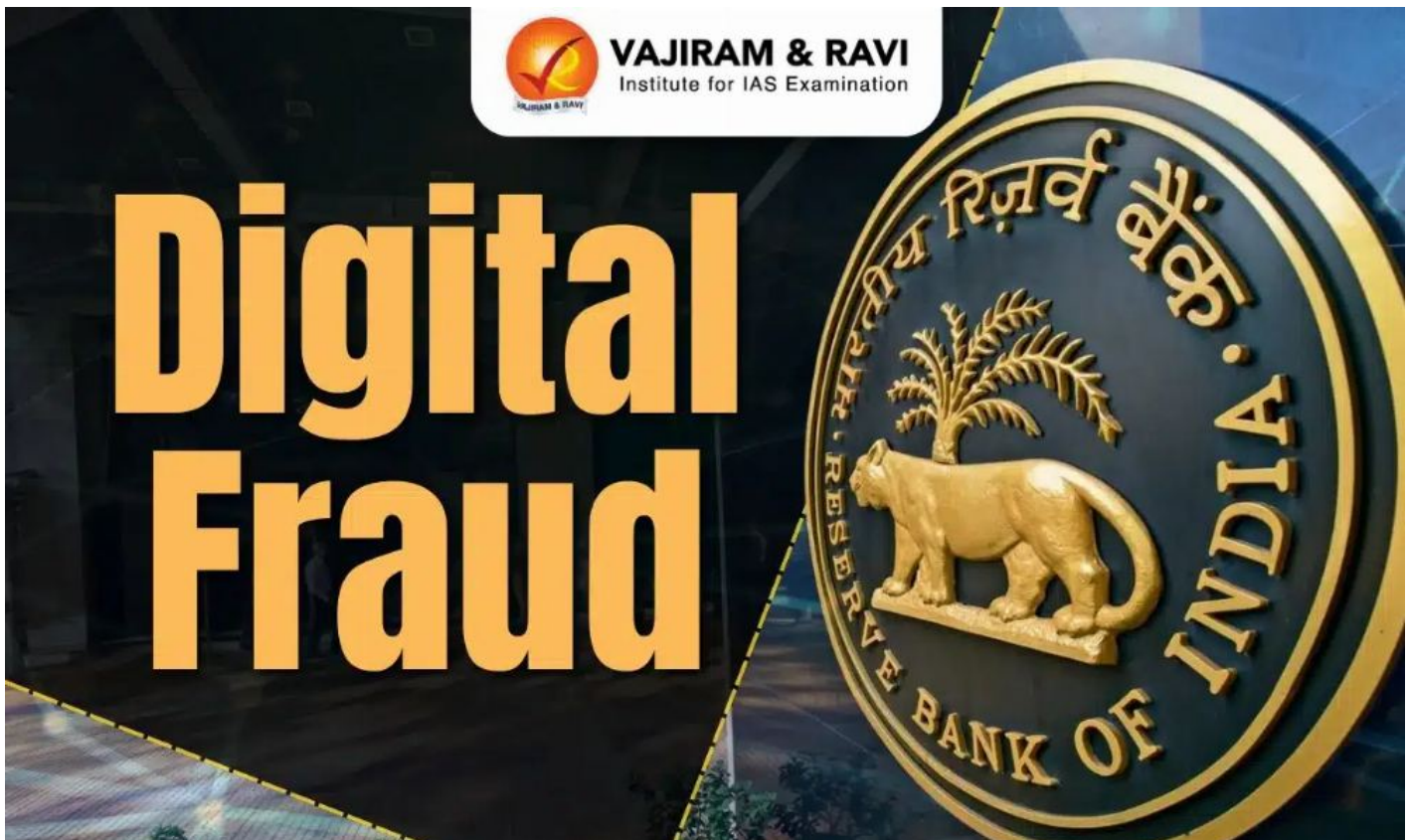


RBI Digital Fraud Compensation Rules: Key Changes to Protect Victims of Online Banking Fraud

June 25, 2026 • vajiramandravi.com



Digital Fraud Latest News

- The Reserve Bank of India (RBI) has unveiled a revised compensation framework for victims of digital payment frauds under the **RBI (Commercial Banks — Responsible Business Conduct) Third Amendment Directions, 2026**.
- The new rules take effect for electronic banking transactions (EBTs) occurring on or after January 1, 2027.

