Saraswat Bank

Saraswat Co-operative Bank Ltd.

(Scheduled Bank)

CUSTOMER PROTECTION POLICY

(UNAUTHORIZED ELECTRONIC BANKING TRANSACTIONS)

Version 1.0

Effective From: 01st-April-2020

Document ID: SCB/DBD/<to be provided>

Document Classification: Confidential

Saraswat Co-operative Bank Ltd

Ekanath Thakur Bhavan, 953,

Appasaheb Marathe Marg,

Prabhadevi, Mumbai- 400 025

SARASWAT BANK – CUSTOMER PROTECTION POLICY

Document Control

Document Name	Customer Protection Policy (Unauthorized Electronic Banking Transactions)
Classification	Internal and Confidential
Document#	Saraswat Co-op Bank – Customer Protection Policy v1
Version	1.0
Date Released	01st-April-2020

Document Ownership

Prepared By:	Digital Banking Department	**Document Owner**	Head - Digital Banking
Reviewed By:	Head - Digital Banking	**Recommended By:**	Head – Information Technology
Approved By:	Board of Directors		

Revision History

Sr. No.	Author	Date	Reason for Revision	Version Number
1	Head – Digital Banking	01st-April-2020	1st Release	Version 1.0

Distribution

Sr. No.	To	Date	Version Number
1	IT Department	01st-April-2020	Version 1.0
2	Digital Banking Department		
3	Risk Management Department		
4	Retail Banking Department		
5	Admin Department		
6	All employees and customers		

Content

A. EXECUTIVE SUMMARY:

- ✓ With surge in Digital transactions across the Banking industry, the associated risks have also multiplied and hence Customer protection against unauthorized electronic banking transactions has assumed greater importance from the regulatory perspective.
- ✓ 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.
- ✓ 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 following:
    - 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 therefrom.
    - A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

B. CUSTOMER PROTECTION POLICY

Objectives of the Policy:

- ✓ Customer protection (including mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions)
- ✓ Customer liability in cases of unauthorized electronic banking transactions
- ✓ Customer compensation due to unauthorized electronic banking transactions (within defined timelines)

Coverage:

I. Scope / Applicability:

- ✓ The Policy guidelines apply to Customers conducting electronic banking transactions using the bank's infrastructure viz. ATM, Cash recycler or

bank's Digital channels viz. Mobile banking, Internet banking etc or other bank's infrastructure viz. ATM, POS, UPI app etc.

- ✓ The Policy further covers the guidelines for determining the Customer's liability for unauthorized electronic banking transactions, its compensation and creating customer awareness on the risks and responsibilities involved in electronic banking transactions.
- ✓ The Policy is applicable to all customers of the Bank and it is intended to be read, understood and practiced by all the employees who directly or indirectly service the customers.

II. Ownership:

The ownership of the Customer Protection Policy (Unauthorized Electronic Banking Transactions) is with the Digital Banking Department. The Policy will be revised/ updated, whenever required/ warranted by the Digital Banking Department.

III. Validity of the Policy:

This Policy will be valid for two years i.e. 2020 - 2022. The Policy would be reviewed annually and modifications if any, will be incorporated and reported to the Board.

IV. Review:

Customer Protection Policy shall be reviewed once in 2 years or earlier, in the event significant changes occur to ensure its continuing suitability, adequacy, and effectiveness. Procedures and Processes will be reviewed and updated accordingly.

V. Approval:

Customer Protection Policy and its updates shall be placed by the Head Digital Banking to the CENMAC. Customer Protection Policy shall be reviewed by CENMAC and approved by Board of Directors.

VI. Change / Version Control:

Head – Digital Banking shall control the change and version of the policy document.

VII. Distribution:

The Customer Protection Policy shall be distributed among following departments/ users;

- ✓ IT Department
- ✓ Digital Banking Department

- ✓ Risk Management Department
- ✓ Retail Banking Department
- ✓ Admin Department
- ✓ All employees and customers

VIII. Enforcement and Compliance:

- ✓ Enforcement of the Customer Protection Policy shall be mandatory.
- ✓ Compliance with Customer Protection Policy is mandatory for all applicants as per Applicability.

IX. Dispensation / Exception:

- ✓ Dispensation to be sought from Head - Digital Banking for any deviations to the Customer Protection Policy based on adequate business justification and recommendation / approval by respective Business Head / Function Head, unless otherwise specified in specific policy in this document.
- ✓ Head – Digital Banking shall present such dispensations to CENMAC Committee for ratification.

X. Construction of this document:

- ✓ The Customer Protection Policy has been developed by referring to:
  - Reserve Bank of India's guidelines & Notifications

XI. Structure:

- ✓ This document containing policies is structured as under:
  - Objective: This describes the objectives for having the relevant policy control in place.
  - Scope: This describes the entities to whom the policy applies.
  - Review & Maintenance: This defines the frequency of review and the person responsible for carrying out the review.
  - Broad Contours: The Policy Statement is intent of the management about the control requirement. This is a management direction for compliance by all those covered under the scope of this document.

