Policy on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions
Version 1

1. Introduction

the growing adoption of digital banking channels, ensuring customer trust and confidence ins at the core of the Bank's customer service philosophy. The Bank is committed to provide re, reliable, and seamless digital banking experiences while protecting customers against potential arising from unauthorised electronic transactions. This Policy has been formulated in line with guidelines DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017, and reflects the Bank's mitment to safeguard customer interests by clearly defining their rights and obligations, limiting omer liability in various scenarios, and strengthening the Bank's systems to prevent fraudulent actions.

Policy is in line with relevant Regulatory / statutory instructions and the Master Directions of rve Bank of India and in case of any discrepancy between the policy and any statutory regulations, atter would prevail. Similarly, in case of any change in the statutory regulations not being in ormity with the policy, the statutory regulations would prevail.

2. Scope

This Policy applies to all customers of the Bank who avail themselves of electronic banking services across various channels, including internet banking, mobile banking, UPI, card transactions, and other digital payment instruments offered by the Bank. It defines the framework for determining customer liability in the event of unauthorised electronic banking transactions. It outlines the Bank's responsibilities to protect customers, address grievances, and ensure fair treatment to all products, services, and digital platforms where electronic transactions are facilitated. This policy shall be read in conjunction with related policies to provide comprehensive customer protection.

This Policy covers all electronic banking transactions, classified as:

1. Remote/Online Payment Transactions: Internet banking, mobile banking, UPI, card-not-present transactions, and Prepaid Payment Instruments (PPIs).

2. Face-to-Face/Proximity Payment Transactions: ATM, POS, or any transaction that requires the physical presence of a card or device.
3. Any other electronic mode of transactions effected from one entity to another currently being used or adopted from time to time.

This policy covers transactions only through the above modes. It excludes electronic banking transactions effected on account of error by a customer (e.g. NEFT carried out to an incorrect payee or for an incorrect amount), transactions done under duress, claims due to opportunity loss, reputation loss, other incidental cost or collateral damage.

3. Objectives

The Policy aims to:

- Protect customers against losses arising from unauthorised electronic banking transactions.
- Define customer liability in various scenarios.
- Strengthen the Bank's fraud detection and prevention systems.
- Educate customers on safe banking practices.

4. Applicability

A. This policy is applicable to entities that hold relationship with the bank viz.:

- Individual and non-individual customers who hold current or savings account or credit facilities.
- Individual / non-individual entities that hold credit card and/or prepaid card.
- Individual / non-individual entities that use other electronic platforms of the Bank like internet banking, mobile banking and e-wallet.

B. This policy is not applicable to:

- Non-Customer that use Bank's infrastructure e.g. ATMs, electronic e-wallet
- Entities that are part of the ecosystem such as Interchange Organizations, Franchises, Intermediaries, Agencies, Service Partners, Vendors, Merchants etc

5. Definitions & Explanations: (for the purpose of this policy)

- Real loss is defined as financial outgo from customer's account e.g. debit to customer's account or card.
- Card not present (CNP) transactions are defined as transactions that require use of Card information without card being physically used e.g. e-commerce transactions.
- Card present (CP) transactions are defined as transactions that require use of physical card e.g. at ATM or shops (POS)
- Payment transactions are defined as transactions that involve transfer of funds from one account/ e-wallet to another electronically and do not require card information e.g. NEFT.
- Unauthorized transaction is defined as debit to customer's account without customer's consent
- Consent includes authorization of a transaction debit either through standing instructions, as per accepted banking practice and regulation, based on account opening process and related matters or based on additional authentication required by the bank such as use of security passwords, input of dynamic password (OTP) or static VBV/ MCSC, challenge questions or use of Card details (CVV/ Expiry date) or any other electronic authentication option provided by the Bank.
- Date & time of reporting is defined as date & time on which customer has submitted a unique complaint. Date of receiving communication from the Bank, is excluded for purpose of computing number of working days for all action specified in this policy. The working schedule of the home branch would be considered for calculating working days for customer reporting. Time of reporting will be as per Indian Standard Time.
- Notification means an act of the customer reporting unauthorized electronic banking transaction to the bank
- Number of days will be computed based on working days of the parent branch.
- Mode of reporting will be the channel through which customer complaint is received first time by the Bank, independent of multiple reporting of the same unauthorized

transaction.

- Loss in foreign currency, if any, shall be converted to Indian currency for the purpose of this policy as per bank's policies on conversion at card rate net of commission.

6. Customer Liability

(a) Zero liability of a customer

A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the event of -

(i) Contributory fraud / negligence /deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer)

(ii) Third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, and the customer notifies the bank within three working days of receiving the communication from the Bank regarding the unauthorized transaction.

(b) Limited Liability of a customer

A customer shall be liable for the loss occurring due to unauthorised transactions in the following case:

(i) In cases where loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorised transactions to the Bank. Any loss occurring after the reporting of the unauthorised transactions shall be borne by the Bank.

