भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA

DOR.MCS.REC.No. /01-01-034/2025-26 March xx, 2026

Draft Reserve Bank of India (Payments Banks - Responsible Business Conduct) Second Amendment Directions, 2026

Instructions on 'Limiting Liability of Customers in Unauthorised Electronic Banking Transactions' for Payments Banks (hereinafter referred to collectively as "PBs" and individually as an "PB") have been consolidated in the Reserve Bank of India (Payments Banks - Responsible Business Conduct) Directions, 2025. Upon a review, it has been decided to issue revised instructions on the subject.

2. In exercise of the powers conferred by Section 35A of the Banking Regulation Act,1949, the Reserve Bank, being satisfied that it is necessary and expedient in public interest so to do, hereby issues the Amendment Directions hereinafter specified.

3. Short Title and Commencement

(1) These Directions shall be called the Reserve Bank of India (Payments Banks - Responsible Business Conduct) Second Amendment Directions, 2026.

(2) These Directions shall apply in cases of electronic banking transactions undertaken by customers of a bank on or after **July 1, 2026**.

4. These Amendment Directions shall modify the Reserve Bank of India (Payments Banks - Responsible Business Conduct) Directions, 2025 as under:

(1) In paragraph 4, the following definition shall be inserted after sub-paragraph 4(2), namely:

"***4(2A) Authorised electronic banking transaction*** *includes:*

(i) a transaction carried out by a customer or a previously authorised third-party registered with the PB by granting approval through a standing instruction / mandate or any form of additional authentication such as a static password or dynamic password (e.g. OTP), answering challenge questions, card details (CVV / Expiry date / PIN) or any other mode of electronic authentication option provided by the PB; or

(ii) a transaction which is

(a) executed by a third-party using the credentials obtained from the customer through fraudulent means; or

(b) executed by the customer by granting approval under coercion or duress from the third-party; or

(c) executed by the customer when he / she is tricked into willingly sending money to a scammer who is posing as a legitimate recipient.".

(2) In paragraph 4, the following definitions shall be inserted after sub-paragraph 4(4), namely:

*"**4(4A) Card Not Present transaction** shall have the same meaning as given in the Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025.*

***4(4B) Card Present transaction** shall have the same meaning as given in the Reserve Bank of India (Authentication Mechanisms for Digital Payment Transactions) Directions, 2025."*

(3) In paragraph 4, the following definition shall be inserted after sub-paragraph 4(7C), namely:

*"**4(7D) Electronic banking transaction** shall have the same meaning as 'electronic funds transfer' given in Section 2(c) of the Payment and Settlement Systems Act, 2007 and inter alia include both Card Not Present and Card Present transactions."*.

(4) In paragraph 4, the following definition shall be inserted after sub-paragraph 4(9), namely:

*"**4(9A) Fraudulent electronic banking transaction** means an authorised electronic banking transaction falling under categories listed at paragraph 4(2A) (ii) above and an unauthorised electronic banking transaction as defined at paragraph 4(13B) below."*.

(5) In paragraph 4, the following definitions shall be inserted after sub-paragraph 4(10), namely:

*"**4(10A) Negligence by a PB** inter alia includes the following actions by the PB:*

(i) not putting in place the mandated systems and procedures to ensure safety and security of electronic banking transactions; or

(ii) not sending mandatory alerts for electronic banking transactions; or

(iii) not providing the mandated channels for reporting of fraudulent electronic banking transactions or loss of payment instruments such as card; or

(iv) not acting diligently upon a customer notification regarding unauthorised electronic banking transaction(s) or loss of payment instrument(s); or

(v) system malfunctions / security breaches / internal frauds leading to unauthorised electronic banking transactions.

***4(10B) Negligence by a customer** inter alia includes the following actions by the customer:*

(i) providing credentials such as PIN, password, OTP or other details for carrying out transactions to another person, whether intentionally or otherwise; or

(ii) not notifying the PB immediately after finding out about a fraudulent electronic banking transaction or loss of a payment instrument; or

(iii) not paying attention to specific, directed and clear warnings from the PB that a prospective transaction is likely a scam; or

(iv) failing to exercise reasonable care in usage of credentials, e.g., writing down and storing the PIN with an ATM card; or

(v) downloading malicious apps.".

