SARVODAYA COMMERCIAL CO-OPERATIVE BANK LTD., MEHSANA

CUSTOMER PROTECTION POLICY- LIMITED LIABILITY OF CUSTOMERS OF THE BANK IN UNATHORISED ELECTRONIC BANKING TRANSACTIONS.

Approved vide Resolution No. 17(22) in the meeting of Board of Directors dated 28/07/2021

Reference : RBI Circular No. DCBR.BPD.(PCB/RCB) Cir.06/12.05.001/2017-18 dated December 14,2017

Preface:

The policy is framed as per guidelines issued by Reserve Bank of India Vide circular Ref. No. DCBR.BPD. (PCB/RCB) Cir.No.06/12.05.001/2017-18 dated December 14, 2017 for Customer Protection- Limited liability of Customer of Co-Operative Banks in unauthorized electronic banking transactions. In terms of the circular it is required to formulate a Board Approved policy to be displayed at branches and formulate necessary procedure there under to be followed for customer protection and the criteria for determining the customer liability relating to unauthorized transaction resulting in debits to their accounts/cards.

Strengthening of systems and procedures

1. Broadly, the electronic banking transactions will be divided into two categories:
   i. 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
   ii. Face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)
2. The systems and procedures in banks is designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, the bank has put in place:
   i. Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers.
   ii. Robust and dynamic fraud detection and prevention mechanism.
   iii. 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.
   iv. Appropriate measures to mitigate the risks and protect themselves against the liabilities arising there form; and
   v. A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

Reporting of unauthorized transactions by customers to banks.

3. The bank will ask the customers to mandatorily register for SMS alerts and, wherever available, register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The customers must be advised to notify their bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction, and informed that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/ customer. To facilitate this, the bank will provide customers with 24*7 access through multiple channels (at a minimum, via phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorized transactions that have taken place and/or theft of payment instrument such as card, etc. The bank shall also enable customers to instantly respond by "Reply" to the SMS e-mail address to notify the objection, if any. Further , a direct link for lodging the complaints. With specific option to report unauthorized electronic transactions shall be provided by the bank on home page of its website. The loss/fraud

reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complain number. The communication systems used by banks to send alerts and receive their responses thereto must record the time and date of delivery of the message and receipt of customer's response, if any, to them. This shall be important in determining the extent of a customer's liability. The bank may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. On receipt of report of an unauthorized transaction from the customer, the bank should take immediate steps to prevent further unauthorized transactions in the account.

Limited liability of a customer

(a) Zero Liability of a Customer

4. A customer's entitlement to zero liability will arise where the unauthorized transaction occurs in the following events:
   i. Contributory fraud/negligence/deficiency on the part of the bank (irrespective of whether of 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 lie 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

5. A customer shall be liable for the loss occurring due to unauthorized transactions in the following cases :
   i. 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 unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction 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 the customer notifies the bank of such a transaction within four to seven working days of receiving a communication of the 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 (ii)

Type of Account	Maximum Liability (□)
• BSBD Account	5,000
• All other SB Account	
• 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 Rs. 25 lakh	10,000
• Credit cards with limit up to Rs. 5 lakh	
• All other Current/Cash Credit/Overdraft Accounts	25,000

Further , if the delay in reporting is beyond seven working days, the customer liability will be liable for the entire loss. Banks will provide the details of their policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Banks will also display their approved policy in public domain for wider dissemination. The existing customers must also be individually informed about the bank's policy.

6. Overall liability of the customer in third party breaches, as detailed in paragraph 4 (ii) and paragraph 5(ii) above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized 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 (□)
Within 3 working days	Zero liability
Within 4 to 7 working days	the transaction value or the amount mentioned in Table 1 Which is lower
Beyond 7 working days	liable for total transaction value.

The number of working days mentioned in Table 2 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 of customer

7. On being notified by the customer, the bank will credit (shadow reversal) 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 (without waiting for settlement of insurance claim, if any). The credit will be value dated to be as of the date of the unauthorized transaction.
8. **Further , bank will ensure that:**
   i. A complaint is resolved and liability of the customer, if any, established and the customer is compensated as per provisions of paragraphs 4 to 7 above, within 90 days from the date of receipt of the complaint;
   ii. Where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 4 to 7 is paid immediately to the customer; and
   iii. In case of debit card/bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

Burden of Proof

9. The burden of proving customer liability in case of unauthorized electronic banking transactions will led on the bank.

Reporting and Monitoring Requirements

10. The banks will put in place a suitable mechanism and structure for the reporting of cases of unauthorized electronic banking transactions to the Board or one of its Committees. The reporting will, inter alia, include volume/number of cases and the aggregate value involved and distribution across various categories of cases viz., card present transaction, card not present transactions, internet banking, mobile banking, ATM transactions, etc. The board of the bank will periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievance redresser mechanism and take appropriate measures to improve the systems and procedures. All such transactions will be reviewed by the bank's internal auditors.

Approval by Board of Directors : This policy have been prepared for two years. It will be reviewed as and when felt necessary by the Board or before March, 31, 2023. The Board of directors approved the customer protection policy vide resolution Number 17 (22) in Board Meeting held on 28/07/2021.