ECONOMIC LAWS PRACTICE
ADVOCATES & SOLICITORS

RBI Tightens Customer Protection Framework for Fraudulent Electronic Banking Transactions

The Reserve Bank of India (**RBI**), through the *Reserve Bank of India (Commercial Banks Responsible Business Conduct) Third Amendment Directions, 2026*, has overhauled the framework governing customer liability in fraudulent electronic banking transactions (**EBTs**)[1]. These revised directions will apply to all electronic banking transactions undertaken by customers on or after **January 1, 2027,** and replace the earlier regime on limiting customer liability in unauthorised electronic transactions.

The amendments come at a time when digital payments have become ubiquitous and incidents involving phishing, vishing, social engineering, credential theft, malicious applications, card frauds and other cyber-enabled financial crimes have increased significantly. Recognising the growing risks faced by customers, RBI has sought to rebalance the relationship between banks and customers by strengthening customer protection measures, imposing higher standards of diligence on banks, and introducing a more structured framework for determination of liability and compensation.

Burden of proof in case of EBT

A notable feature of the revised framework is that RBI has shifted the burden of proof in disputes involving fraudulent EBTs. The bank is now required to examine each complaint, classify it under the prescribed categories and establish customer liability wherever it seeks to deny reimbursement or compensation. In other words, the presumption is no longer automatically against the customer; rather, the bank must demonstrate that the loss arose due to customer negligence or otherwise falls outside the categories entitling the customer to protection

Obligation on Banks

The directions also impose significant operational obligations on banks. Banks are required to maintain robust fraud detection and prevention systems, provide 24x7 reporting channels, send transaction alerts, maintain records of customer complaints and acknowledgements, and act promptly upon receipt of reports of fraudulent transactions. They must formulate transparent board-approved policies detailing customer rights, complaint resolution timelines, liability determination mechanisms and grievance redressal procedures.

Zero Liability

From a customer's perspective, the revised framework provides substantial safeguards. Customers are entitled to **zero liability** where the fraud is attributable to negligence or deficiency on the part of the bank and, in specified cases involving third-party breaches, provided they report the fraud within the prescribed time. The directions further require banks to reverse eligible transactions without causing loss of interest to customers and introduce a compensation mechanism for certain categories of small-value frauds.

Evolution of the RBI Framework on Unauthorised Electronic Banking Transactions

The 2026 amendments build upon and substantially expand the customer protection framework that was already embedded in the Reserve Bank of India (Commercial Banks Responsible Business Conduct) Directions, 2025. The 2025 Directions had consolidated RBI's earlier instructions on unauthorised electronic banking transactions and established foundational principles such as mandatory transaction alerts, 24x7 reporting channels, prompt complaint registration, customer liability standards, reversal timelines, board-approved customer protection policies and, significantly, the principle that the burden of proving customer liability rests upon the bank.

[1] NT16738E653AADCEC4217BEFFA92C050F69AD.PDF

While the earlier framework principally dealt with "unauthorised electronic banking transactions", the 2026 amendments introduce a more comprehensive regime centred around "fraudulent electronic banking transactions" and provide considerably greater clarity regarding the allocation of liability among banks, customers and third parties.

The revised framework introduces detailed definitions of bank negligence, customer negligence and third-party breaches, strengthens reporting and investigation obligations, shortens resolution timelines, mandates transaction reversals in specified situations and introduces an innovative compensation mechanism for victims of small-value digital frauds. The amendments therefore represent a significant evolution from the earlier liability-limitation framework to a broader customer-protection regime aimed at enhancing trust and confidence in India's rapidly expanding digital payments ecosystem.

Regulatory Background

The RBI's approach to customer liability in digital frauds has evolved progressively over the last decade. The foundation was laid through the RBI Circular dated **6 July 2017 on "Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions"**, which introduced the concepts of zero liability, limited liability and mandatory reporting mechanisms. The 2025 Responsible Business Conduct Directions subsequently consolidated these requirements into a single master framework applicable to commercial banks. The 2026 amendments are therefore not a departure from the earlier regime but rather the next stage in RBI's continuing effort to strengthen consumer confidence in digital banking by making banks more accountable for fraud prevention, complaint handling and customer compensation.