(6) In paragraph 4, the following definitions shall be inserted after sub-paragraph 4(13), namely:

***"4(13A) Third-party breach** refers to a situation where the deficiency lies neither with the PB nor with the customer but lies elsewhere in the system and includes deficiency on the part of an intermediary such as a Third-Party Application Provider (TPAP), Payment Aggregator (PA), Payment Gateway (PG), Telecom Service Provider (TSP), etc.*

***4(13B) Unauthorised electronic banking transaction** means an electronic banking transaction which does not qualify as an authorised electronic banking transaction."*.

(7) In Chapter III on 'Customer Guidance and Protection', the section **C. Limiting Liability of Customers in Unauthorised Electronic Banking Transactions** and paragraphs 21 to 33 thereunder shall be deleted and substituted with the following section and paragraphs, namely:

"CA. Customer Protection in Electronic Banking Transactions

CA.1 Policy

33A. *A PB, keeping in view the instructions contained in these Directions, shall formulate a policy to cover aspects of customer protection in electronic banking transactions, such as:*

(1) channels for alerting customers about occurrence of electronic banking transactions;

(2) define the rights and obligations of customers in case of electronic banking transactions, including fraudulent electronic banking transactions, after taking into account the risks to customers arising out of customer negligence / PB negligence / banking system frauds / third-party breaches in specified scenarios;

(3) timeline for resolution of complaints and disclosure to customer; and

(4) mechanism for creating customer awareness on their rights and obligations involved in electronic banking transactions along with the risks involved.

The policy must be transparent, non-discriminatory and shall be displayed on the PB's website along with the details of grievance handling / escalation procedure.

33B. *A PB shall design its systems and procedures to make customers feel safe about carrying out electronic banking transactions. To achieve this, the PB shall put in place:*

(1) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers, including those mandated under the Master Direction on Digital Payment Security Controls, as amended from time to time;

(2) robust and dynamic fraud detection and prevention mechanism;

(3) mechanism to assess the risks (for example, gaps in the PB's existing systems) arising from fraudulent electronic banking transactions and measure the liabilities arising out of such events;

(4) appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom; and

(5) a system of continually and repeatedly making the customers aware about evolving electronic banking and payments related frauds and the ways to protect themselves from such frauds.

CA.2 Alerts for electronic banking transactions

***33C.** A PB shall ask its customer, availing the facility of electronic banking transactions (other than ATM cash withdrawals), to mandatorily provide his / her mobile number and wherever available, email address, to the PB.*

***33D.** A PB shall mandatorily send instant SMS alerts to the customers for all electronic banking transactions of value more than ₹500. For electronic banking transactions of value up to ₹500, a PB may decide to send instant SMS as per its internal policy.*

***33E.** A PB shall send email alerts for all electronic banking transactions, wherever email address is provided by the customer.*

***33F**. SMS and/ email alerts as above shall be in addition to any other form of alerts, e.g. in-app / push notifications, etc., which the PB may send as per its internal policy.*

CA.3 Reporting of fraudulent electronic banking transactions by customers to PBs

***33G.** A PB shall advise its customers that on occurrence of any fraudulent electronic banking transaction at the earliest after the occurrence of such transaction, they should notify the bank and also lodge a complaint through National Cyber Crime Reporting Portal or National Cyber Crime Helpline (1930) at the earliest. The PB shall also inform its customers that the longer the time taken to notify the PB, the higher will be the risk of loss to customer and also to the PB. To facilitate the same, the PB shall:*

(1) provide customers with 24x7 access through multiple channels including via phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc., for reporting fraudulent electronic banking transactions that have taken place and / or loss or theft of payment instrument such as card, etc.;

(2) provide a number in the transaction alert SMS itself, to which the customer can immediately send an SMS to notify his / her objection, if any; and

(3) provide a direct link on the home page of its website for reporting fraudulent electronic banking transactions.

