CUSTOMER PROTECTION POLICY

With the increased thrust on financial inclusion through Electronic Banking transactions and customer protection, it is important to inform and educate the customers about their rights and responsibilities, unauthorised transaction and process of notifying the Bank.

The objective of the Policy is to establish a system where the customer can notify the Bank timely and seamlessly about any unauthorised transactions and reporting of any financial loss the customer might have incurred due to electronic banking transaction .

This policy document covers the following aspects:

1. Definition of electronic Banking transactions
2. Risks and responsibilities of the customer
3. Reporting of unauthorised transactions by customer to the Bank
4. Liability of the Customer
5. Timeline to the Bank for settling of such transaction
6. Escalation matrix
7. Reporting and Monitoring Requirements

1. Definition of Electronic Banking transactions

In a broad sense, electronic banking transactions can be divided into two categories:

- Remote/ online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions e.g. internet banking, mobile banking, card not present (CNP) transactions), Pre-paid Payment Instruments (PPI), and
- Face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)

2. **Risk and Responsibilities of the Customer :**

Before doing his/her first electronic fund transaction and consequent ones, a customer should ensure the following :

a. To register his/her own valid mobile number and email ID with the Bank and avail SMS & email alert service of the Bank .

b. To take utmost care that the ATM /Debit card is in his/her possession, and if lost, intimate the Bank immediately through the various means provided by the Bank. Also,

c. police intimation in this regard is to be made informing the concerned police station about the loss/misplacement of the ATM/Debit card and a copy of the acknowledged intimation to be provided to the Bank.

d. To set a PIN for ATM/Debit card which is different from address, telephone number, Social Security number, or Birth Date. This will make it more difficult for a fraudster to use his/her card.

e. To be alert at all times and not share ATM/Debit card PIN or card with any one.

f. To keep and compare his/her receipts notification from Bank for all types of Electronic Financial Transaction (EFT) transactions with his/her statements so that he/she can find errors or unauthorized transfers and report them.

3. **Reporting of unauthorised transactions by customer to the Bank**

Customer should verify the notifications received from the Bank through SMS /email, and if he/she comes across any transaction not initiated by him/her, such unauthorised EFT should be reported to the Bank for blocking the card. In case of theft/ misplacement of ATM /Debit card too, he/she should inform the Bank for blocking the card.

A. In order to mitigate any loss a customer should block his/her ATM/Debit card, through any one of the following channels

(i) By sending an SMS : On identifying unauthorised EFT and to stop the ATM/Debit card a customer shall :

a. Use his/her registered mobile number to send the SMS to the Bank

b. Send it to pre-determined number given by the Bank for the purpose.

c. Bank, after verifying customer's registered mobile number will send a response to his/her registered mobile number.

d. Verify the response and confirm that the card has been successfully stopped

(ii) calling his/her base branch :

If the unauthorised transaction happens on a working day and during business hours, customer may also contact his/her base branch and notify the Bank about such unauthorised transaction and request to "STOP/Block " the ATM/Debit card .

(iii) By calling the customer care number :

Customer can call the Bank's predetermined Customer Care number, and request to stop/block the concerned ATM/debit card. This customer care number would be accessible 24x7 only for blocking of ATM/debit card.

B. Process for reporting unauthorised EFT and claiming reversal

After taking necessary steps for blocking the ATM/debit card, customer should adopt the following process to inform the Bank about the unauthorised transaction.

a. Customer shall collect the ATM/debit card dispute charge back form, from any of the branches of the Bank or download the same from Bank's website

b. Customer shall correctly fill the necessary information in the form and submit the same to his/her base Branch.

c. Customer shall fill a fresh ATM/debit card application form and select the option – "Lost" for new ATM / debit card and submit the same to the base Branch.

4. **<u>Limited Liability of a Customer</u>**

A. Zero Liability of a Customer :

A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs in the following events:

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

b. 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 unauthorised transaction.

B. Limited Liability of a Customer :

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

- In cases where the 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 transaction to the bank. Any loss occurring after the reporting of the unauthorised transaction shall be borne by the bank.
- In cases where the responsibility for the unauthorised 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 1, whichever is lower.

Table (1)

Maximum Liability of a Customer under point 4 (A) & (B)

Type of Account	**Maximum**
	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards (as & when introduced) • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current Accounts/ Overdraft Accounts of Individuals with	10,000
• All other Current / Overdraft Accounts	25,000
Irrespective of above set limits, if the customer fails to report unauthorised transaction within 7 working days from the date of receipt of communication from the Bank	**Entire loss to be borne by customer**

Overall liability of the customer in third party breaches, as detailed in paragraph **4 A (ii)** and paragraph **4 B (ii)** above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table 2:

Table (2)

Summary of Customer's Liability

Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's Liability (Rs)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the
Beyond 7 working days	**Entire loss to be borne by customer.**

The number of working days mentioned in Table 1 shall be counted as per the working schedule of the base branch of the customer excluding the date of receiving the communication.

5. **Timeline to the Bank for settling of such transaction**

On being notified by the customer, the Bank shall

a. 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 the process of establishing the liability to be completed .

b. In not more than 90 working days, bank shall establish the liability of the customer if any and notify the customer accordingly

c. Bank shall clearly notify the customer about the status of the complaint and settlement of the charge.

d. Only on receipt of this notification from the Bank, the shadow reversal of the amount will be available for the customer.

e. The credit shall be value dated to be as of the date of the unauthorised

transaction. This will ensure that customer does not lose any interest on the amount.

The onus of proving customer liability in case of unauthorised electronic banking transactions shall lie on the Bank.

6. **Escalation matrix**

Bank as mentioned in point 5, has to revert and resolve the complaint/dispute within the stipulated time. In case of non-receipt of any update/confirmation the customer may escalate the matter as below

Table (3)
Escalation Matrix

Day	Description	Reporting
1	Reporting of unauthorised transaction as mentioned in point 3(B) above	Base branch
10	On non receipt of the shadow reversal or final settlement of the disputed amount	Base branch
12	No response from the Base branch	Chargeback Team.
20	No response from Chargeback Team	Head of Operations

7. **Reporting and Monitoring Requirements :**

Unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon along with Customer liability cases shall be informed to the Finance Committee/Board on a quarterly basis. i.e. July for Q1, October for Q2, January for Q3 and April for Q4 of every year. 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 Committee/Board shall take appropriate measures to improve the systems and procedures.

All such transactions shall also be reviewed by the Bank's internal auditors.