Significance of the 2026 Amendments

From a policy perspective, three themes emerge clearly from the revised directions:

- ***Shift from customer fault to bank accountability****:* RBI has reinforced that the bank bears the burden of proving customer negligence and must classify and investigate every complaint before denying relief.
- ***Recognition of modern fraud typologies****:* The directions expressly recognise phishing, credential theft, coercion-based approvals, intermediary failures, payment aggregator failures, telecom-related breaches and other third-party ecosystem risks.
- ***Customer-centric restitution framework****:* The focus is no longer limited to determining liability. The directions now deal comprehensively with prevention, reporting, investigation, reversal, compensation, monitoring and governance, thereby creating an end-to-end consumer protection architecture.

Key Changes Introduced by RBI in the Framework Governing Fraudulent Electronic Banking Transactions (EBTs)

- **Introduction of the Concept of "Fraudulent Electronic Banking Transaction"**

One of the most significant changes is the introduction of the definition of "Fraudulent Electronic Banking Transaction" (Fraudulent EBT). Earlier, the framework primarily focused on unauthorised transactions. The revised definition now expressly covers:

- Transactions executed by a third party using customer credentials obtained through fraud;
- Transactions undertaken by customers themselves under coercion, intimidation or duress exerted by fraudsters;
- Transactions otherwise falling within the scope of unauthorised electronic banking transactions.

This change is important because it recognises modern fraud patterns where customers are manipulated into authorising transactions through social engineering, phishing, vishing, digital arrest scams, impersonation frauds and similar coercive practices. Such transactions can no longer be dismissed merely because the customer technically "authorised" the payment.

- **Statutory Recognition of Bank Negligence**

For the first time, RBI has expressly defined what constitutes "negligence by a bank". The definition includes:

- Failure to implement mandated security systems and controls;

- Failure to send mandatory transaction alerts;
- Failure to provide 24x7 fraud reporting mechanisms;
- Failure to act diligently upon customer complaints;
- System failures, cybersecurity breaches or internal frauds resulting in unauthorised transactions.

This is a significant strengthening of customer rights because banks can no longer rely upon broad or undefined standards while assessing liability. The Directions create objective benchmarks against which bank conduct can be evaluated.

- **Detailed Definition of Customer Negligence**

The amendments also specify circumstances that may constitute negligence by the customer, including: Sharing PINs, passwords, OTPs or other credentials; Failing to promptly report fraudulent transactions or loss of cards; Ignoring clear and specific scam warnings issued by the bank; Downloading malicious applications; Failing to update registered mobile numbers or email addresses.

By providing a non-exhaustive list, RBI seeks to bring greater certainty and consistency in determining customer liability.

- **Introduction of the Concept of "Third-Party Breach"**

The Directions introduce a specific category called "third-party breach", where the deficiency lies neither with the bank nor the customer but elsewhere within the payment ecosystem.

Illustrative examples include failures attributable to:

- Third Party Application Providers (**TPAPs**);
- Payment Aggregators;
- Payment Gateways;
- Telecom Service Providers; and
- Other intermediaries involved in the digital payments chain.

This recognises the increasingly complex payment ecosystem and allocates liability more appropriately.

- **Expanded Scope of Electronic Banking Transactions**

The amended framework introduces comprehensive definitions covering: Electronic Banking Transactions (**EBTs**); Card Present Transactions; Card Not Present Transactions; Fraudulent EBTs; and Unauthorised EBTs.

The revised framework, therefore, applies uniformly across the digital payments ecosystem and is no longer limited to conventional internet banking transactions.

- **Clear Allocation of Burden of Proof on Banks**

The Directions reiterate and strengthen the principle that, "The burden of proving customer liability shall lie on the bank." Banks are now specifically required to: Examine every complaint; Categorise the complaint appropriately; Establish the applicable category of fraud; and Demonstrate the basis for fixing liability on the customer.

This significantly shifts the evidentiary burden away from customers.

