

[60] *EU Payment Services Regulation: Banks Must Prevent Fraud and Pay Compensation*, LOVGUIDEN (Nov. 3, 2026), https://www.lovguiden.dk/en/det-offentlige/eur-lex-kommissionsforslag/2026-11-03-eu-payment-services-regulation-banks-must-prevent-fraud-and-pay-compensation.

[61] Eng Han Goh & Nicholas Tok, *Singapore to Implement Shared Responsibility Framework for Phishing Scams*, REED SMITH (Nov. 1, 2024), https://www.reedsmith.com/articles/singapore-to-implement-shared-responsibility-framework-for-phishing-scams/.

[62] Scams Prevention Framework Act 2025 (Cth) sch. 1 (Austl.).

[63] *Australia Enacts 'World-Leading' Scams Prevention Framework*, VIXIO (Feb. 17, 2025), https://www.vixio.com/insights/pc-australia-enacts-world-leading-scams-prevention-framework; GILBERT + TOBIN, *The Scams Prevention Framework Legislation Passes Parliament: Time to Get Your House in Order* (Feb. 2025), https://www.gtlaw.com.au/insights/the-scams-prevention-framework-legislation-passes-parliament-time-to-get-your-house-in-order2.

[64] Charlotte Henry, Chris Ninan & Chee Hian Kwah, *Australia's World-Leading Scams Prevention Framework Is Nearing Implementation*, FINANCIER WORLDWIDE (Aug. 2026), https://www.financierworldwide.com/australias-world-leading-scams-prevention-framework-is-nearing-implementation.

Regime	Covers coerced or deceived authorised payments?	Basis of liability	Cap	Receiving-side contribution
India: 2017 Circular	No	Fault; unauthorised transactions only	Full reversal where zero liability applies	None
India: 2026 Directions	In the definition, but no liability rule for a careful coerced customer	Fault, plus a small-loss compensation mechanism for negligent customers	₹25,000 (losses up to ₹50,000)	Beneficiary bank pays a small share
United Kingdom (from Oct. 2024)	Yes	Mandatory reimbursement, with narrow exceptions	£85,000 per claim	50% of reimbursement
European Union (agreed Nov. 2025)	Only where a bank employee is impersonated	No-fault refund	Full amount	Not specified
Singapore (Dec. 2024)	No; authorised transactions excluded	Duty-based "waterfall"	Not applicable	Telecom operators may bear losses
Australia (Act of 2025)	Only where a business breached its obligations	Fault-based redress through dispute resolution	Not fixed	Banks, telecoms and platforms may each be liable

Table 4: How five regimes treat scam payments authorised by the victim. Source: author's analysis of the sources cited in Parts 4 and 6.

VII. Why the loss should fall on the payment system

A. Coercion is not negligence

Indian law has long recognised that consent extracted by threats is not real consent. The Indian Contract Act, 1872 defines coercion to include threatening to commit any act forbidden by the penal law with the intention of causing a person to enter into an agreement, and makes an agreement so caused voidable at the option of the coerced party.[65] The analogy is not exact, since the victim's instruction is given to her bank rather than to the person threatening her, but the principle that consent obtained by threat is defective applies with equal force. A digital-arrest victim acts under a threat of arrest, often after hours of supervised "custody" on camera. The 2026 Directions themselves name "coercion or duress" in their definition of fraud. It is inconsistent to recognise coercion at the stage of definition and then, at the stage of liability, either to give the coerced customer no rule at all or to treat her failure to resist as negligence.

The behavioural evidence points the same way. In Stanley Milgram's obedience study, 26 of 40 ordinary participants continued to the highest shock level on the instructions of an experimenter in a grey technician's coat whose only authority came from the setting of a university

[65] The Indian Contract Act, No. 9 of 1872, India Code (1872), §§ 15, 19.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

laboratory.[66] Digital-arrest scripts use far stronger cues: uniforms, case numbers and forged orders carrying the seal of the Supreme Court. At the hearing on 29 October 2026 the *amicus curiae* made the same point to the Court: it is fear of arrest that drives the victims.[67] A rule that labels compliance with apparent state authority as carelessness asks victims to be braver than ordinary people are. Fault-based rules work when the person who bears the loss could reasonably have avoided it. A frightened and isolated customer is the person least able to do so.