33H. *The PB's communication systems, deployed for sending alerts and receiving the responses thereto, shall record the date and time of delivery of the message and receipt of customer's response, if any.*

33I. *A PB shall ensure that its system registers the reporting of the fraudulent electronic banking transaction as a complaint and sends an immediate acknowledgement to the customer along with the complaint number and the date and time of receipt of the complaint.*

33J. *On receipt of a complaint regarding any fraudulent electronic banking transaction from a customer, a PB shall take immediate steps to prevent further unauthorised electronic banking transactions in his / her account under advice to the customer.*

CA.4 Processing of Complaints and Establishing Liability in Fraudulent Electronic Banking Transactions

33K. *The burden of proving customer liability in complaints involving fraudulent electronic banking transactions shall lie on the PB. Accordingly, it shall examine and classify each complaint under the relevant categories of electronic banking transactions as defined in these directions.*

33L. *A customer shall be entitled to zero liability and reversal of the transaction in cases where the fraudulent electronic banking transaction occurs due to negligence / deficiency on the part of the PB (irrespective of whether the transaction is reported by the customer or not) and in cases of third-party breach where the customer reports the unauthorised fraudulent electronic banking transaction to the bank within five calendar days from the date of its occurrence.*

33M. *In cases of third-party breach reported to the bank after five calendar days, the customer shall be compensated, in eligible cases, for his / her loss as per the provisions detailed at paragraph 33T below. In cases of third-party*

breach not eligible for compensation as per these provisions, the customer's liability shall be determined as per the bank's policy.

***33N**. In cases where the fraudulent electronic banking transaction occurs due to negligence by the customer, he / she shall be liable for the loss incurred by him / her, to the extent of loss not eligible for compensation as per the mechanism detailed at paragraph 33T below, until he/ she reports the fraudulent electronic banking transaction to the PB.*

***33O**. Loss arising from any unauthorised transaction occurring after the reporting of the fraudulent electronic banking transaction by a customer to a PB shall be borne by the PB.*

***33P.** The PB may also, at its discretion, decide to waive off any customer liability in case of fraudulent electronic banking transactions.*

***33Q.** A PB shall ensure that complaints involving fraudulent electronic banking transactions are examined, liability therein is established and response, as applicable, is issued to the customer within such time as may be specified in the PB's policy, but not exceeding 30 calendar days from the date of receipt of the complaint. In cases where the customer is entitled to zero liability as provided at paragraph 33L above, the response shall also include details of reversal of the transaction(s) concerned. In cases falling under either paragraph 33M or 33N above, the response shall include details regarding the compensation mechanism prescribed at paragraph 33T below.*

***33R.** In cases where the PB is required to reverse a fraudulent electronic banking transaction, it shall ensure that the reversal is value dated to its original date of occurrence and the customer does not suffer loss of interest or bear any additional burden of interest/ charges, as applicable.*

***33S**. In case of rejected complaints i.e., in cases where customer liability is established, a PB shall disclose the reason for such rejection (along with supporting details such as OTP logs, SMS logs, transaction logs, etc.) to the customer.*

CA.5 Compensation for Small Value Fraudulent Electronic Banking Transactions

33T. *(1) A bona fide victim, being an individual person and having lodged a complaint involving gross loss of an amount up to ₹50,000 on account of fraudulent electronic banking transaction(s) covered under paragraphs 76M and 76N above, shall be compensated 85 per cent of the net loss amount (calculated after reducing recoveries made, whether before or after paying the compensation, from the gross loss amount), or ₹25,000, whichever is less, once during his / her lifetime, subject to the following:*

(a) loss is established to be bona fide, as per the internal processes covered in the SFB's policy, and

(b) the victim has reported the fraudulent electronic banking transaction(s) on the National Cyber Crime Reporting Portal or National Cyber Crime Helpline (1930) and to the bank within five calendar days from its occurrence.

Explanation: In case of joint account(s), only one of the account holders may submit a claim for compensation. The customer availing compensation as a joint account holder shall not be eligible for claiming compensation in his / her capacity as a single account holder in future and vice versa.

(2) (a) For a complaint related to fraudulent electronic banking transaction(s) involving a loss amount of less than ₹29,412, where a compensation of 85 per cent is paid, 65 per cent shall be borne by the Reserve Bank, 10 per cent by the customer's bank and the remaining 10 per cent by the beneficiary bank.

(b) For a complaint related to fraudulent electronic banking transaction(s) involving a loss amount of ₹29,412 or more but up to ₹50,000, where a compensation of ₹25,000 is paid, the Reserve Bank, the customer's bank and the beneficiary bank shall contribute ₹19,118, ₹2,941 and ₹2,941 respectively towards the compensation.

(3) In case any recovery is made in relation with a complaint involving fraudulent electronic banking transaction(s) after the compensation is paid, the customer's bank shall recalculate the compensation payable on the net loss amount and accordingly make additional payment from the recovered amount after factoring in the excess amount of compensation, if any, paid before the recovery.