- **Expanded Zero Liability Protection**

Customers are entitled to complete reversal of the transaction and zero liability where the fraud occurred due to negligence or deficiency on the part of the bank; or the fraud resulted from a third-party breach and is reported within five calendar days.

The earlier framework was based on reporting within specified working days. The revised framework simplifies and strengthens customer protection.

- **Recognition of Customer Liability Only in Cases of Proven Negligence**

The Directions now expressly state that customer liability arises only where the fraudulent EBT occurs due to customer negligence. The bank must, therefore, establish customer negligence before denying reimbursement.

- **Complete Protection for Transactions Occurring After Reporting**

The Directions clarify that once a fraudulent transaction is reported, any subsequent unauthorised transaction shall be borne entirely by the bank. This places responsibility on banks to immediately freeze or secure the relevant account, card or payment instrument after notification.

- **Mandatory Complaint Resolution Timelines**

Banks are now required to resolve domestic fraud complaints within 45 calendar days; and resolve cross-border fraud complaints within 60 calendar days.

- **Mandatory Value-Dated Reversal**

Where reversal is warranted, the bank must ensure that the reversal is value dated to the original transaction date; customers do not suffer loss of interest; and customers are not subjected to additional charges or interest burdens.

This prevents customers from suffering indirect financial losses while the complaint remains under investigation.

- **Introduction of Shadow Reversal Mechanism**

A new concept of "shadow reversal" has been introduced. Under this mechanism:

  - In credit card fraud cases, banks must provide provisional credit equivalent to the disputed amount within five calendar days of notification.
  - Customers are protected from interest and penal charges during investigation.

- **Compensation Scheme for Small-Value Digital Fraud Victims**

Perhaps the most innovative change is the introduction of a compensation mechanism for bona fide victims of small-value fraudulent EBTs. This is applicable to losses up to ₹50,000; and provide for compensation up to 85% of net loss, subject to a cap of ₹25,000. This is applicable where fraud is reported both to the bank and the National Cyber Crime Reporting Portal within five calendar days. The compensation burden is shared among RBI, the customer's bank and, where applicable, the beneficiary bank.

- **Greater Governance and Board Oversight**

Banks are now required to formulate dedicated policies on fraudulent EBTs; maintain monitoring and reporting mechanisms; periodically report fraud complaints to the Board or designated committee and review complaint trends and systemic weaknesses.

- **Shift from Liability Determination to Customer Protection**

The most fundamental change is philosophical. The earlier framework focused primarily on determining the extent of customer liability. The revised Directions adopt a broader customer protection approach encompassing: Prevention, Fraud detection, Customer awareness, Reporting mechanisms, Liability allocation, Reversal of transactions, Compensation, Governance and oversight.

Obligations of Customers under the Revised Fraudulent EBT Framework

While the revised Directions significantly strengthen customer protection and place substantial responsibility on banks, RBI has also emphasized that customers have an important role in preventing and mitigating losses arising from fraudulent electronic banking transactions. The framework is therefore based on a principle of shared responsibility, under which customers are expected to exercise vigilance and promptly report suspicious transactions.

- **Duty to Promptly Report Fraudulent Transactions**

The most important obligation cast upon customers is to report any fraudulent electronic banking transaction immediately upon becoming aware of it. The Directions repeatedly emphasize that delays in reporting increase the risk of financial loss and may adversely affect the customer's entitlement to reimbursement or compensation. Customers are therefore expected to notify the bank at the earliest opportunity after detecting a fraudulent transaction or loss of a payment instrument.

- **Duty to Report Fraud through Official Cyber Crime Channels**

A significant new feature of the revised framework is the expectation that customers should not merely inform the bank but should also lodge complaints through the National Cyber Crime Reporting Portal or the National Cyber Crime Helpline (1930). RBI has expressly required banks to advise customers to report frauds through these channels at the earliest.

- **Duty to Preserve Evidence and Complaint Records**

Customers should retain copies of transaction alerts, complaint acknowledgements, cybercrime complaint numbers and all communications exchanged with the bank. Since the timing of reporting may determine entitlement to zero liability, compensation or reimbursement, maintaining documentary evidence of complaints becomes critical.

