INDRAPRASTHA SEHKARI BANK LTD.

Customer Protection Policy
(Unauthorized Electronic Banking Transactions)

Need for: With the surge in digital transactions across the Banking Industry, associated risks have also multiplied hence Customer Protection against unauthorized electronic banking transactions has assumed greater significance from regulatory perspectives. As such, the Reserve Bank of India has issued guidelines regarding Customer Protection vide its circular dated 14.12.2017 limiting liability of customers of Co-operative Banks in Unauthorized Electronic Banking Transactions and instructed banks to formulate policy procedures to make customers feel safe while 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 resulting from unauthorized transactions and measure the liabilities arising out of such events;
- Appropriate measures to mitigate and risks and protect themselves against the liabilities arising therefrom; and
- A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

1.Objectives of the policy:

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).

2.Applicability:

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 are directly or indirectly involved in customer service.

3. Broad outlines:

A. Electronic Banking transactions:

(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).

(ii) Face-to-face/ proximity payment transactions (transactions which require the physical payment instrument such as card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)

The Policy covers transactions only through the above modes and does not include Electronics Banking Transactions done through NEFT/RTGS.

B. Transaction Alerts:

- The Bank would ask customers to mandatorily register for SMS alerts, wherever available, register for e-mail alerts;
- SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent wherever registered;
- The 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 risk of loss to them.

C. Reporting of unauthorized electronic banking transactions by customers:

- The Bank provide its customers, 24x7 access through multiple channels (at a minimum via website, phone banking (call center), SMS, e-mail, a dedicated helpline etc) for reporting unauthorized transactions that have taken place and /or loss or theft of payment instrument such as card etc.
- The Bank shall immediately send a response to the customers acknowledging their complaints.

.

D. Third Party Breach:

Where deficiency lies neither with the Bank nor with the customer but elsewhere in the system, would be considered as a Third-Party Breach, for example:

- Application fraud
- Hacking
- Account take over
- Skimming/cloning
- External frauds/compromise of other systems (e.g. ATMs/mail-servers, being compromised)

E. 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.

F. Zero Liability of customer: A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:

- Customer shall be entitled to full compensation of real loss in the event of contributory fraud / negligence / deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).

- Customer has Zero liability in all cases of third party breach where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system and the customer notified the bank within **three working days** of receiving the communication from the banking regarding the unauthorized transaction.

G. Limited Liability of customer: Customer shall be liable for the loss occurring due to unauthorized transactions in the following cases:

i. Liability in case of financial losses due to unauthorized electronic transactions where responsibility for such transactions lies neither with the bank nor with the customer, but lies elsewhere in the system, and

ii. There is a delay on the part of customer in notifying / reporting to the Bank beyond 3 working days and less than or equal to 7 working days (after receiving the intimation from the Bank), the liability of the customer per transaction shall be limited to transaction value or amounts mentioned in Table-I whichever is lower.

TABL E- 1

Maximum Liability of a Customer under paragraph 5 (ii)

Type of Account	Maximum Liability(Rs)
BSBD accounts	5000
• 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	10,000
All other Current/Cash Credit/Overdraft Accounts	25000

H. Complete Liability of customer:

i) 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/ 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 until he reports unauthorized transaction to the bank. Any loss occurring after reporting of unauthorized transaction shall be borne by the bank.

ii) 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.

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 to 7 working days	The transaction value or the amou mentioned in Table 1, whichever is lower
Beyond 7 working days	100% liability of the customer.

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.

I. 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
- Bank may also at its 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.

J. 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.
- Onus to prove all logs / proofs / reports and 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.

4. Roles & Responsibilities of the Bank:

a) The Bank shall ensure that the Customer protection policy is available on the Bank's website as well as at Bank's branches for the reference by customers. The Bank shall also ensure that existing customers are individually informed about the bank's policy.

b) The Bank will regularly conduct awareness on carrying out safe electronic banking transactions to its customers and staff. Such information will include rights and obligation of the customers as well as non-disclosure of sensitive information e.g. password, PIN, OTP, date of birth, etc.

c) The Bank shall communicate to its customers to mandatorily register their mobile number for SMS alerts. The Bank will send SMS alerts to all valid registered mobile number for all debit electronic banking transactions. The Bank may also send alert by email where email Id has been registered with the Bank.

d) The Bank will provide a contact number which can be accessed 24x7 by the customers for reporting of unauthorized transaction by customers. The contact number should also be available on home page of website.

The customer can also report the unauthorized transactions in the account or card through its branches.

e) On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account or card.

f) The 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, failing which, bank would pay compensation as described in Table 1.

g) During investigation, in case it is detected that the customer has falsely claimed or disputed a valid transactions, the bank reserves its right to take due preventive action of the same including closing the account or blocking card limits.

h) The Bank may restrict customer from conducting electronic banking transaction including ATM transaction in case of non-availability of customer's mobile number.

5. Rights & Obligations of the Customer:

a. Customer is entitled to

i. SMS alerts on valid registered mobile number for all financial electronic debit transactions. Customer must verify transaction details with the SMS received for financial electronic debit transactions.

ii. Register complaints to the Bank through modes – as specified by the Bank i.e. at valid mobile Phone/E-mail.

iii. 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 Table-1.

b. Customer is bound by following obligations with respect to banking activities:

(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 authorities and provide all assistance.

(v) Customer must not share sensitive information (such as Debit/Credit Card details & 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 including updation of 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.

6. Notifying the Bank of the unauthorized transaction:

a) Customer shall report unauthorized transaction to the Bank at the earliest, with basic details such as Customer ID and/ or Card number (last 4 digits), date & time of transaction and amount of transaction.

b) Customer shall follow bank's reporting process as specified in 6(d) :

i. Notify/ report through the options listed in the section on Roles & responsibilities of Bank. In case customer is unable to do so, customer could report through phone banking or at the nearest branch.

ii. Lodge police complaint and maintain copy of the same and furnish police complaint when sought by bank's authorized personnel.

c) Customer shall authorize the bank to block the debit card/ account(s) to reduce likelihood of additional loss.

d) Customer to clearly specify the facilities to be blocked failing which the Bank reserves the right to block all electronic transactions of the customer to protect the customer's interest. Also, revoking these blocks would require explicit consent from customer for each facility.

e) Customer shall share relevant documents as needed for investigation or insurance claim.

f) Fully co-operate and comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.

7. 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.

8. Reporting and Monitoring Requirement

The Bank shall report the cases of unauthorized Electronic Banking Transactions to the Board on quarterly basis. The reporting shall inter alia, include volume, number of cases and the aggregate value involved in unauthorized banking transactions. The Board shall also review the unauthorized Electronic Banking Transaction reported by the Customer and also action taken thereon, as well as the functioning of the grievance redressal mechanism.

9. **Conclusion:** Customer Protection Policy (Unauthorized Electronic Banking Transactions) has been formulated on the basis of RBI guidelines on Customer Protection – Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions. The Policy document may be amended from time to time to align with any fresh guidelines received from RBI in this regard.