Draft RBI (Commercial Banks – Responsible Business Conduct) Third Amendment Directions, 2026

RBI Proposes Overhaul of Digital Fraud Liability Framework: Key Changes and Implications

The Reserve Bank of India has released **draft** Third Amendment Directions to the RBI (Commercial Banks – Responsible Business Conduct) Directions, 2025. These amendments overhaul the framework for customer protection in electronic banking transactions – replacing the existing Section D ("Limiting Liability of Customers in Unauthorised Electronic Banking Transactions") with an entirely new Section DA ("Customer Protection in Electronic Banking Transactions").

The draft is open for public comment until **April 6, 2026**, and if notified, will apply to electronic banking transactions on or after **July 1, 2026**. Similar drafts are also published with respect to Small Finance Banks, Payments Banks, Regional Rural Banks, and Local Area Banks.

The Context

The existing framework dates back to the circular titled "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions" dated July 06, 2017, which was later consolidated into the 2025 Master Directions. That 2017 framework was designed for a simpler era of digital payments. Since then, UPI alone has scaled to billions of transactions per month, and the nature of fraud has shifted dramatically:

- **Volume of small-value frauds**: According to RBI Governor Sanjay Malhotra, nearly 65% of digital frauds involve amounts below ₹50,000.
- **New fraud types**: Social engineering, phishing, OTP-sharing scams, and coerced transactions (where victims are tricked into sending money themselves) were not adequately covered by the old "unauthorised transaction" definition.
- **Burden of proof gap**: Under the old framework, customers often struggled to prove their innocence; the new draft reverses this by placing the burden on banks.
- **No compensation for "authorised-but-fraudulent" transactions**: If you were tricked into entering your own OTP, you technically "authorised" the transaction – the old framework left you with no recourse.

Major Changes at a Glance

Aspect	Old Framework (2017/2025)	New Draft (2026)
Scope	Only "unauthorised" electronic banking transactions	All "fraudulent" electronic banking transactions – covers both unauthorised AND authorised-but-fraudulent (coerced, tricked, phished)
Burden of Proof	Effectively on the customer to prove innocence	Explicitly on the bank to prove customer liability (Para 76K)
Reporting Timeline	3 working days for zero liability; 4–7 days for limited liability; beyond 7 days – bank's policy	5 calendar days for zero liability (third-party breach) or compensation eligibility; beyond 5 days – bank's policy
Customer Liability (Bank Negligence)	Zero liability	Zero liability (unchanged) – even if unreported (Para 76L)

Customer Liability (Customer Negligence)	Customer bears full loss until reporting	Customer bears loss, BUT may still get partial compensation up to ₹25,000 under the new mechanism (Para 76N + 76T)
Limited Liability Caps (Third-party breach, delayed report)	Tiered: ₹5,000 / ₹10,000 / ₹25,000 based on account type	Replaced by compensation mechanism: 85% of net loss or ₹25,000, whichever is lower (Para 76T)
Compensation Mechanism	None – only shadow reversal within 10 working days	NEW: 85% of net loss (max ₹25,000), cost shared among RBI (65%), customer's bank (10%), and beneficiary bank (10%)
Compensation Eligibility	N/A	Once-in-a-lifetime per individual; gross loss up to ₹50,000; must report to bank + NCRP/1930 within 5 days
Complaint Resolution	90 working days	30 calendar days (Para 76Q)
SMS Alerts	Mandatory for all electronic transactions	Mandatory instant SMS for transactions > ₹500; bank's discretion for ≤₹500 (Para 76D)
SMS Charges	Not explicitly addressed	Banks cannot charge for regulatory/promotional/awareness SMS (Para 85 substituted)
Rejected Complaint Disclosure	Not specified	Bank must disclose reason with supporting evidence (OTP logs, SMS logs, transaction logs) (Para 76S)
RBI as Financial Contributor	No – RBI had no direct financial stake	Yes – RBI contributes 65% of compensation amount (first time ever)
Duration of Compensation Scheme	N/A	One year from effective date (Para 76U); intent to gradually shift burden to banks

New Definitions Introduced

The draft introduces several critical definitions that did not exist in the old framework:

New Term	What It Means & Why It Matters
Authorised Electronic Banking Transaction (Para 4(3A))	Includes: (i) transactions with OTP/PIN/password authentication; AND critically (ii) transactions where customer was tricked, coerced, or had credentials stolen. This means even OTP-authenticated scam transactions are now "authorised but fraudulent" – bringing them within the protection framework.
Fraudulent Electronic Banking Transaction (Para 4(15A))	A new umbrella term covering BOTH authorised-but-fraudulent transactions (Para 4(3A)(ii)) AND unauthorised transactions. This is the key definitional expansion.
Negligence by Bank (Para 4(20A))	Defined with 5 specific instances: failure to implement security systems, failure to send alerts, failure to provide reporting channels, failure to act on

	customer notification, and system malfunctions/security breaches/internal fraud.
Negligence by Customer (Para 4(20B))	Defined with 5 specific instances: sharing credentials (even unintentionally), delayed reporting, ignoring clear scam warnings from bank, failing to safeguard credentials (e.g., PIN stored with card), and downloading malicious apps.
Third-Party Breach (Para 4(26A))	Fault lies with neither bank nor customer but with intermediaries: TPAPs, Payment Aggregators, Payment Gateways, Telecom Service Providers, etc.
Unauthorised Electronic Banking Transaction (Para 4(26B))	Residual definition: any e-banking transaction that does NOT qualify as "authorised."

