**POLICY ON CUSTOMER PROTECTION - LIMITING LIABILITY**

**TABLE OF CONTENTS**

1. Introduction
2. Objective
3. Scope
4. Applicability
5. Definitions and Explanation
6. Points covered under Policy
7. Third Party Breach
8. Roles and Responsibilities of the Bank
9. Rights and Obligation of the Customer
10. Notifying the bank on unauthorized transactions
11. Proof of Customer Liability
12. Redressal of Complaints / Grievance
13. Force Majeure
14. Annexure

**1. Introduction:**

The Bank is committed to provide superior and safe customer service experience to all its customers. The Bank has over the years invested in technology and has robust security systems and fraud detection and prevention mechanisms in place.

**2. Objective:**

This policy aims at defining the rights and obligations of customers in dealing with digital channels offered by the Bank and also limiting customer liability in the event of unauthorized transactions. The intent of the policy is to build customer confidence in digital transactions and to ensure that the customer does not suffer loss due to unauthorized transactions arising out of incidents beyond their control. This Policy is prepared based on the Reserve Bank of India’s (RBI) Circular on ‘Customer Protection – Limiting Liability of Customers in Unauthorized Electronic Banking Transactions’ dated July 06, 2017 [DBR.No.Leg.BC.78/09.07.007/2016-17] and as amended from time to time. This policy will be reviewed periodically and updated as per regulatory guidelines/changes to processes/products.

**3. Scope:**

The policy defines the roles and responsibilities of the Bank and the customer with respect to transactions conducted through digital channels and also defines the framework for limiting customer liability in case of unauthorized transactions. This policy will also address the various electronic banking channels.

**4. Applicability:**

This policy is applicable for all the customers of the Bank maintaining various types of accounts viz. Savings Bank Accounts, Current Accounts, Overdraft Accounts, Cash Credit Accounts, etc., who are availing electronic banking services/channels. This Policy covers unauthorized transactions occurring in the following electronic banking channels:

* Internet Banking
* Mobile Banking
* Debit Cards (Online / PoS / ATM / International Transactions)
* UPI
* Prepaid cards
* IMPS
* NEFT
* RTGS
* BBPS
* Any other electronic banking transaction as may be applicable from time to time.

**5. Definitions and Explanation:**

a. **Customer:** The account holder(s) of The Bank, availing electronic banking services. b. **Electronic Banking Transaction:** A transaction effected by debiting or crediting a customer’s account, through electronic channels such as internet banking, mobile banking, ATM, PoS, UPI, card present/card not present, etc. c. **Unauthorized Electronic Banking Transaction:** An electronic banking transaction not initiated by the customer. d. **Contributory Fraud/Negligence/Collusion:** Unauthorized electronic banking transaction(s) which occur due to the act of omission or commission on the part of the customer. e. **Third Party Breach:** Unauthorized electronic banking transaction(s) where the fraud has occurred at the Bank’s/system’s end or where there is no contributory fraud/negligence/collusion on the part of the customer. f. **Zero Liability:** The customer’s liability will be zero when the unauthorized transaction occurs due to Third Party Breach, even if the customer delays in reporting the unauthorized transaction. g. **Limited Liability:** The customer will have limited liability in cases of unauthorized electronic banking transactions, where the customer’s contributory negligence is established due to his/her acts of omission or commission but the customer notifies the Bank of the unauthorized transaction within the stipulated time frame.

**6. Points covered under Policy:**

This policy covers the following points with respect to customer liability for unauthorized electronic banking transactions:

**A. Zero Liability of a customer:** A customer's liability in an unauthorized electronic banking transaction will be zero in the following events:

i. **Contributory Fraud/Negligence/Collusion:** Where the unauthorized transaction occurs due to contributory fraud, negligence, or collusion on the part of the Bank or the fraud is within the Bank’s systems, the customer will not be liable even if he/she does not report the unauthorized transaction. ii. **Third Party Breach:** Where the unauthorized transaction occurs due to a third-party breach where the deficiency lies neither with the Bank nor with the customer, and the customer reports the unauthorized transaction to the Bank within three working days of receiving the communication from the Bank regarding the unauthorized transaction.

**B. Limited Liability of a customer:** The customer’s liability will be limited in the following events:

i. **Customer's Contributory Negligence:** Where the unauthorized transaction is due to the customer’s contributory fraud, negligence, or collusion, for example, the customer shares payment credentials, then the customer will be liable for the entire loss until he/she reports the unauthorized transaction to the Bank. Any loss occurring after the reporting of the unauthorized transaction will be borne by the Bank. ii. **Third Party Breach with delayed reporting:** Where the unauthorized transaction is due to a third-party breach where the deficiency lies neither with the Bank nor with the customer, but the customer reports the unauthorized transaction with a delay of more than three working days, the customer’s liability will be capped depending on the type of account:

| S. No. | Customer accounts | Maximum Customer Liability (₹) |

|---|---|---|

| 1. | Basic Savings Bank Deposit Accounts (BSBDAs) | 5,000 |

| 2. | All other SB accounts, Pradhan Mantri Jan-Dhan Yojana (PMJDY) accounts, Current Accounts and Overdraft Accounts of individuals | 10,000 |

| 3. | Current Accounts and Overdraft Accounts of non-individuals | 25,000 |

The liability will be capped at the transaction value or the amount mentioned in the table, whichever is lower.

