भारतीय रिज़र्व बैंक

RESERVE BANK OF INDIA

DoR.MCS.REC.No. /01-01-032/2026-27 XXXX XX, 2026

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

The Reserve Bank had issued the Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026 dated June 24, 2026 on **'Customer Protection in Fraudulent Electronic Banking Transactions'**, which, *inter alia*, strengthened the existing framework for limiting liability of customers in unauthorised Electronic Banking Transactions (EBTs). While the revised framework primarily addresses customer liability in the event of fraudulent EBTs, a need is felt to further strengthen the same from a preventive perspective by providing customers with greater control over the manner and extent to which digital payment channels are used. Accordingly, based on the public feedback received on the Discussion Paper 'Exploring safeguards in digital payments to curb frauds' dated April 09, 2026, it has been decided to issue directions on customer-induced controls and an additional layer of authentication through a Trusted Person Mechanism (TPM). Further, on a review to bring uniformity in practices adopted by banks and ensure that customers are protected against specific acts of omission or commission on part of the banks, it has been decided to expand the scope of the definition of 'negligence by a bank' specified in the aforementioned Amendment Directions.

Accordingly, these directions are issued to all Commercial Banks (other than Small Finance Banks, Payments Banks, Regional Rural Banks, and Local Area Banks) (hereinafter referred to collectively as "banks" and individually as a "bank") under the Reserve Bank's Responsible Business Conduct Directions, 2025.

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 (Commercial Banks - Responsible Business Conduct) Fifth Amendment Directions, 2026.

(2) These Directions shall come into effect from July 1, 2027, or on such earlier date as a bank may decide to implement, except the provisions contained in clauses (i) to (vi), (ix) and (x) of sub-paragraph 4(20B) specified below which shall come into effect from January 1, 2027.

4. These Amendment Directions shall substitute the definition of 'negligence by a bank' prescribed in the Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Third Amendment Directions, 2026 as under:

> ***"4(20B) Negligence by a bank*** *means any act of omission or commission on part of the bank which results in or contributes to the occurrence of a fraudulent electronic banking transaction in a customer account, including the following:*
>
> > *(i) not implementing instructions related to factors of authentication for EBTs, as prescribed under Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions, 2025;*
> >
> > *(ii) not implementing multi factor authentication for creation of new account linkages (addition / modification / deletion of beneficiaries), change in account details or revision to fund transfer limits, as prescribed under paragraph 46 of Reserve Bank of India (Commercial Banks – Digital Payment Security Controls) Directions, 2026;*
> >
> > *(iii) not sending mandatory alert for an EBT, as prescribed under paragraph 76D of these Directions;*
> >
> > *(iv) not providing 24x7 channels for reporting of fraudulent EBTs or loss of debit / credit card, as prescribed under paragraph 76G of these Directions;*
> >
> > *(v) not acting promptly upon a customer notification regarding fraudulent EBT(s) or loss of debit / credit card, as prescribed under paragraph 76J of these Directions;*

(vi) not blocking the digital payment channel and / or notifying the customer consequent to the maximum number of failed login or authentication attempts, where such failure contributed to the fraudulent EBT, as prescribed under paragraphs 50 and 51 of Reserve Bank of India (Commercial Banks – Digital Payment Security Controls) Directions, 2026);

(vii) not providing the facility of mandatory customer-induced controls or not implementing the controls for EBTs as set by the customer, as prescribed under these Directions;

(viii) not providing Trusted Person Mechanism or failing to implement the directions with respect to the mechanism, as prescribed under these Directions;

(ix) a system malfunction or security breach at the bank's end, which facilitates or results in a fraudulent EBT; and

(x) collusion or connivance of an employee of the bank or any third party engaged by the bank, which facilitates or results in a fraudulent EBT."

