SVC CO-OPERATIVE BANK LTD. | (Multi-State Scheduled Bank) ESTD.1906

HUM SE HAI POSSIBLE

CUSTOMER PROTECTION POLICY

Introduction

With the increased thrust on financial inclusion through Electronic Banking transactions, customer protection against unauthorized transactions is very important. Banks are responsible to inform and educate the customers about their rights and responsibilities.

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

This policy document covers the following aspects, based on the RBI guidelines vide its circular no. DCBR.BPD. (PCB/RCB). Cir.No.06/ 12.05.001/2017-18 dated 14th December 2017 regarding Customer Protection - Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions:

1. Definition of electronic Banking transactions
2. Risks and responsibilities of the customer
3. Reporting of unauthorized 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

This policy is applicable to all customers of the Bank and it is intended to be read, understood and practiced by all employees who directly or indirectly service the customers.

1. Definition of Electronic Banking transactions

Broadly speaking, electronic banking transactions can 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), UPI transactions etc.)

ii. 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, QR Scan etc.)

2. Risk and Responsibilities of the Customer:

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

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

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

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

(iii) To set a PIN for 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.

(iv) To be alert at all times and not share Debit card PIN or card with any one.

(v) To keep and compare their receipts, notifications, SMS etc. From Bank for all types of Electronic Financial Transaction (EFT) transactions with their statements so that they can find errors or unauthorized transfers and report them timely.

(vi) 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 unauthorized EFT should be reported to the Bank for blocking the channel

3. <u>Reporting unauthorized transactions by customer to the Bank</u>

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 unauthorized 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) Customer should block/deactivate the respective or all digital/electronic channels immediately on realizing unauthorized transactions/s in the account.

B) Blocking of Debit Card, UPI & Internet/Mobile banking

(i) **<u>By sending an SMS</u> :** On identifying unauthorized EFT and to stop the Debit card, UPI & Internet banking a customer should: Use their registered mobile number to send the SMS to the Bank

i. In case Card - SMS "STOP CARD "–9820620454
ii. In case of UPI - SMS "STOPUPI" –9820620454
iii. In case of Internet /Mobile banking - SMS "STOPIB" –9820620454
iv. Bank, after verifying customer's registered mobile number will send a response to their registered mobile number.
v. Verify the response and confirm that the concern channel has successfully blocked.

(ii) **By calling the Customer Care Number:**

Customer can call the Bank's Customer Care number 1800 313 2120 and request to Stop/block the digital/electronic channel. This customer care number would be accessible 24x7 only for blocking of channels.

(iii) **Calling the Base Branch:**

If the unauthorized transaction happens on a working day and during business hours, customer may also contact his/her base branch and notify the Bank about such unauthorized transaction and request to block the concerned digital/electronic channel.

.

C) Process for reporting unauthorized digital/electronic transaction

After taking necessary steps for blocking the channels customer should adopt the following process to inform the Bank about the unauthorized transaction.

A. The customer to report unauthorized Card transactions through Online Dispute Resolution (ODR) portal, Svc care call center or by visiting nearest branch. While reporting on Bank's ODR portal or to the branch the customer should ensure to fill-up correct information in the form.

B. Simultaneously, the customer to file complaint with National Cyber Crime Reporting Portal (NCRP) through their website https://cybercrime.gov.in or by calling on the Helpline Number – '1930'

4. Limited Liability of a Customer

I) Zero Liability of a Customer :

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

(i) Contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or 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 lies 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.

II) Limited Liability of a Customer:

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 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 liability (Rs)**
• BSBD Accounts	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 annual average balance (during 365 days preceding the incidence of fraud)/ limit up to Rs.25 lakh	10,000
• All other Current / Overdraft Accounts	25,000 or transaction value whichever is lower
Irrespective of above set limits, In cases where the responsibility for unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere in the system and when there is a delay on the part of the customer in reporting to the Bank beyond seven working days.	**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 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 (Rs)**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table 1, whichever is lower
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.

III) Complete Liability of the customer:

- Customer shall bear the entire loss in cases where the loss is due to negligence by the customer, e.g. where the customer has shared payment credentials or Account/ Transaction details, viz. Internet Banking User ID & Password, mobile banking PIN, UPI PIN, Debit / Credit Card details including Card number, expiry month & year, CVV, Card PIN / OTP or any other critical information through which fraudster may onboard / execute any transaction on any electronic channel or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing / Smishing attack. This could also be due to SIM deactivation by the fraudster. Under such situations, the customer will bear the entire loss until the customer reports unauthorized transaction to the bank.
- In cases where the responsibility for unauthorized electronic banking transaction lies neither with the Bank nor with the customer, but lies elsewhere in the system and when there is a delay on the part of the customer in reporting to the Bank beyond seven working days, the customer would be completely liable for all such transactions.

5. Timeline to the Bank for settling of such transaction

On being notified by the customer, the Bank shall

(i) 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 the process of establishing the liability to be completed .

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

(iii) Bank shall clearly notify the customer about the status of the complaint and settlement of the charge.
Only on receipt of this notification from the Bank, the shadow reversal of the amount will be available for the customer.

(iv) The credit shall be value dated to be as of the date of the unauthorized transaction. This will ensure that customer does not lose any interest on the amount.

(v) In case of debit card/ bank account, the customer does not suffer loss of interest

The burden of proving customer liability in case of unauthorized 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(C) 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	AGM/DM Operations

7. Roles & Responsibilities of the Bank:

- Bank shall ensure that the Customer Protection Policy (unauthorized electronic banking transactions) is available on the Bank's website as well as at Bank's branches for customer reference.
- Bank will regularly conduct awareness on carrying out safe electronic banking transactions to its customers and staff. Information of Safe Banking practices will be made available through campaigns on any or all of the following – website, emails, ATMs, phone banking, net banking, mobile banking or any alternative channel.
- Bank shall communicate to its customers to mandatorily register their mobile number for receiving SMS alerts and e-mail notifications wherever e-mail id is registered.
- SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.
- Bank should not provide electronic channels for Customers not having their mobile number registered with the bank.
- Bank should periodically educate Customers via SMS/ e-mails to notify bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction and make them aware that the longer the time taken to notify the bank, the higher will be the risk of loss to them.
- Bank will enable various modes for reporting of unauthorized transaction by customers.
- Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement specifying complaint number, date and time of transaction alert sent and date and time of receipt of customer's notification.
- On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card.
- Bank shall ensure that all such complaints are resolved and liability of customer if any, established within a maximum of 90 days from the date of receipt of complaint.
- During investigation, in case it is detected that the customer has falsely claimed or disputed valid transactions, the bank reserves its right to take due preventive action of the same including closing the account or blocking card limits.

- Bank may restrict customer from conducting any electronic banking transaction including ATM transaction in case of non-availability of customer's mobile number.
- This policy should be read in conjunction with Grievance Redressal Policy and Customer Compensation Policy of the Bank.

8. Duties & Obligations of the Customer:

- Customer shall mandatorily register valid mobile numbers with the Bank and even email id wherever available with them.
- Customer shall regularly update his /her registered contact details as soon as such details are changed. Bank will only reach out to customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes shall be considered as customer negligence. Any unauthorized transaction arising out of this delay shall be treated as customer liability.
- Customer should provide all necessary documentation as required by the bank to conduct the investigation, for determining customer liability for compensating the customer.
- Customer should co-operate with the Bank's investigating authorities and provide all assistance.
- Customer must not share sensitive information (such as Debit/Credit Card details & PIN, CVV, NetBanking Id & password, OTP, transaction PIN, challenge questions) with any individual, entity, including bank staff.
- Customer must protect his/her device as per best practices specified on the Bank's website, including updation of latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab or any other similar device).
- Customer shall abide by the tips and safeguards mentioned on the Bank's website.
- Customer shall go through various instructions and awareness communication sent by the bank on safe and secured banking.
- Customer must verify transaction details from time to time in his/her bank statement and/ or credit card statement and raise query with the bank as soon as possible in case of any mismatch.

9.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.

- Updated on 07.08.2026