Illustration 1: *Amount reported lost under the complaint – ₹40,000*

Recovery made & credited to customer before compensating – ₹15,000

Net loss faced by the customer - ₹25,000

Compensation to be paid to the customer (85% of net loss) – ₹21,250

Contribution of Reserve Bank - ₹16,250

Contribution of customer's bank and beneficiary bank - ₹2,500 each

Illustration 2: *Amount reported lost under the complaint – ₹40,000*

Compensation paid to the customer – ₹25,000

Contribution of Reserve Bank - ₹19,118

Contribution of customer's bank and beneficiary bank - ₹2,941 each

Recovery made - ₹40,000

Apportionment of recovery shall be as under:

To customer – ₹15,000

To Reserve Bank - ₹19,118

To customer's bank and beneficiary bank – ₹2,941 each

Illustration 3: *Amount reported lost under the complaint – ₹40,000*

Compensation paid to the customer – ₹25,000

Contribution of Reserve Bank - ₹19,118

Contribution of customer's bank and beneficiary bank - ₹2,941 each

Recovery made after compensation is paid - ₹15,000

Net loss - ₹25,000

Compensation payable – ₹21,250

Additional amount payable - ₹15,000 + ₹21,250 - ₹25,000 = ₹ 11,250

Apportionment of recovery shall be as under:

To customer – ₹ 11,250

To Reserve Bank - ₹19,118 – 16,250 = ₹2,868

To customer's bank and beneficiary bank – ₹2941 - ₹2,500 = ₹441 each

(4) Based on its examination, where the bank is satisfied that the complaint is bona fide, it shall provide the customer an application form as per the format provided at ***Annex I(1)*** *to claim compensation for the loss suffered by him / her.*

(5) The PB shall, within five calendar days of receipt of the application from a customer, compensate the customer as given above.

(6) The PB shall seek reimbursement of the applicable amount from the Reserve Bank on a quarterly basis.

***33U**. The compensation shall be payable for losses incurred on fraudulent electronic banking transactions occurring up to one year from the effective date of these directions.*

CA.6 Monitoring Mechanism

***33V.** A PB shall put in place a suitable mechanism and structure for periodic reporting of complaints involving fraudulent electronic banking transactions to the Board or one of its Committees. The reporting shall, inter alia, include volume / number of cases and the aggregate value involved and distribution across various categories of cases, viz., card present transactions, card not present transactions, internet banking, mobile banking, ATM transactions, etc. The Board or its Committee shall periodically review the fraudulent electronic banking transactions reported by customers, the action taken thereon, functioning of the grievance redressal and compensation mechanism, etc., and take appropriate measures to improve the systems and procedures.".*

(8) In Chapter III on 'Customer Guidance and Protection', paragraph 42 shall be substituted by the following, namely:

"A PB shall not levy any charges on its customers for SMS sent in compliance to extant regulations or those sent for promotional / marketing / customer awareness purposes. In case of SMS sent for other purposes, the PB may levy or waive charges as per its internal policy.".

(9) In Annexures, the following Annexure shall be inserted after Annex II, namely:

"Annex II(1) - Application Form for Compensation for Small Value Fraudulent Electronic Banking Transactions

The Branch Manager, *Date:* _____

_____ *Bank*

_____*Branch*

Madam/ Dear Sir,

Application for Compensation for Small Value Fraudulent Electronic Banking Transactions

Please refer to my complaint lodged with National Cyber Crime Reporting Portal (https://cybercrime.gov.in/Default.aspx) / National Cyber Crime Helpline (1930) with reference / complaint no. _____ regarding the fraudulent electronic banking transaction(s) in my bank account / credit card no. _____.

***2.** I understand that compensation for small value fraudulent electronic banking transactions is available to an individual only once and declare that I have not previously availed such a compensation from any bank.*

***3.** As per the advice dated _____ received from the bank, an amount of ₹_____ (Rupees _____ only) may please be credited to my aforesaid bank account / credit card.*

Signature of the applicant:

Name of applicant: _____

Aadhaar No. (mandatory): _____

Address: _____

_____

_____

_____

Contact No.: _____

Email Address: _____

FOR OFFICE USE

(may be modified by the PB as per its own requirement)

”.

(Veena Srivastava)
Chief General Manager