5. These Amendment Directions shall modify the provisions of the Reserve Bank of India (Commercial Banks - Responsible Business Conduct) Directions, 2025 (hereinafter referred to as the Directions) as under:

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

*"**4(9A) Customer-induced Control** means a customer-configurable restriction, limit, lock, safeguard or permission applicable to the customer's account."*

(2) In paragraph 4 of the Directions, the following definition shall be inserted after sub-paragraph 4(10.1A), namely:

***"4(10.1B) Digital Payment Channel** means any electronic interface, device, network or set of procedures provided by a bank, through which a customer can undertake a digital payment transaction / electronic banking transaction."*

(3) In paragraph 4 of the Directions, the following definition shall be inserted after sub-paragraph 4(19), namely:

*"**4(19A) Merchant** shall have the same meaning as defined in the Master Direction on Regulation of Payment Aggregator (PA)."*

(4) In paragraph 4 of the Directions, the following definition shall be inserted after sub-paragraph 4(24), namely:

*"**4(24.1A) Prepaid Payment Instrument (PPI)** shall have the same meaning as defined in the Master Directions on Prepaid Payment Instruments (PPIs)."*

(5) In paragraph 4, the following definition shall be inserted after sub-paragraph 4(25A), namely:

*"**4(25B) Stop Switch** means a facility through which a customer can disable all customer initiated future debits associated with her / his account(s) as per these Directions."*

(6) In paragraph 4 of the Directions, the following definition shall be inserted after sub-paragraph 4(26A), namely:

*"**4(26AA) Trusted Person** means a natural person aged 18 years or above, registered by a bank's customer, to act as an additional factor of authentication as per these Directions."*

(7) In Chapter IV on 'Customer Guidance and Protection' of the Directions, in the section 'DA. Customer Protection in Fraudulent Electronic Banking Transactions', the following sub-sections and paragraphs shall be inserted after the sub-section 'DA.2 Alerts for EBTs', namely:

*"**DA.2A. Preventive Safeguards for EBTs***

DA.2A.1 Customer-induced controls for EBTs

DA.2A.1.1 Customer-induced controls for digital payment channels other than cards

***76FA.** A bank shall provide all its customers with the facility to disable one or more digital payment channels linked to their account, and to subsequently re-enable such channel through the physical or digital interfaces of the bank, in accordance with the procedure specified in paragraphs 76FI and 76FJ hereunder.*

76FB. *Where a digital payment channel has been disabled by the customer, no customer-initiated debit transaction shall be permitted through that channel until it is re-enabled.*

76FC. *In addition, a bank shall provide the following controls to its customers, which may be exercised by them at their option:*

(1) to set or modify a maximum amount limit per transaction, per beneficiary or for the transactions in aggregate in a day that may be undertaken through a digital payment channel, within the overall limits otherwise applicable to that channel;

Illustration 1: *Beneficiary level limit – A customer sets a maximum limit of ₹20,000 per day for payments to a particular beneficiary. Even if the limit for the digital payment channel set by the payment system operator / the bank permits a higher amount, transactions to that particular beneficiary cannot exceed ₹20,000 per day.*

Illustration 2: *Transaction amount limit – A customer sets a maximum limit of ₹10,000 per transaction for a particular digital payment channel. Any transaction above ₹10,000 through that digital payment channel would not be permitted.*

Illustration 3: *Daily limit – A customer sets an overall daily limit of ₹50,000 for transactions done through a particular digital payment channel, even though the payment systems operator or the bank permits a higher limit. Any transaction above the daily limit would not be permitted through that digital payment channel.*

(2) to set or modify, a maximum limit for the transactions that may be undertaken in a day, through all the available digital payment channels taken together;

(3) to set a time window during which one or more digital payment channels linked to the customer's account shall remain disabled; and

(4) any other control introduced by the bank over and above the controls prescribed at 76FC (1) to 76FC (3) above, which may further strengthen customer options to safeguard their EBTs.

DA.2A.1.2 Customer-induced controls for cards (Debit, Credit, and Prepaid Payment Instruments (PPI) Card))

76FD. *A bank shall provide to all its cardholders the facility to switch on / off and set / modify transaction limits (within the overall card limit, if any, set by the issuer) for all types of transactions – domestic or international; at Point of Sale (PoS) / ATMs / online transactions / contactless transactions, etc.*

76FE. *The card-specific directions are not applicable to Gift PPI cards and Transit PPI Cards.*

DA.2A.1.3 Stop Switch facility in customer accounts

76FF. *A bank shall provide its customers with a Stop Switch facility for immediate disablement of all outward future debits associated with her / his account(s). However, any debits due to ongoing recurring payment mandates and standing instructions, and marking of lien or debits initiated by the bank to recover due charges, loan instalment, etc., shall be excluded from the scope of Stop Switch.*

