BHAGINI NIVEDITA
SAHAKARI BANK LTD, PUNE
A Bank that makes Dreams Worthwhile

Customer protection Policy
Limiting Liability of Customers in Unauthorized Electronic Banking Transactions.

1 BACKGROUND

This document is in terms of Information Technology Act, 2000 and rules there under as applicable and the amended provisions pertaining to electronic records in various statutes as amended by the Information Technology Act, 2000. This electronic record is generated by a computer system and does not require any physical or digital signatures.

This document is published in accordance with the RBI Circular No. RBI/2017-18/109 DCBR.BPD. (PCB/RCB).Cir.No.06/12.05.001/2017-18

Bhagini Nivedita Sahakari Bank Ltd. (The Bank), since its inception has been committed to rendering excellent services to its customers. All the branches of the Bank are fully computerized having Core Banking Software (CBS) and apart from the traditional banking operations, customers are offered services through various digital delivery channels such as ATM, POS, IMPS, mobile banking etc. The Bank has its own state of the art Data Center and has implemented adequate security controls and procedures to ensure security of electronic banking transactions.

However, taking into account the probable risks arising out of unauthorized electronic transactions, the aspect of customer protection in such situations, if any, has been considered by the Bank's Board of Directors In this new policy.

2 OBJECTIVES

This policy seeks to communicate in a fair and transparent manner the Bank's policy on:

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

3 SCOPE

The scope of the policy is given below:

- Giving assurance to customers regarding Bank's secured systems and procedures for electronic banking transactions
- Bank's efforts for Creation of customer awareness on the risks and responsibilities involved in electronic banking transactions
- Defining the rights and obligations of the customers as well as the Bank for measuring the liability arising out of unauthorized electronic transactions.
- Customer liability in cases of unauthorized electronic banking transactions resulting in debits to customers' accounts.
- Mechanism and timelines for compensating the customers for the losses due to unauthorized electronic banking transaction

4 APPLICABILITY:

This policy is applicable to the electronic banking transactions which can be broadly divided into two categories –

1. Remote/online payment transactions which are internet banking, mobile banking, card not present (CNP) transactions (transactions that do not require physical payment instruments to be presented at the point of transactions).
2. Face-to-face/ proximity payment transaction which are ATM, POS, IMPS or any other electronic mode of payment (transactions which require the physical payment instrument such as card or mobile to be present at the point of transaction).
3. a)This policy is applicable to entities that hold relationship with the bank viz.:

    i. Individual and non-individual customers who hold current or savings account.
    ii. Individual / non-individual entities that hold ATM card and / or Debit Card.

iii. Individual / non-individual entities that use other electronic platforms of the Bank like mobile banking, net banking.

b) This policy is not applicable to:

i. Non-Customer that use Bank's infrastructure e.g.ATMs
ii. Entities that are part of the ecosystem such as interchange organizations, Franchises, Intermediaries, Agencies, Service partners, Vendors, Merchants etc.

5 DEFINITIONS & EXPLANATIONS: (for the purpose of this policy)

a) Real loss is defined as financial outgo from customer's account e.g. debit to customer's account or card.
b) Card not present (CNP) transactions are defined as transactions that require use of Card information without card being physically used e.g. e-commerce transactions.
c) Card present (CP) transactions are defined as transactions that require use of physical card e.g. at ATM or shops (POS).
d) Payment transactions are defined as transactions that involve transfer of funds from one account/ wallet to another electronically and do not require card information e.g. NEFT.
e) Unauthorized transaction is defined as debit to customer's account without customer's consent.
f) Consent includes authorization of a transaction debit either through standing instructions, as per accepted banking practice and regulation, based on account opening process and related matters or based on additional authentication required by the bank such as use of security passwords, input of dynamic password (OTP) or static VBV/ MCSC, challenge questions or use of Card details (CVV/ Expiry date) or any other electronic authentication option provided by the Bank.
g) Date & time of reporting is defined as date & time on which customer has submitted a complaint in dispute form prescribed by the bank. The number of working days mentioned in point no 6.4 shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication from customer. Time of reporting will be as per Indian Standard Time.
h) Notification/Notify means an act of the customer reporting unauthorized electronic banking transaction to the bank in accordance with point no 6.3.
i) Number of days will be computed based on working days.
j) Mode of reporting will be the channel through which customer complaint is received first time by the Bank, independent of multiple reporting of the same unauthorized transaction.
k) NPCI means National Payment Corporation of India

l) Loss in foreign currency if any shall be converted to Indian currency for the purpose of this policy as per bank's policies on conversion at card rate net of commission.

6 POINTS COVERED UNDER THE POILICY:

6.1 Bank's measures to ensure safety and security of electronic banking transactions:

For ensuring safety and security of electronic banking transactions carried out by the customers, the Bank has implemented various safeguards and procedures through documented IT Security policies and procedures duly approved by the Bank's Board of directors.

Some of the security measures in respect of electronic banking transactions are given below -

- Bank has implemented System to analyze / monitor transactions to identify suspicious transactions.
- Monitoring of transactions and monitoring of network is regularly carried out to check authenticity of source of transaction.
- SMS alerts are sent to customers for every electronic banking transaction carried out by them.
- The Risk Assessment and analysis in respect of security of IT systems is carried out every six months and also whenever the situation demands. Changes are made to Bank's policies accordingly and approved by Bank's Board of Directors.
- The customers, who wish to carry out electronic banking transactions, are mandatorily asked by the Bank to register their mobile number for receiving SMS alerts.

6.2 Bank's efforts for creating customer awareness on the risks and responsibilities involved in electronic banking transactions:

- The Bank will regularly conduct awareness programme on carrying out safe electronic banking transactions to its customers and staff. The Bank repeatedly advise its customers about the risks and responsibilities involved in electronic banking transactions by various means such as -

1. Frequent SMS alerts are sent to customer regarding importance of maintaining confidentially of data such as card no, pin, cvv, user id and password.
2. Mentoring of individual customers who require help in electronic banking transaction at branch level
3. Training programs for the customers
4. Messages on web-site.
5. Customer education through user manuals prescribed by NPCI.

6.3 Customer liability in cases of unauthorized electronic banking transactions:

In spite of all the efforts, described in above paragraph, if any unauthorized electronic transaction takes place in the customer's account, the customer should inform the Bank immediately by any of the following means -

- By calling bank's 24 / 7 available toll free helpline no. 18002337006
- By personally reporting to home branch during working hours of the Branch.

On receipt of report of an unauthorized transaction, the Bank will take immediate steps to prevent further unauthorized transactions in the account.

6.4 Customer liability in cases of unauthorized electronic banking transactions resulting in debits to customers' accounts.

If, unfortunately, an unauthorized transaction takes place the liability of the customer shall be measured as per the table given below -

A) ZERO LIABILITY OF A CUSTOMER

Customer will have no liability when the unauthorized transaction takes place in the following scenarios:

1. Contributory fraud/negligence/deficiency on the part of bank
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 unauthorized transaction.
3. The number of working days shall be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

B) LIMITED LIABILITY OF CUSTOMER

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

1. In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials details namely viz, internet banking user id /PIN, Debit Card PIN/OTP or due to improper protection on customer devices like mobile/ laptops/desktops leading to malware/Trojan or phishing/vishing attacks, the customer will bear the entire loss incurred until he/she reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

2. 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 and when there is a delay beyond three working days in reporting by the customer,i.e if a customer notifies the Bank within 4 to 7 working days of receiving a communications of the transaction, the per transaction liability of the customer shall be **limited to the transaction value or the amount as shown below in table, whichever is lower.**

Maximum liability of a customer under paragraph 6.4
Table 1 :

Type of account	Maximum liability (Rs.)
• Basic Savings Bank Deposit Account	5,000
• All other Savings Bank accounts	10,000
• Current / Cash Credit / Overdraft accounts of individuals with average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lakh	10,000
• All other Current / Cash Credit / Overdraft Accounts	25,000

C) COMPLETE LIABILITY OF CUSTOMER

1. 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 & PIN, Debit Card PIN/OTP or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing attack. This could also be due to SIM deactivation by the fraudster.

   Under such situations, the customer will bear the entire loss incurred until the customer reports unauthorized transaction to the bank. Any loss occurring after reporting of unauthorized transaction shall be borne by the bank.

2. 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 7 working days, the customer would be completely liable for all such transactions.

D) ADDITIONAL POINTS

i) Customer would not be entitled to compensation of loss if any, in case customer does not agree to get the card hot listed or does not cooperate with the Bank by providing necessary documents including but not limited to police complaint and cardholder dispute form.

ii) Compensation would be limited to real loss after deduction of reversals or recoveries received by the customer.

Summary of the Customer's Liability :

Particulars	**Customer's liability (₹)**
1. In case of Bank's default 2. In case of Third party breach and customer notifies the bank within 3 working days	Zero liability
1. In case of Third party breach and customer notifies the bank within 4 to 7 working days	The transaction value or the amount mentioned in Table no 1, whichever is lower
1. In case of Customer's default 2. In case of Third party breach and customer notifies beyond 7 working days.	Complete liability

6.5 REVERSAL TIMELINE FOR ZERO LIABILITY AND LIMITED LIABILITY OF CUSTOMERS:

- On being notified by the customer, the Bank shall 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

  The credit shall be value dated to be as of the date of unauthorized transaction. However, the customer will not be able to withdraw it unless the complaint is fully resolved.

- The Bank shall ensure that –

  (i) A complaint is resolved and liability of the customer if any, established within 90 days from the date of receipt of the complaint and the customer is compensated as prescribed in clause 6.4 above.

  (ii) Where the Bank is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in clause 6.4 above is paid to the customer; and

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

6.6 THIRD PARTY BREACH

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

a) Application frauds;

b) Account takeover;

c) Skimming / cloning;

d) External frauds / compromise of other systems, for e.g. ATMs / mail servers etc. being compromised.

6.7 RIGHTS & OBLIGATIONS OF THE CUSTOMER

a) Customer's Rights:

i. SMS alerts on valid registered mobile number for all financial electronic debit transactions.

ii. Email alerts where valid email Id is registered for alerts with the Bank.

iii. Register complaint through the modes specified in this document.

iv. Information on valid registered email / mobile number with complaint number and date & time of complaint.

v. Receive compensation in line with this policy document where applicable. This would include getting shadow credit within 10 working days from reporting date and final credit within 90 days of reporting date subject to customer fulfilling obligations detailed herein and with customer liability being limited as specified in clause 6.4 above.

b) Customer obligations :

i. Customer shall mandatorily register valid mobile number with the Bank.

ii. 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.

iii. Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide copy of the same to the Bank.

iv. Customer should co-operate with the Bank's investigating team and provide all assistance.

v. Customer must not share sensitive information (such as Debit, PIN, CVV, Net-Banking Id & password, OTP, transaction PIN, challenge questions) with any entity, including bank staff.

vi. Customer must protect his/her device as per best practices and update latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab)

vii. Customer shall go through various instructions and awareness communication sent by the bank on secured banking

viii. Customer must set transaction limits to ensure minimized exposure.

ix. Customer must verify transaction details from time to time in his/her bank statement and raise query with the bank as soon as possible in case of any mismatch.

x. Customer should attend training / awareness programs conducted by the bank.

6.8 FORCE MAJEURE:

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.

6.9 COMPLIANCE

The report of unauthorized electronic banking transactions and actions taken there on shall be placed before every board meeting. All such transactions will be reviewed by Bank's internal Auditors.

The Board of Directors has powers to make changes in the Policy from time to time.

-----x-----