Digital Payment Frauds: Nature, Scale, and India's Regulatory Response

- India's rapid shift to digital payments — driven by UPI, mobile banking, net banking, and credit/debit cards — has been accompanied by a sharp rise in financial fraud.
- **Common types** of digital payment frauds include SIM swapping, phishing, vishing (voice call fraud), OTP theft, fake UPI handles, QR code scams, and increasingly sophisticated AI-driven deepfake frauds.

- **Vulnerable populations** — elderly citizens, first-time digital users, and rural consumers — are disproportionately affected.
- The scale of the problem is significant. In 2023-24, RBI reported over 36,000 fraud cases involving Rs 13,930 crore in the banking sector.

RBI Steps to Address the Issue of Digital Payment Frauds

- **Limited Liability Framework (2017, updated)** – RBI’s earlier circular on Customer Protection — Limiting Liability of Customers in Unauthorised Electronic Banking Transactions established the principle that customers bear zero or limited liability if they report fraud promptly. The 2026 revision builds on and strengthens this framework.
- **UPI Transaction Limits and Two-Factor Authentication** – RBI mandates two-factor authentication (2FA) for all digital transactions. UPI transactions require both device binding and UPI PIN. Additional friction has been introduced for large-value transactions to reduce impulsive fraud-driven transfers.
- **Real-Time Fraud Monitoring** – RBI has directed banks to implement real-time transaction monitoring systems to flag suspicious patterns. Banks are required to maintain a **Fraud Risk Management system** and report frauds above Rs 1 lakh to the Central Fraud Registry.
- **Mule Account Crackdown** – RBI and banks have been directed to identify and freeze mule accounts — accounts used by fraudsters to receive and quickly transfer stolen funds. These are a critical link in the digital fraud chain.
- **RBI’s ‘100 Days 100 Pays’ Campaign** – RBI launched this initiative to trace and return the top 100 unclaimed deposits in every bank within 100 days. While focused on unclaimed deposits, it reflects the broader push for financial accountability and consumer protection.

Remaining Challenges

- Despite these steps, significant gaps remain. Public awareness — especially in semi-urban and rural areas — is still low.
- Fraud recovery rates are poor. Cross-border frauds are difficult to prosecute.
- Mule account networks are sophisticated and rapidly evolving.
- AI-enabled deepfake voice frauds and social engineering attacks are outpacing regulatory responses.

News Summary: Key Changes in Compensation Rules

- **Who Is Eligible** – A bona fide victim who reports the fraud to the National Cyber Crime Reporting Portal or National Cyber Crime Helpline (1930) AND to their bank — within five calendar days of the fraud occurring — is eligible for compensation. This benefit is available once in a lifetime.
- **How Much Is Compensated** – For losses up to Rs 50,000: the victim receives 85% of the net loss amount or Rs 25,000, whichever is less.

Who Bears the Compensation Cost

- **Domestic Fraud — Loss Below Rs 29,412** (85% compensation applies) – RBI bears 65%, customer's bank bears 10%, beneficiary bank bears 10%.
- **Domestic Fraud — Loss Between Rs 29,412 and Rs 50,000** (Rs 25,000 fixed compensation) – RBI contributes Rs 19,118, customer's bank Rs 2,941, and beneficiary bank Rs 2,941.
- **Cross-Border Fraud** – RBI bears 65% and the customer's bank bears 20% (no beneficiary bank liability since it is foreign).
- The beneficiary bank is the bank where the fraudulently debited amount is first credited.
- If multiple beneficiary banks are involved, the liability is shared proportionally based on amounts credited.

Special Provisions

- **Credit Card Fraud** – For fraudulent EBT on a credit card, the bank must provide a shadow reversal — a temporary hold restoring the disputed amount — within five calendar days of receiving the customer's complaint.
- **Post-Recovery Adjustment** – If money is recovered after compensation has already been paid, the bank must recalculate the actual net loss and adjust the compensation accordingly — paying additional amounts or accounting for excess already paid.

Source: **IE** | **ET**

Source: <https://vajiramandravi.com/current-affairs/rbi-digital-fraud-compensation-rules-to-protect-victims-of-online-banking-fraud/>

© Vajiram & Ravi. For personal use only.