76FG. *Upon activation of the Stop Switch, no customer-initiated debit transaction, creation of new payment mandates, setting up of new standing instructions or registration of UPI on new third-party payment applications shall be permitted in the account.*

76FH. *The activation of a customer-induced control or Stop Switch shall however not affect any inward credits into the customer's account.*

DA.2A.1.4 Re-enablement of digital payment channels or Deactivation of Stop Switch

76FI. *A bank shall provide customers the facility to re-enable digital payment channels or deactivate the Stop Switch to re-enable operations in the customer's account, subject to customer authentication. A bank shall ensure that any request for re-enablement is subject to, at the minimum, the authentication requirements prescribed under the Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions dated September 25, 2025, as amended from time to time. The authentication for such requests shall be at least as stringent as those applied while enabling the corresponding digital payment channel and may be enhanced based on the bank's risk assessment laid down in its policy.*

76FJ. *Based on its risk assessment, a bank shall impose a reasonable cooling period or other risk mitigation measures, before giving effect to such re-enablement requests.*

DA.2A.1.5 Default controls and other aspects

76FK. *A bank shall keep all digital payment channels disabled by default at the time of customer onboarding. Such channels shall be enabled only upon an explicit consent from the customer and after complying with the applicable authentication requirements.*

76FL. *Notwithstanding the above,*

(1) in case of cards -

- *(i) at the time of their issue, all cards (physical and virtual) shall be enabled for use only at contact-based points of usage (viz. ATMs and Point of Sale (PoS) devices) within India.*
- *(ii) at the time of their re-issue, the existing card controls shall be mapped to re-issued cards.*
- *(iii) forex prepaid cards shall be enabled for both contact, and contactless points of usage outside India at the time of their issue / re-issue.*

(2) in case of other digital payment channels, where a bank has enabled a particular channel for a customer at the time of customer onboarding or subsequently, it shall specify a ceiling on the aggregate value of fund transfers that the customer can undertake across the channel over the initial period of 24 hours, based on the bank's risk assessment. After the initial period of 24 hours, the bank may provide for gradual enhancements to the ceiling, based on its channel risk assessment and internal policy. The bank shall allow modification of the initial or enhanced ceiling (if implemented) through the exercise of customer controls provided at paragraph 76FC above and subject to compliance with the applicable authentication requirements. However, such modification shall be allowed only after the initial period of 24 hours has lapsed post activation of the digital payment channel.

76FM. *The facilities for activation, modification and deactivation of customer-induced controls and Stop Switch shall be made available to all customers through the available points of customer interface such as branches, ATMs, internet banking, mobile banking, Interactive Voice Response (IVR), etc.*

76FN. *Upon any activation, modification, deactivation or re-activation of any of such facilities, a bank shall immediately notify the customers through the available channels of communication, including but not limited to SMS and e-mail.*

76FO. *A bank shall maintain tamper proof audit logs of controls and the Stop Switch initiated by customers to facilitate review and resolution of disputes.*

76FP. *A bank shall undertake outreach efforts on an ongoing basis to inform customers regarding availability of the customer-induced controls and Stop Switch facility and attendant aspects such as process to activate or deactivate the same, implications of the activation, etc.*

DA.2A.2 Authentication through Trusted Person Mechanism

DA.2A.2.1 Applicability

76FQ. *A bank shall put in place a mechanism, called the Trusted Person Mechanism (TPM), to enable customers to register a trusted person to act as an additional factor of transaction authentication. The TPM shall apply to electronic fund transfers initiated through the physical and digital channels available under such customer's account beyond the threshold set by the customer, except for transactions initiated for:*

(1) payments made through the UPI channel linked to the customer's account;

(2) merchant payments, irrespective of the payment channel or instrument used; and

(3) recurring payments through standing instructions, e-mandates or NACH mandates.

76FR. *A bank shall offer the TPM to all its customers, whose availment shall be entirely voluntary, based on explicit requests of the customer and the trusted person, and are subject to the thresholds put in place by the customer.*

76FS. *The TPM shall be available in bank accounts operated by individuals solely or in such joint accounts operated under any of the survivorship clauses.*

DA.2A.2.2 Registration and onboarding of trusted person

76FT. *A bank shall facilitate, through its physical and digital channels, the registration of a trusted person, activation of the TPM, and configuration of related transaction-level thresholds by customers.*

76FU. *For registering a trusted person, a bank shall:*

(1) obtain the trusted person's name, mobile number, email address and copy of at least one Officially Valid Document (OVD);

(2) verify the identity and eligibility of the trusted person on the basis of the OVD and such other information or documentation as may be reasonably required; and

(3) verify the mobile number and email address of the trusted person through an appropriate authentication mechanism.

76FV. *The mobile number registered for the trusted person shall be distinct from the mobile number linked to the customer's account.*

76FW. *A bank, while obtaining the consent for TPM registration, shall clearly inform the customer and the trusted person that registration under the mechanism:*

(1) does not confer upon the trusted person the status of a joint account holder, nominee, mandate holder or authorised signatory;

(2) does not grant the trusted person any right, title or beneficial interest in the account;

(3) does not authorise the trusted person to independently access or operate the account, initiate any transaction, or otherwise issue instructions in relation to the account;

(4) does not result in the trusted person incurring any financial liability when she / he approves or rejects a transaction; and

(5) requires the trusted person to authenticate or reject the transaction within the time window prescribed by the bank and in a manner compliant with paragraph 76FZ ibid.

76FX. *Subsequent to registration of the trusted person, a bank shall send an acknowledgement to the customer and the trusted person through the available channels of communication, informing them of the successful registration.*

76FY. *A bank shall observe a 24 hour cooling period before the TPM is activated for a customer. Upon activation of the TPM, the bank shall promptly notify the customer and the trusted person through the available channels of communication.*

DA.2A.2.3 Authentication process for transactions under TPM

76FZ. *Any transaction beyond the threshold indicated by the customer will be notified to the trusted person for authentication through the available channels of communication. The notification shall include the amount of transaction, beneficiary details [viz., name, account number, mobile number, etc.,] to which the amount is being transferred and narration (if any) entered by the customer while initiating the transaction. A trusted person shall have a one-hour window from being notified, to give consent to the transaction through the trusted mode as prescribed by the bank for TPM. The transaction shall be executed only upon the trusted person's consent to the transaction, subject to the bank's fraud risk controls and other applicable requirements. In case there is a negative response or there is no response from the trusted person within the prescribed time window as above, the transaction shall be rejected.*

76FZA. *The consent of the trusted person to authenticate a transaction may be taken either through physical / digital signature or any other form of authentication given in Reserve Bank of India (Authentication mechanisms for digital payment transactions) Directions dated September 25, 2025, as amended from time to time. The bank shall also maintain appropriate logs / records of the same.*

76FZB. *A bank shall ensure that the trusted person is not privy to aspects pertaining to the customer's banking relationship (including but not limited to account balance, fixed deposits, investments, or insurance details) at any stage, including during transaction validation. The role of the trusted person shall be strictly limited to the transaction authentication.*

DA.2A.2.4 Customer controls

76FZC. *A bank shall provide customers with controls to change an existing trusted person, modify the threshold amount or payment channels chosen for the TPM, or opting out of the TPM itself. Exercise of such controls shall be subject to a cooling period of 24 hours and shall be authenticated by the customer. Further, if a customer is assessed to be more vulnerable to falling prey to cyber-enabled financial crimes / frauds, the bank shall resort to additional checks, e.g. requiring a mandatory branch visit or a tele-verification call, etc.*

76FZD. *In case of change or removal of a trusted person, a bank shall notify both the customer and the outgoing trusted person through the available communication channels of the change before it takes effect.*

DA.2A.2.5 Implementation and customer awareness

76FZE. *A bank shall give wide publicity to the availability of the TPM and provide guidance to customers regarding its applicability and features. Such communications shall be disseminated in English, Hindi and local language of the region through all available channels of customer outreach available to the bank, such as branches, SMS, email, etc. The bank shall ensure that the communication explicitly delineates the role of the trusted person, benefits and limitations of the TPM, etc."*

(R Sathish)
Chief General Manager