Compensation Mechanism under Para 76T of the Directions

This is the most novel feature of the draft. For the **first time ever**, RBI will contribute directly to compensating fraud victims.

Who is Eligible?

- **Individual persons** only (not corporates/firms)
- **Gross loss up to ₹50,000** from fraudulent electronic banking transactions
- Complaint falls under Para 76M (third-party breach, reported after 5 days) or Para 76N (customer negligence)
- Loss is **bona fide** as per the bank's internal policy
- Reported to **both** the bank AND the National Cyber Crime Reporting Portal / Helpline (1930) within **5 calendar days**
- **Once in a lifetime** per individual (joint account claim exhausts individual's eligibility too)

How Much Compensation?

Loss Amount	Compensation	RBI's Share	Each Bank's Share
Less than ₹29,412	85% of net loss	65% of net loss	10% each (customer's bank + beneficiary bank)
₹29,412 to ₹50,000	₹25,000 (flat cap)	₹19,118	₹2,941 each

Note: The ₹29,412 threshold is the breakpoint where 85% equals ₹25,000 (i.e., 85% × ₹29,412 = ₹25,000).

Practical Examples

Example 1: OTP Phishing Scam (₹20,000 lost)

Ravi, a retired person, receives a call from someone posing as his bank's KYC officer. Under pressure, he shares his OTP. ₹20,000 is debited from his account. He reports it to the bank and files a complaint on the 1930 helpline within 2 days.

- **Classification**: Authorised-but-fraudulent transaction (credentials shared under deception) – customer negligence under Para 4(20B)(i).

- **Old framework**: Customer bears entire loss (he shared OTP = negligence). No compensation.
- **New framework**: Despite customer negligence, Ravi is eligible for compensation: 85% of ₹20,000 = **₹17,000**. RBI pays ₹13,000 (65%), each bank pays ₹2,000 (10%). Ravi's effective loss: ₹3,000.

Example 2: Payment Gateway Breach (₹40,000 lost)

Meera's card details are stolen through a compromised payment gateway. ₹40,000 is siphoned off. She reports within 3 days. The bank recovers ₹15,000 before compensation.

- **Classification**: Third-party breach (Para 4(26A)) – reported within 5 days = zero liability under Para 76L.
- **Old framework**: If reported within 3 working days = zero liability. Same outcome.
- **New framework**: Zero liability; bank must reverse the full ₹40,000 with value dating. The compensation mechanism (Para 76T) is not needed here because zero liability already applies.

Example 3: Third-Party Breach Reported Late (₹40,000 lost)

Same facts as Example 2, but Meera discovers the fraud only after 8 days and reports then. Bank recovers ₹15,000.

- **Classification**: Third-party breach, reported AFTER 5 calendar days – falls under Para 76M.
- **Old framework (reported after 7 working days)**: Liability as per bank's board-approved policy. Likely full loss.
- **New framework**: Net loss = ₹40,000 – ₹15,000 = ₹25,000. Compensation = 85% of ₹25,000 = **₹21,250**. RBI pays ₹16,250; each bank pays ₹2,500. Meera's effective loss: only ₹3,750.

Example 4: Customer Ignores Bank's Scam Warning

Ajay is about to transfer ₹45,000 to someone posing as a customs officer. His bank sends a specific, clear warning that this looks like a scam. Ajay ignores it and proceeds. He reports within 4 days.

- **Classification**: Authorised-but-fraudulent + customer negligence (Para 4(20B)(iii) – ignored clear scam warning).
- **Old framework**: Not covered at all (Ajay "authorised" the transaction himself).
- **New framework**: Despite negligence, compensation applies: 85% of ₹45,000 would be ₹38,250 but is capped at **₹25,000**. RBI pays ₹19,118; each bank pays ₹2,941. Ajay's effective loss: ₹20,000.