\*\*Note:\*\* The customer's liability for delays beyond 7 working days will be determined by the Bank's Board, subject to the RBI guidelines.

**7. Third Party Breach:**

In cases where the loss is due to a third-party breach, the Bank shall credit (shadow reversal) the amount involved in the unauthorized electronic transaction to the customer’s account within 10 working days from the date of notification by the customer.

**8. Roles and Responsibilities of the Bank:**

a. **Transaction Alerts:** The Bank shall send electronic transaction alerts to customers for all electronic banking transactions. The alerts should be sent to the customer’s registered mobile number or email id. b. **Reporting Channels:** The Bank shall provide customers with 24x7 channels for reporting unauthorized electronic banking transactions. This includes a dedicated helpline, website, email, SMS, IVR, etc. c. **Timely Redressal:** The Bank shall endeavor to resolve customer complaints within 90 days of reporting. d. **Security Measures:** The Bank shall implement robust fraud detection and prevention mechanisms and ensure the security of its electronic banking channels. e. **Customer Awareness:** The Bank shall undertake awareness campaigns to educate customers about safe banking practices and how to protect themselves from online fraud. f. **Burden of Proof:** The burden of proving customer liability in unauthorized electronic banking transactions shall lie with the Bank.

**9. Rights and Obligation of the Customer:**

a. **Register for Alerts:** Customers should register for electronic transaction alerts (SMS/e-mail) for all banking transactions. b. **Monitor Transactions:** Customers should regularly monitor transaction alerts and account statements to detect any unauthorized transactions. c. **Protect Credentials:** Customers should take all necessary precautions to protect their banking credentials (e.g., PIN, OTP, passwords) and avoid sharing them with anyone. d. **Report Promptly:** Customers are obligated to report any unauthorized electronic banking transaction to the Bank as soon as they detect it, through the available channels. Prompt reporting can limit or eliminate their liability.

**10. Notifying the Bank on unauthorized transactions:**

Customers can notify the Bank of any unauthorized transaction through the following channels:

* Customer Care/Helpdesk
* Email
* Visit to Branch

The customer must report the transaction as soon as possible after detecting it.

**11. Proof of Customer Liability:**

The burden of proving customer liability in unauthorized electronic banking transactions shall lie with the Bank. The Bank will require sufficient evidence to demonstrate that the customer was negligent or involved in the fraud.

**12. Redressal of Complaints / Grievance:**

The Bank will resolve all customer complaints related to unauthorized electronic banking transactions within 90 days from the date of reporting. If the customer is not satisfied with the resolution, they may escalate the complaint to the concerned Banking Ombudsman/Ombudsman for NBFCs or the Customer Education and Protection Cell (CEPC) in RBI.

**13. Force Majeure:**

The Bank shall not be liable for any loss arising out of unauthorized electronic banking transactions due to reasons beyond its control, including but not limited to, acts of God, war, riot, civil commotion, strike, lockout, industrial dispute, fire, explosion, sabotage, storm, flood, earthquake, or any other natural calamity or disaster, or any other cause whatsoever beyond the reasonable control of the Bank.

**14. Annexure:**

**UNAUTHORIZED ELECTRONIC BANKING TRANSACTION REPORTING FORM**

(This form is for internal reporting and tracking of unauthorized electronic transactions. Customers should use the Bank's designated channels for reporting.)

**Complaint Details:**

1. Name of Customer:
2. Account Number:
3. Mobile Number:
4. Email ID:
5. Type of Unauthorized Transaction: (e.g., Debit Card, Internet Banking, Mobile Banking, UPI)
6. Date & Time of Unauthorized Transaction:
7. Amount of Unauthorized Transaction:
8. Details of Unauthorized Transaction: (e.g., merchant name, transaction ID)
9. Was the Debit Card used at the Branch? (Yes/No)
10. Mode of Reporting the Unauthorized transaction to Bank: (e.g., Customer Care, Email, Visit to Branch, Other)
11. Date & Time of reporting the Unauthorized transactions to Bank:

**Declaration:** I hereby authorize the Bank to take necessary action, including closing linked services (e.g., card, mobile banking, net banking) immediately, due to unauthorized transactions. I confirm that the averments made by me within this form are bona-fide and the information provided is true and accurate to the best of my knowledge and belief. In case this claim is determined by the Bank to be false or maliciously made, I shall be fully responsible for the consequences which may include civil/criminal lawsuit being initiated by the Bank. In case if the Bank compensates the loss due to the above mentioned disputed transactions either partly or fully, and if I/we receive any insurance claim subsequently for the same disputed transaction(s), I will inform the matter to the Bank and agree to pay back the compensation paid by the Bank.

Customer Name: Signature: Place: Date: