Customer Protection Policy -Limiting Liability of Customers in Unauthorised Electronic Banking 2018-19

INDEX

1) Introduction

Customer Protection is an integral aspect of the functioning of an Organisation. The Consistent growth in Bank's business can be ensured only with an effective customer service at all levels. As the quality and content of dispensation of customer service definitely requires a hassle free delivery it also requires the customer to know their liability in terms of banking transactions.

2) Purpose and scope

The Customer Protection Policy outlines the basic responsibility on part of the customers towards transactions entered with the Bank. The policy applies to all products and services offered by the CITIZENCREDIT Co-operative Bank Ltd., through interactive electronic device ,on internet or by any other electronic method.

3) Objective

The policy defines a sense of creating customer awareness on the risks and responsibilities involved in various electronic banking transactions, and customers liability in case of unauthorised electronic banking transactions, procedure for reporting unauthorised electronic banking transactions and acknowledgement of complaints. The Policy has been formulated in line with guidelines prescribed by RBI from time to time

4) Systems and procedures

The systems and procedures of the bank are designed to make customers feel safe about carrying out banking transactions (Specially Electronic Banking). To achieve this, the bank has to put in place:

4.1) Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers
4.2) A fraud detection Reporting cell and prevention mechanism
4.3) Mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events
4.4) Appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom
4.5) A system of continually and repeatedly advising customers on how to protect themselves from fraud related to electronic banking and payments.

5) Reporting of unauthorised transactions by customers to banks

5.1) The Bank shall ask their customers to mandatorily register for SMS alerts and, wherever available, register for e-mail alerts.. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.

5.2) The customers must be advised to notify their bank of any unauthorised 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.

5.3) The bank should provide 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised electronic banking transactions that have taken place and/or loss or theft of payment instrument.

5.4) The bank should provide a specific option for lodging the complaints or to report unauthorised electronic banking transactions on home page of their website.

6) Measures to be taken on part of the bank.

6.1) 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 complaint number.
6.2) The communication systems used by the Bank 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.
6.3) On receipt of report of an unauthorised transaction from the customer, the Bank shall take immediate steps to prevent further unauthorised transactions in the account.
6.4) The Bank shall report of cases of unauthorised banking transactions to the Board or one of its Committees (as shall be the case). The reporting shall, inter alia, include volume/number of cases and the aggregate value involved.
6.5) The Board shall periodically review the unauthorised 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.
6.6) The bank may not offer facility of electronic transaction, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank.

7) Liability of a Customer

With the increased thrust on IT enabled financial inclusion and related customer protection issues, and considering the recent surge in customer grievances relating to unauthorised electronic banking transactions resulting in debits to their accounts/cards, the criteria for determining the customer liability in these circumstances have been reviewed by RBI.

(7.a) Zero Liability of a Customer

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

7.a.1) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether the transaction is reported by the customer or not).

7.a.2) 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.

(7.b) Limited Liability of a Customer

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

7.b.1) 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 electronic banking transaction shall be borne by the bank.

7.b.2) 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 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 the customer

Type of account	**Maximum Liability (₹)**
BSBDA & BSBDA(Small)	5,000/-
All other SB accounts CD/ CC/ OD accounts of MSMEs CD/ CC/ OD accounts of individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs 25 lakh	10,000/-
All other CD/ CC/ OD	25,000/-

Further, if the delay in reporting is beyond **seven working days**, the customer liability shall be capped at ₹ 50,000/- . The Bank shall provide the details of the policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the account. The Bank shall also display their approved policy in public domain for wider dissemination. The existing customers must also be individually informed about the Bank's policy.

(7.b.3) Overall liability in third party breaches, as detailed in 7.a.2 &7.b.2 where the deficiency lies neither with the bank nor with the customer but lies somewhere 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 (₹)**
Within 3 working days	Zero liability
Within 4-7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower.
Beyond 7 working days	₹ 50,000/-

Note: The number of *working days* mentioned in Table 2 shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

8) Reversal Timeline

8.1) On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised electronic banking transaction to the customer's account within 10 working days from the date of such notification by the customer.
8.2) The credit shall be value dated to be as of the date of the unauthorised transaction. Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence.
8.3) If a complaint is resolved and liability of the customer, if any, is established and the customer is compensated as per approval of the concerned authorities the same should not exceed 90 days from the date of receipt of the complaint.
8.4) The Bank if unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation is to be paid via approval of HOC
8.5) The Bank has to ensure 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.

9) Burden of Proof

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