B. The cheapest cost avoider

Law and economics offers a second justification. Calabresi and Hirschoff argued that strict liability should fall on the party best placed to weigh the costs of an accident against the costs of avoiding it and to act on that judgment.[68] Calabresi had earlier framed the task as finding the activity with the readiest means of reducing those costs.[69] In coerced payment fraud that party is the banking system. Banks see every transaction and the customer's history. They can tell when a pensioner who has never sent more than a few thousand rupees suddenly breaks fixed deposits and sends lakhs to a new payee, and when an account opened a few weeks earlier starts receiving large sums and passing them on within minutes. The RBI itself studied the efficacy of transaction-monitoring systems in major banks during 2025-26.[70] Banks also have the tools: the RBI's innovation hub built MuleHunter.AI by studying nineteen patterns of mule-account behaviour with banks.[71] And they can spread the residual cost thinly across millions of accounts or insure against it. The victim has none of these advantages. Putting the loss on her deters no one, since nobody chooses to be terrorised, while putting it on banks pays for the systems that stop the fraud.

C. The receiving bank and the mule account

A digital-arrest fraud cannot succeed without a bank account to receive the money. Mule accounts are opened by banks under know-your-customer rules and are monitored by them. The Supreme Court's decision to let the Central Bureau of Investigation pursue bankers involved in opening such accounts recognises that part of the problem lies inside the banking system.[72] A

---

[66] Stanley Milgram, *Behavioral Study of Obedience*, 67 J. ABNORMAL & SOC. PSYCH. 371, 373, 376 (1963).
[67] Jain, *supra* note 6.
[68] Guido Calabresi & Jon T. Hirschoff, *Toward a Test for Strict Liability in Torts*, 81 YALE L.J. 1055, 1060 (1972).
[69] GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 155 (1970).
[70] RESERVE BANK OF INDIA, *supra* note 12, at 106.
[71] *RBI Innovation Hub Develops MuleHunter.ai to Combat Mule Account Frauds*, BUSINESS STANDARD (Dec. 6, 2024), https://www.business-standard.com/finance/news/rbi-innovation-hub-develops-mulehunter-ai-to-combat-mule-account-frauds-124120601042_1.html; *What Is MuleHunter.ai, RBI's Latest Initiative to Tackle Financial Frauds*, BUSINESS TODAY (Dec. 6, 2024), https://www.businesstoday.in/personal-finance/banking/story/what-is-mulehunterai-rbis-latest-initiative-to-tackle-financial-frauds-456480-2024-12-06.
[72] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 6(i) (S.C. Dec. 1, 2025) (order) (India).

rule that makes the receiving bank bear half the loss gives it a direct reason to tighten account opening and to act on suspicious inflows. That was the logic of the British equal split, and the evidence from the regime's first year, together with the regulator's data for its first eighteen months, suggests that the logic works. India's 2026 Directions accept the principle but give the beneficiary bank a token share, about ₹2,941 on a ₹25,000 payment, which is too small to change behaviour.

D. The moral-hazard objection

The strongest objection to reimbursement is that it may make customers careless or invite collusive claims, in which an account holder stages a "fraud" and then claims a refund. Both risks are real, but neither justifies the present allocation. Carelessness is an odd worry in a fraud that works by terror; the promise of reimbursement does not make anyone more willing to be threatened with arrest. Collusion can be handled as the UK handles it, by excluding first-party fraud and allowing time to investigate. A cap keeps exposure bounded, and a narrow gross-negligence exception covers the customer who ignores a specific, personal warning from her bank. Experience also answers the objection. In the UK, losses fell after reimbursement became mandatory,[73] and after eighteen months the regulator saw no sign that customers had become significantly less careful; only 3 per cent of claims failed for want of care.[74] And the RBI has itself moved some way in this direction, since its new mechanism can compensate a victim even where she shared a one-time password.[75]

VIII. A PROPOSAL: THE COERCED PAYMENT REIMBURSEMENT SCHEME

The RBI already has power to issue binding directions to banks under the Banking Regulation Act, 1949 and to participants in payment systems under the Payment and Settlement Systems Act, 2007.[76] A reimbursement scheme could therefore begin as an RBI direction. A lasting regime, however, should rest on statute, as the British one does, so that it does not depend on a regulator's discretion or on a court's continuing supervision. An amendment to the Payment and Settlement Systems Act requiring the RBI to maintain a reimbursement scheme for coerced and impersonation payments, on the model of section 72 of the British statute, would achieve this. The main features of the proposed Coerced Payment Reimbursement Scheme are set out in Table 5.

[73] Lovegrove & Carnegie, *supra* note 58.
[74] PAYMENT SYS. REGULATOR, *supra* note 56.
[75] *Hit by Digital Fraud?*, *supra* note 14; 2026 Directions ¶¶ 4(20C)(i), 76T(1).
[76] The Banking Regulation Act, No. 10 of 1949, INDIA CODE (1949), § 35A; The Payment and Settlement Systems Act, No. 51 of 2007, INDIA CODE (2007), § 18.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Element	Proposal	Reason
Scope	Authorised payments by individuals and micro-enterprises induced by threats or by impersonation of a public authority or financial institution	Closes the gap left by the 2017 Circular and the 2026 Directions; can later extend to other scams
Trigger	Presumption of reimbursement once the victim reports to the NCRP or helpline 1930 and to her bank within 30 days	Five days is unrealistic for victims who are isolated and promised a refund
Cap	₹10 lakh per claim; larger losses left to consumer and civil remedies on proof of fault	Covers the average case many times over while keeping exposure bounded
Cost sharing	50% sending bank, 50% bank holding the first receiving account, with recovery from banks further down the chain	Gives both ends of the payment a reason to prevent fraud
Timing	Credit within 10 working days, extendable to 35 days where first-party fraud is suspected	Builds on the ten-day shadow reversal in the 2017 Circular
Exceptions	Complicity; gross negligence, limited to disregarding a specific, personal intervention by the bank	Prevents abuse without penalising frightened victims
Vulnerable customers	No gross-negligence exception for customers aged 60 or above or living with a disability	Senior citizens are frequent targets
Prevention duties	Payee-name confirmation; short hold on unusual first-time high-value transfers; temporary debit holds on suspected mule accounts	Builds on the Court's directions and the RBI's draft KYC amendments
Transparency	RBI to publish bank-wise data on scam reports and reimbursements	Public comparison sharpens incentives
Recourse	Banks may recover from telecom operators and platforms that breached their own duties	Spreads cost to other links in the fraud chain

Table 5: The proposed Coerced Payment Reimbursement Scheme. Source: author's proposal.

Four design choices need explanation. A cap of ₹10 lakh is many times the average reported loss, yet leaves the largest claims to consumer forums and civil courts, where fault can be examined in detail. A thirty-day reporting window reflects how these frauds unfold: victims are isolated, told to keep silent and promised a refund, and many realise the truth only after the calls stop. An equal split between the sending bank and the bank holding the first receiving account mirrors the British design, and recovery down the chain pushes the cost towards the accounts that moved the money. Finally, funding. The RBI's share of 65 per cent in the 2026 mechanism may suit a one-year pilot, but a central bank subsidy weakens the incentive that liability is meant to create. A permanent scheme should place the cost on the institutions whose systems can prevent the loss.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Reimbursement must work alongside prevention: payee-name confirmation, a short hold on unusually large first-time payments and temporary debit holds on suspected mule accounts would all reduce losses at source. The Court has already directed work on the last of these and has listed temporary suspension of unusual transactions among the safeguards it expects,[77] and the RBI's draft KYC amendments respond to that direction. Reimbursement gives banks a continuing financial reason to make such measures work.

IX. CONCLUSION

Indian law has treated a digital-arrest payment as the victim's own decision because, in a narrow technical sense, it is. She typed the password and approved the transfer. But a payment made because a uniformed stranger on a video call has threatened arrest is not a free choice, and a liability rule built on the fiction that it is places the loss on the person least able to prevent it. The 2026 Directions take an important first step by naming coercion in the definition of fraud. But a coerced customer who took reasonable care falls under none of their liability rules, and their compensation mechanism confines relief to negligent customers' losses of ₹50,000 or less, once in a lifetime and for a single year, while the average reported digital-arrest loss in 2024 exceeded ₹1.5 lakh.

The comparative evidence shows that a better rule is workable. The United Kingdom faced the same doctrinal wall in *Philipp*, removed it by statute, and has since seen reimbursement rise and losses fall. India can do the same, adapted to its own payment system: a presumption of reimbursement for coerced and impersonation payments, an equal split between the sending and receiving banks, a cap high enough to cover the real distribution of losses, and exceptions narrow enough not to punish fear. The Supreme Court has opened the door with its October 2026 direction. The task now belongs to the RBI and, ultimately, to Parliament. A payment system that depends on public trust should not leave the cost of these frauds with the customers it exists to serve.

*****

[77] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 7(i) (S.C. Aug. 4, 2026) (order) (India); *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025, ¶ 5 (S.C. Oct. 29, 2026) (order) (India).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]