Liability Determination Flowchart (New Framework)

Under the new directions, banks must classify each complaint into one of the following categories:

Scenario	Who Is at Fault?	Reporting Timeline	Customer's Liability	Reference
A	Bank negligence	Irrelevant (even if unreported)	ZERO – full reversal	Para 76L
B	Third-party breach	Within 5 calendar days	ZERO – full reversal	Para 76L
C	Third-party breach	After 5 calendar days	Compensation mechanism applies (85% / ₹25K cap)	Para 76M + 76T
D	Customer negligence	Within 5 calendar days	Bears loss, BUT compensation mechanism applies (85% / ₹25K cap)	Para 76N + 76T
E	Customer negligence	After 5 calendar days	Full loss (no compensation)	Para 76N

New/Enhanced Bank Obligations

Obligation	Details
Board-level Policy	Banks must formulate a transparent, non-discriminatory policy on customer protection, displayed on website with grievance escalation details (Para 76A)
Security Systems	Must comply with Master Direction on Digital Payment Security Controls + have robust, dynamic fraud detection (Para 76B)
Mandatory Mobile Registration	Banks must require customers to provide mobile number (and email where available) for all e-banking except ATM withdrawals (Para 76C)
Instant SMS Alerts	Mandatory for transactions > ₹500; bank's discretion for ≤₹500 (Para 76D)
Email Alerts	Mandatory for ALL e-banking transactions where email is provided (Para 76E)
24×7 Multi-Channel Reporting	Phone banking, SMS, email, IVR, toll-free helpline, home branch – all must be available round the clock (Para 76G)
SMS Reply for Objections	Transaction alert SMS must include a number for the customer to immediately object via SMS (Para 76G(2))
Website Reporting Link	Direct link on bank's homepage for reporting fraud (Para 76G(3))
Instant Acknowledgement	System must auto-register complaint and send acknowledgement with complaint number + date/time (Para 76I)
Immediate Freezing	On receiving fraud complaint, bank must immediately prevent further unauthorised transactions in the account (Para 76J)

30-Day Resolution	Examine, establish liability, and respond within 30 calendar days (down from 90 working days) (Para 76Q)
Value-Dated Reversal	Reversal must be backdated to original transaction date; no interest burden or extra charges on customer (Para 76R)
Transparency on Rejection	If complaint is rejected, bank must share OTP logs, SMS logs, transaction logs etc. with customer (Para 76S)
Board Monitoring	Periodic reporting to Board/Committee on volume, value, and category of fraud complaints; review of grievance redressal (Para 76V)
No SMS Charges	Banks cannot charge for SMS sent for regulatory compliance or promotional/awareness purposes (Substituted Para 85)
Compensation Payout	Within 5 calendar days of receiving customer's application form (Para 76T(5))

What Should Customers Know?

Under the new framework, customers benefit significantly but also have clear obligations:

Customer Rights	Customer Obligations
Zero liability if bank is at fault (even without reporting)	Must provide mobile number (and email) to the bank
Zero liability for third-party breach if reported within 5 days	Must report fraud to bank AND file complaint on NCRP/1930
Partial compensation (up to ₹25,000) even for own negligence	Must report within 5 calendar days for compensation eligibility
30-day resolution guarantee	Must not share PINs, OTPs, passwords with anyone
Full transparency if complaint is rejected (logs shared)	Must pay attention to bank's scam warnings
No SMS charges for regulatory/awareness messages	Must not download malicious apps or store PINs with cards

Critical Observations & Open Questions

1. **Once-in-a-lifetime cap**: The compensation is a one-time benefit. Repeat fraud victims get no further compensation under this mechanism. This may be inadequate for senior citizens or less digitally literate customers who are targeted repeatedly. We need to push "Cyber Insurances" with easier terms and higher cover to further bring the umbrella of protection.
2. **Aadhaar mandatory for claiming**: The application form (Annex II(1)) requires mandatory Aadhaar. This raises DPDP Act and privacy considerations, and may exclude customers without Aadhaar.
3. **Beneficiary bank identification**: If fraud proceeds go to crypto wallets, foreign accounts, or non-bank payment channels, identifying and collecting from the "beneficiary bank" may be impractical.
4. **One-year sunset clause (Para 76U)**: The compensation scheme applies only for one year from July 1, 2026. RBI has signalled it will gradually increase banks' share and reduce its own contribution. This creates regulatory uncertainty.

5. **"Calendar days" vs. "working days"**: The shift from working days (old) to calendar days (new) for reporting and resolution timelines is significant – it tightens timelines for customers (5 calendar days < 7 working days in practice) but also for banks (30 calendar days < 90 working days).
6. **Moral hazard concerns**: By compensating even negligent customers, there is a risk that customers become less careful. However, the once-in-a-lifetime cap and 85% (not 100%) recovery partially mitigate this.
7. **No coverage for large frauds**: Losses above ₹50,000 are outside the compensation mechanism entirely. The framework is silent on a structured redressal for high-value individual frauds.
8. **Customer awareness of scam warnings**: The new definition of customer negligence includes "not paying attention to specific, directed and clear warnings from the bank." This creates incentive for banks to issue more warnings, which may lead to warning fatigue.

Key Dates

Date	Event
March 6, 2026	Draft Amendment Directions released by RBI
April 6, 2026	Last date for public comments/feedback
July 1, 2026	Effective date (applicable to e-banking transactions from this date)
June 30, 2027	Compensation mechanism expires (one year from effective date); review expected