- **Duty to Monitor Transaction Alerts**

The revised framework presumes that customers will actively monitor SMS alerts, email alerts and other transaction notifications sent by banks. Prompt review of transaction alerts enables early detection of fraud and facilitates immediate reporting. Failure to review alerts or prolonged inaction after receiving notifications may be relied upon by banks while assessing customer negligence.

- **Duty to Cooperate with Fraud Investigation**

Customers are expected to provide relevant information, transaction details and supporting documents sought by the bank during investigation of a fraudulent EBT.

- **Duty to Protect Banking Credentials**

The Directions expressly identify customer negligence to include failure to exercise reasonable care in protecting credentials such as PINs, passwords, OTPs and other authentication details. Customers are therefore expected to maintain confidentiality of such credentials and avoid sharing them with any person, whether intentionally or inadvertently.

- **Duty to Heed Scam Warnings Issued by Banks**

The revised framework introduces a new concept whereby customer negligence may be established if the customer disregards specific, directed and clear warnings issued by the bank that a proposed transaction is likely to be fraudulent. This places an obligation on customers to exercise caution when banks generate scam alerts or warnings during digital transactions.

- **Duty to Maintain Secure Digital Practices**

Customers are expected to avoid downloading malicious or unverified applications and to adopt reasonable cyber hygiene practices while using digital banking channels. The Directions specifically identify downloading malicious applications as an instance of customer negligence.

- **Duty to Keep Contact Information Updated**

Customers are required to ensure that their registered mobile number and email address remain current. Failure to update contact details with the bank may result in non-receipt of transaction alerts and has been specifically identified as a form of customer negligence under the Directions.

- **Duty to Immediately Report Loss of Cards or Payment Instruments**

Customers are expected to promptly report loss, theft or compromise of debit cards, credit cards or other payment instruments through the various reporting channels provided by banks. Immediate reporting enables the bank to block further transactions and minimise losses.

Thus, the revised framework seeks to strike a balance between customer protection and customer responsibility. While the burden of proving customer negligence remains on the bank, customers who fail to exercise reasonable care, ignore fraud warnings, delay reporting fraudulent transactions or fail to maintain updated contact information may face exposure to liability under the framework.

Introduction of a Compensation Mechanism for Small-Value Fraudulent EBTs

Another noteworthy innovation introduced by the 2026 Directions is a dedicated compensation mechanism for victims of small-value fraudulent electronic banking transactions. Under the scheme, an individual customer (including a sole proprietor) who suffers a loss of up to ₹50,000 due to a fraudulent EBT and whose claim is found to be bona fide is entitled, once in a lifetime, to compensation equal to 85% of the net loss suffered or ₹25,000, whichever is lower. To avail this

benefit, the customer must report the fraudulent transaction both to the bank and through the National Cyber Crime Reporting Portal or National Cyber Crime Helpline (1930) within five calendar days of its occurrence.

The compensation mechanism is funded through a unique cost-sharing arrangement involving the Reserve Bank of India, the customer's bank and, in domestic fraud cases, the beneficiary bank receiving the fraudulently transferred funds. For smaller losses, RBI bears the major portion of the compensation, while the customer's bank and beneficiary bank share the balance. The Directions also contain detailed provisions for recalculating compensation where recoveries are subsequently made from fraudsters and for reimbursement claims by banks from RBI and beneficiary banks.

The scheme is intended as a limited and transitional customer protection measure and applies only to fraudulent EBTs occurring within one year from the effective date of the Directions.

Judicial Approach to Liability of Banks in Unauthorised Electronic Transactions

Although the RBI framework is the primary source governing customer liability in electronic banking frauds, courts and consumer fora have increasingly emphasised that banks bear a significant responsibility to maintain secure payment systems and cannot automatically shift losses arising from cyber frauds onto customers.

