Customer Protection Policy Limiting Liability of Customers in Unauthorised Electronic Banking

Department	Operations Department
Committee Review	Directors Planning, Business Development, Communications And Marketing Committee
Last Review Date	03.09.2022
Placed at the Planning Committee for FY 2024-26	27.08.2024
Placed at the Board	31.08.2024

CITIZEN CREDIT CO-OP
C.A.O. Mirjan

INDEX

CITIZEN CREDIT CO-OP. BANK LTD. C.A.O. Malad

1) Introduction

Banks are repositories of public trust. Hence customer protection is an intrinsic feature of the functioning of the Bank. Consistent growth in a Bank's business can be achieved only through effective customer service at all levels. It is therefore one of the primary responsibilities of the bank to ensure that its customer's interests are protected through a well documented Customer Protection policy.

2) Purpose and scope

The main purpose of the Customer Protection Policy outlines the responsibility on part of the customers towards transactions entered with the Bank. The scope of the policy extends to all products and services offered by the CITIZENCREDIT Co-operative Bank Ltd., electronically, via the internet or through any other electronic medium.

3) Objective

The objective of the policy aims to create customer awareness on the risks and responsibilities involved in various electronic banking transactions, customer liability in case of unauthorised electronic banking transactions, and the procedure for reporting unauthorised electronic banking transactions and acknowledgement of complaints. The Policy has been formulated in keeping with the guidelines prescribed by RBI from time to time.

Electronic banking transactions are divided into two categories:

1. 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 (credit or a debit card), Pre-paid Payment Instruments (PPI) & UPI

2. Face-to-face/ proximity payment transactions (transactions which require physical payment instrument such as a card (includes credit, debit or any prepaid instrument including Forex card) or mobile phone to be present at the point of transaction, e.g. ATM, POS, etc.)

4) Systems and Procedures

The Bank has put in place systems and procedures designed to ensure customer safety while carrying out banking transactions (Specially Electronic Banking). The bank has taken the following safety measures :

4.1) Creation of a fraud detection and reporting cell and prevention mechanism

4.2) Mechanism and procedures to assess risks -example, gaps in the bank's existing systems - which result from unauthorised transactions. And to measure the liabilities arising out of such events.

4.3) Putting appropriate steps in place to mitigate the risks and protect themselves against the liabilities arising therefrom

4.4) Putting a system in place to continually and repeatedly educate customers to protect themselves from fraud related to electronic banking and payments.

CITIZENCREDIT CO-OP. BANK LTD. C.A.O. Mumbai

5) Reporting of unauthorised transactions by customers to banks

5.1) The Bank to advise customers to mandatorily register for SMS alerts and also educate customers of the features available vide the CCB Mobile App.

5.2) The customers must be made aware to notify the bank of any unauthorised electronic banking transaction at the earliest/immediately after the occurrence of such a transaction. The customer should also be made aware that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank and the customer.

5.3) The bank shall 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 the home page of their website.

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

6.1) The Branch or ATM Dept.to immediately block the card on receipt of loss of card or fraud reporting.If, the card has been blocked by ATM Dept. or by the customer himself through CCB Mobile App, the branch to cross verify the same.

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 cases of unauthorised banking transactions to the Board or one of its Committees (i.e Directors of the Audit Committee). 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.

6.7) The bank to encourage customers to provide mobile numbers and register for SMS transactions when offered any electronic transaction services inclusive of ATM and importance of CCB App.

6.8) Branches are advised to educate their customers on the feature available vide the CCB Mobile App of blocking the card and unblocking the same whenever required.

7) Defining Customers Liability

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.

Zero Liability of a Customer	Limited Liability of a Customer
A customer's entitlement to zero liability shall arise where the unauthorised transaction occurs in the following events:	A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:
a. 1) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether the transaction is reported by the customer or not).	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.
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.	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. Further, if the delay in reporting is beyond seven working days, the customer liability shall be capped as per Table-1. 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 the approved policy at the Branch and on the Bank's website. The existing customers must also be individually informed about the Bank's policy.
	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 summarized in Table 2

CITIZEN CREDIT CO-Op. BANK LTD. C.A.O. Malad

**Third party breaches: Third party breaches would cover (Examples) following unauthorised transactions without customer knowledge;
1. SIM duplication – Cloning of original SIM to create duplicate SIM
2. Application related frauds – Stolen customer identity which is used to avail banks product & services
3. Skimming/Cloning – Collect data from the magnetic strip of the card and copying the information onto another plastic

TABLE 1- Maximum Liability of the Customer	
Type of account	**Maximum Liability (₹)**
• BSBDA & BSBDA(Small)	5,000/-
• All other SB accounts • Pre-paid Payment Instrument and Gift Cards • 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/-

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	100% Customers Liability

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.

CITIZENCREDIT CO-OP. BANK LTD. C.A.O. Malad

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.(without waiting for settlement of insurance claim,if any).The credit shall be value dated to be as of the date of the unauthorised transaction.

8.2) The Bank may at its discretion decide to waive off any customer liability in case of unauthorised electronic banking transaction 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 as prescribed in the above para is to be paid immediately 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.

9) Burden of Proof

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

10) Review of Policy

The Policy will be reviewed by the Board through the Directors' Planning, Business Development, Communications and Marketing Committee, once in two years or as and when there is a major change in the Master Circular issued by RBI.

CITIZEN CREDIT CO-OP. BANK LTD. C.A.O. Mahad