C. BROAD CONTOURS OF THE POLICY:

a. Definitions:

- ✓ **"Information"** means information regarding the money or other relevant particulars relating to customer, or any User, or the Account or any Transaction.
- ✓ **"PIN"** means a Personal Identification Number, a numeric code generated by customer to access the banking services post login into mobile banking app and/or UPI app and/or execute any financial or non-financial transaction or to access banking services via debit card at ATM or any similar device.
- ✓ **"Password"** means an alphanumeric code generated by the customer to access the banking services post login into internet banking portal and/or execute any financial or non-financial transaction.
- ✓ **"Point of Sale/ POS Transactions"** means transactions initiated at Merchants' point of sale terminals.
- ✓ **"Transaction"** means any transaction or instruction effected or issued, or purported to be effected or issued, by customer through the mobile banking, Internet Banking, UPI, by use of Debit Card etc.
- ✓ **"OTP"** means an automatically generated numeric or alphanumeric string of characters that authenticates the customer for a single transaction.
- ✓ **"Fraudulent transaction"** means a transaction unauthorized by the customer or account holder of bank.
- ✓ **"Hacking"** means gaining of unauthorized access to data in a system or computer.
- ✓ **"Skimming"** means a method used by fraudulent individual to capture financial information from typically a debit / credit card holder.
- ✓ **"Phishing"** refers to fraudulent activity that attempts to obtain sensitive information over the internet.
- ✓ **"Smishing"** means a type of social engineering attack that uses text messages in order to deceive recipients.
- ✓ **"Vishing"** means the fraudulent activity of making phone calls in order to induce individuals to reveal financial information.

b. Electronic banking transactions:

Transactions conducted by the Customer other than from the branch channel can be broadly categorized as below:

- ✓ Remote/ online payment transactions (transactions that do not require physical payment instruments to be presented at the point of transactions eg. Internet banking, mobile banking, UPI, Prepaid instruments, online transactions through card (Card not present) etc.

- ✓ 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 transactions i.e. ATM, POS, QR Scan & Pay etc).

c. Transaction alerts:

- ✓ Bank would ask customers to mandatorily register for SMS alerts and, wherever available, register for e-mail alerts.
- ✓ SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.
- ✓ Bank would not provide electronic channels for Customers not having their mobile number registered with the bank.
- ✓ Bank would 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 may explore any alternative channel for sending alerts and may discontinue existing channel as per the business case.

d. Reporting of unauthorized electronic banking transactions by Customers:

- ✓ Bank must provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking (call center), SMS, e-mail, IVR, a dedicated toll-free helpline etc.) for reporting unauthorized transactions that have taken place and/or loss or theft of payment instrument such as card, etc.
- ✓ Bank shall also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any.
- ✓ Additionally, a direct link for lodging the complaints with specific option to report unauthorized electronic banking transactions would be provided by the bank on home page of the website.
- ✓ Bank shall also implement a loss/ fraud reporting system to ensure that immediate response/ auto-response is sent to the Customers acknowledging the complaint along with the registered complaint number and would also record the date & time of the message and receipt of Customer's response if any.
- ✓ Bank may explore any alternative channel for receiving complaints from customers as per the business case.

e. Third Party Breach:

The following would be considered as Third-party breach where deficiency lies neither with the Bank nor with the customer but elsewhere in the system:

- ✓ Application frauds
- ✓ Hacking
- ✓ Account takeover
- ✓ Skimming / cloning
- ✓ External frauds / compromise of other systems, for e.g. ATMs / mail servers etc. being compromised.

f. Working days:

The number of working days shall be counted as per the working schedule of the home/ nearest branch of the Customer excluding the date of receiving the communication.

g. Zero Liability of the Customer:

A customer's entitlement to zero liability shall arise where the unauthorized 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 unauthorized transaction.

h. Limited liability of the Customer:

A Customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

- ✓ 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.
- ✓ 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 the communication from the Bank, the **per transaction liability** of the Customer shall be as under:

Type of account	Maximum liability in Rs.
For Basic Savings deposit account (Suvidha)	5,000 or transaction value whichever is lower
• 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 Rs.25 lakh • Credit cards with limit up to Rs.5 lakh	10,000 or transaction value whichever is lower
• All other Current/ Cash Credit/ Overdraft Accounts	25,000 or transaction value whichever is lower

* Bank may revise the liability as per the business case wherever warranted.

i. **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.

j. Reversal timeline for Zero liability/ Limited liability of the Customer:

- ✓ On being notified by the customer, the bank shall credit (shadow reversal – lien) 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 shall be value dated to be as of the date of the unauthorized transaction.
- ✓ Banks may also at their discretion decide to waive off any customer liability in case of unauthorized electronic banking transactions even in cases of customer negligence.
- ✓ Customer's complaint shall be resolved and post determining the liability of the customer, the customer is compensated (removing the lien) within 90 days from the date of receipt of the complaint.
- ✓ If the complaint is not resolved or customer liability is not determined, the bank shall compensate the Customer (removing the lien) not exceeding 90 days from the date of receipt of the complaint as per the schedule mentioned earlier in the policy.
- ✓ 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.

k. Burden of proof of Customer liability:

- ✓ The burden of proving Customer liability in case of unauthorized electronic banking transactions shall be with the bank.
- ✓ Bank has a process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India.
- ✓ The Onus to prove all logs / proofs / reports are availability of two factor authentication is on the bank.
- ✓ Any unauthorized electronic banking transaction which has been processed post second factor authentication known only to the customer, would be considered as sufficient proof of customer's involvement / consent in effecting the transaction.

l. Insurance cover:

Bank shall cover its liability by taking adequate insurance cover either through its Bankers indemnity policy, card protection policy or through any cyber insurance policy, if available.

m. 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.
- ✓ 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.

n. Duties & Obligations of the Customer:

- ✓ Customer shall mandatorily register valid mobile number with the Bank and even e-mail 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.

o. Reporting and monitoring:

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

D. CONCLUSION:

Customer Protection Policy (Unauthorized Electronic Banking Transactions) has been framed based on the RBI's guidelines on Customer Protection - Limiting Liability of Customers of Co-

operative Banks in Unauthorized Electronic Banking Transactions and shall remain in force for the period 2020-22.

E. LIST OF ABBREVIATIONS

Abbreviation	Full Form
RBI	Reserve Bank of India
UPI	Unified Payment Interface
PIN	Personal Identification Number
QR	Quick Response
POS	Point of Sale
OTP	One Time Password