- **Subodh Korde v. HDFC Bank Ltd. (Bombay High Court, 2026)[2]**

One of the most significant recent decisions is the judgment of the Bombay High Court directing HDFC Bank to reimburse approximately ₹38 lakh lost by a customer through a sophisticated SIM-swap fraud. The Court held that the customer had acted diligently and had promptly reported the fraudulent transactions. Relying upon the RBI's 2017 Circular on customer liability in unauthorised electronic banking transactions, the Court held that the burden of establishing customer negligence rested upon the bank and that mere proof of OTP generation or authentication was insufficient to deny reimbursement.

- **Rakesh Totuka v. IDBI Bank (Rajasthan High Court, 2025)[3]**

In another significant decision, the Rajasthan High Court upheld directions requiring IDBI Bank to refund approximately INR 38.93 lakh lost through multiple fraudulent online transfers. The Court rejected the bank's contention that the customer may have been negligent and held that, in the absence of evidence establishing customer fault, liability could not be shifted to the account holder. The Court emphasised that banks are responsible for maintaining robust security systems capable of preventing unauthorised access and cyber frauds and that third-party cyber breaches cannot automatically be attributed to customers.

- **Namrata Naman Jha v. Indian Bank (District Consumer Commission, Chandigarh, 2025)[4]**

The Chandigarh Consumer Commission directed Indian Bank to refund amounts withdrawn through unauthorised ATM transactions after finding that the customer had immediately reported the fraud and blocked the card. The Commission held that the bank had failed to discharge the burden imposed under the RBI framework of proving customer negligence and consequently could not deny reimbursement. The decision reiterates the principle that once timely reporting is established, the bank must affirmatively prove customer fault before rejecting a claim.

- **State Bank Of India vs Sri. Prodosh Kumar Banerjee (NCDRC, 2026)[5]**

In a case involving fraudulent withdrawals of approximately INR 1.99 lakh following a seemingly innocuous online transaction, the National Consumer Disputes Redressal Commission directed State Bank of India to refund the amount together with compensation. The Commission underscored that banks cannot evade responsibility where customers promptly report unauthorised electronic transactions and the bank fails to demonstrate negligence on the part of the customer.

Emerging Judicial Principles

The following principles emerge consistently from the reported decisions:

[2] Subodh C Korde vs Union Of India Through Ministry Of Finance Decided on 6 April, 2026- Writ Petition NO.11990 OF 2023
[3] Idbi Bank Limited vs Rakesh Totuka S/O Lt. Sh. Prakash Chand – Decided on 12 November, 2025- D.B. Special Appeal Writ No. 927/2025
[4] Consumer Complaint No. DC/AB1/44/CC/56/2021- decided on 17.11.2025
[5] Second Appeal No. 540 OF 2025- Decided on 15.04.2026

- **The burden of proving customer negligence lies on the bank.**
- **Prompt reporting by the customer is a critical factor in determining liability.**
- **Mere use of OTPs, passwords or authentication credentials does not by itself establish customer authorisation or negligence.**
- **Banks are expected to maintain robust fraud detection and security systems.**
- **Where customer negligence is not established, losses arising from cyber frauds and unauthorised electronic transactions are generally required to be borne by the banking system rather than the customer.**
- **Failure to promptly investigate complaints or reverse transactions may amount to deficiency in service.**

Conclusion

Viewed in the backdrop of recent judicial pronouncements, the 2026 RBI Directions do not represent a departure from the existing legal framework but rather strengthen principles that have increasingly been recognised by courts and consumer fora in disputes involving electronic banking frauds. The emerging judicial trend places greater emphasis on the bank's duty to maintain secure systems, promptly investigate complaints and establish customer negligence before denying relief.

The revised framework accordingly shifts the focus from merely limiting customer liability to creating a comprehensive customer protection regime encompassing prevention, reporting, investigation, reversal of transactions and compensation. While customers continue to bear responsibility for safeguarding credentials and promptly reporting frauds, banks are now subject to clearer obligations and higher standards of accountability.

We trust you will find this an interesting read. For any queries or comments on this update, please feel free to contact us at insights@elp-in.com or write to our authors:

Mukesh Chand, Senior Counsel – Email – *mukeshchand@elp-in.com*