Thane Bharat Sahakari Bank Ltd.
(Scheduled Bank)

Customer Protection Policy
(Unauthorized Electronic Banking Transactions)

- **Introduction –**

With growing Digital transactions across the Banking industry, the risks associated with it have multiplied and hence Customer protection against unauthorized electronic banking transactions has assumed greater importance in today banking world. This policy covers aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities, and customer liability arising in specific scenarios of unauthorized electronic banking transactions.

In this regard, RBI vide its circular no. DCBR.BPD.(PCB/RCB).Cir.No.06/ 12.05.001/2017-18 dated 14th December 2017 has issued guidelines regarding Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions. The policy defines the following aspects –

- Rights and Obligations of customers in case of unauthorized transactions in specified scenarios i.e. debit to customer accounts owing to customer negligence / bank negligence / banking system frauds / third party breaches etc.
- Mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions, and customer liability in case of unauthorized electronic banking transactions and acknowledgement of complaints.
- Robust Grievance Redressal structure as per extant instructions, escalation matrix, clear timelines for resolution of customer complaints, and compensation keeping in view the instructions contained in 6 below.

- **Strenghthing of Systems and Procedures**

Electronic banking transactions can be broadly 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.)

- **Bank commitment to ensuring customer protection:**

RBI has instructed banks to design their systems and procedures to make Customers feel safe about carrying out electronic banking transactions by putting in place the below described systems and procedures.

- Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers.

- Robust and dynamic fraud detection and prevention mechanism.

- Mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events.

- Appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from.

- A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

- **Reporting of unauthorised transactions by customers to Bank**

- The Bank will ensure that customers are mandatorily registered for SMS alerts and wherever available for email alerts, for electronic banking transactions. Bank will mandatorily send SMS alerts to the customers, while the email alerts may be sent wherever registered.

- The bank will not be able to offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. These facilities will be withdrawn for customers after due notice is provided to them.

- The Bank requires customers to notify the Bank about any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction as longer the time taken to notify the bank, the higher will be the risk of loss to the bank/customer.

- To enable this to be done in a smooth and efficient manner, the Bank will provide customers with 24x7 access through multiple channels (via website, SMS, e-mail, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc.

- Further, the Bank will provide a direct link for lodging the complaints, with specific option to report unauthorised electronic transactions in the home page of the Bank's website. Immediate response (including auto response) will be sent to the

customers acknowledging the complaint along with the registered complaint number.

- The communication systems used by the Bank to send alerts and receive their responses thereto will record the time and date of delivery of the message and receipt of customer's response, if any, to the Bank. On receipt of report of an unauthorised transaction from the customer, the Bank will take immediate steps to prevent further unauthorised transactions in the account. On being notified by the customer, the Bank will undertake a preliminary investigation to establish the reason for the dispute.

- **Liability of a Customer**

- **Zero Liability of a Customer**

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

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

- 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.

- **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, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Transactions where a Password / PIN / OTP (One Time Password) has been used or where the transaction has been performed with information available only with the customer or can be done only with the knowledge of the customer will be treated as 'transaction performed due to customer negligence'. Any loss occurring after the reporting of the unauthorised transaction will 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 paragraph 5 (b) (ii)

Type 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 Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to up to Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000
• All other Current/ Cash Credit Overdraft Accounts	25,000

Further, if the delay in reporting by the customer is beyond seven working days, the customer shall be liable for the entire value of the transaction(s) involved.

The Bank will provide the details of policy with regard to customers' liability at the time of opening the accounts. The Bank will display the approved policy in bank's website. The existing customers would also be informed about the Bank's policy through publication on the website and where possible, through SMS and email alerts.

Overall liability of the customer in third party breaches, as detailed in paragraph 5 (a) (ii) and paragraph 5 (b) (ii) above, where the responsibility for the unauthorised electronic banking transaction lies neither with the bank nor with the customer, but lies elsewhere in the system is summarised in 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 amount mentioned in Table 1 of the Policy whichever is lower
Beyond 7 working days	The customer liability to the extent of the value of the transaction(s).

The number of working days will be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

- **Reversal Timeline for Zero Liability/ Limited Liability of customer**

On being notified by the customer, the Bank will credit the amount involved in the unauthorized electronic transaction to the customer's account within 10 working days from the date of such notification by the customer. The credit will be value dated to be as of the date of the unauthorized transaction. The credit will be provided as a shadow credit, which means that the customer will not be able to use the funds credited by way of temporary/shadow credit till the dispute is resolved in favour of the customer. Bank may also at its discretion decide to waive off any customer liability in case of unauthorized electronic banking transactions even in cases of customer negligence.

Further, the Bank will ensure that:

- a complaint is resolved and liability of the customer, if any, established within a period not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraph no 5 & 6 above

- where Bank is unable to resolve the complaint, or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraph no 5 & 6 above will be paid to the customer; and

- in case of debit card/ bank account, the customer does not suffer loss of interest.

For all disputed cases, customers shall be required to provide the supporting documents namely, dispute form, copy of the FIR, etc. within the stipulated timeframe. In case the customer is unable to provide the documents or there is a delay on part of the customer in submitting the documents within the stipulated timeframe, post due follow up by the Bank, the Bank shall term such disputes as unable to conclude and the liability of the unauthorized transactions in such cases will remain with the customer only.

- **Reporting and Monitoring Mechanism**

- Banks shall put in place a suitable mechanism and structure for the reporting of cases of unauthorized electronic banking transactions to the Board / Committee of Board.

- 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 / Committee of Board shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the Grievance Redressal Mechanism and take appropriate measures to improve the systems and procedures.

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

- **Linkage to other Customer Service Policies of the Bank:**

This Policy shall be read in conjunction with the Customer Compensation policy and Customer Grievance Redressal policy.

- **Burden of proof of Customer liability:**

The burden of proving Customer liability in case of unauthorized electronic banking transactions shall be with the bank.