(ii) In cases where the responsibility for the unauthorized electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system and when there is a delay (of four to seven working days after receiving the communication from the Bank) on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in table below, whichever is lower:

Types of Account	Maximum Liability (Rs.)
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current / Cash Credit / Overdraft Accounts of MSMEs • Current Account Cash Credit Overdraft Accounts of individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit up to Rs.25 lacs. • Credit card with limit above Rs.5 lacs.	10,000
• All other Current / Cash Credit / Overdraft Accounts • Credit Cards with limit above Rs.5 lacs	25,000

If the delay in reporting is beyond seven working days, the customer liability shall be treated as 100%.

Summary of Customer's Liability

Time taken to report the fraudulent transactions from the date of receiving the communication	**Customer's Liability (in Rs.)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned Table above, whichever is lower
Beyond 7 working days	Will be treated as 100% Customer liability

The number of working days mentioned in the table above shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

c. Other Points

- Customer shall bear the entire loss in cases where the loss is due to negligence by the customer, e.g. where the customer has shared payment credentials or Account/Transaction details, viz. Internet Banking user Id & PIN, Debit/Credit Card PIN/OTP or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing /Vishing attack. Under such situations, the customer will bear the entire loss until the customer reports unauthorized transaction to the bank. Any loss occurring after reporting of unauthorized transaction shall be borne by

the bank.

- In cases where the responsibility for unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere in the system and when there is a delay on the part of the customer in reporting to the Bank beyond 7 working days, the customer would be completely liable for all such transactions.
- In cases of zero / limited liability, the Bank shall credit (shadow reversal) the amount involved in the unauthorised electronic transaction to the customer's account within 10 working days from the date of such notification by the customer (without waiting for settlement of insurance claim, if any); the credit shall be value dated to be as of the date of unauthorized transaction. In cases where prima facia, customer negligence is evident or in cases of complete liability of customer, no shadow credit will be provided. If the investigation proves negligence in cases where shadow credit is already given, the amount will be reversed. Customer will be given 30 days' time from date of reporting to submit documents for consideration of the complaint.
- Within 90 days of date of receipt of complaint, the Bank shall either establish customer negligence or provide final credit to customer. Customer will be given value dated credit (based on date of unauthorized transaction) when customer becomes eligible to be compensated. In case of debit card/ bank account, the customer shall not suffer loss of interest and in case of credit card; customer shall not bear any additional burden of interest.
- Compensation would be limited to real loss after deduction of reversals or recoveries received by the customer.

7. Third Party Breach

The following would be considered as Third party breach where deficiency lies neither with the Bank nor customer but elsewhere in the system:

- Application frauds
- Account takeover
- Skimming / cloning
- External frauds / compromise of other systems, for e.g. ATMs / mail servers etc. being

compromised.

8 Reversal Timeline

- Upon customer notification, **credit (shadow reversal)** shall be provided within **10 working days**, value dated to the date of transaction.
- Final resolution, including establishing liability, shall be within **90 days**.
- If unresolved within 90 days, compensation as per the paragraphs above shall be paid to the customer.
- In debit card/bank accounts, the customer shall not suffer loss of interest; in credit cards, the customer does not bear any additional burden of interest.

9. Customer Obligations

- Customer shall mandatorily register valid mobile number with the Bank; if not provided, bank may not offer facility for electronic transactions.
- Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer's liability.
- Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide copy of the same to the Bank.
- Customer should co-operate with the Bank's investigating authorities and provide all assistance.
- Customer must not share sensitive information (such as Debit/Credit Card details & PIN, CVV, Net Banking Id & password, OTP, transaction PIN, challenge questions) with any entity, including bank staff.
- Customer shall go through various instructions and awareness communication sent by the bank on secured banking available at banks website.
- Customer must set transaction limits to ensure minimized exposure.

- Customer shall abide by the tips and safeguards on Secured Banking available at Bank's website.
- Customer must verify transaction details from time to time in his/her bank statement and/or credit card statement and raise query with the bank as soon as possible in case of any mismatch.

10. Notifying the Bank of the unauthorized transaction:

- Customer shall report unauthorized transaction to the Bank at the earliest, with basic details such as Account Number and/ or Card number (last 6 digits), date & time of transaction and amount of transaction
- Customer shall follow bank's reporting process including lodging police complaint and maintain copy of the same and furnish police complaint when sought by bank's authorized personnel.
- Customer shall authorize the bank to block the credit/ debit card/ net banking/ mobile banking / UPI / other channels of transaction in the account(s) to reduce likelihood of additional loss.
- Customer to clearly specify the facilities to be blocked failing which the Bank reserves the right to block all electronic transactions of the customer to protect his/her interest.
- Customer shall share relevant documents as needed for investigation or insurance claim viz. cardholder dispute form, copy of passport in case of international transactions and police complaint.
- Fully co-operate and comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.

11. Burden of Proof

The burden of proving customer liability in unauthorised transactions shall lie on the Bank. Any unauthorised electronic banking transaction which has been processed post second factor authentication known only to the customer, would be considered as sufficient proof of customer involvement/consent in effecting the transaction.

18.Force Majeure:

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank) prevents it from performing its obligations within the specified service delivery parameters.