THE UDAIPUR MAHILA SAMRIDHI URBAN CO-OP. BANK LTD

(Further referred as "Mahila Samridhi Bank")

CUSTOMER PROTECTION POLICY

(Unauthorized Electronic Banking Transactions)

1. Introduction

Mahila Samridhi Bank, is committed to provide superior and safe customer service experience to all its customers. To enable the above, the Bank has over the years invested in technology and has robust security systems and fraud detection and preventions mechanisms in place to ensure safe and secure banking experience to its customers. Keeping in mind the increasing thrust on financial inclusion & customer protection, the Reserve Bank of India had issued a circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. (RBI/2017-18/109 DCBR.BPD.(PCB/RCB).CIR.NO06/12.05.001/2017-18, December 14, 2017) which inter-alia requires Banks to formulate a Board approved policy in regard to customer protection and compensation in case of unauthorized electronic banking transactions.

2. Objective

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

Electronic banking transactions usually cover transactions through the below modes:

a) 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), etc.)

b) 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, etc.)

c) Any other electronic modes of credit effected from one entity to another currently being used or adopted from time to time

This policy covers transactions only through the above modes. The policy excludes electronic banking transactions effected on account of error by a customer (e.g. NEFT carried out to an incorrect payee or for an incorrect amount), transactions done under duress, claims due to opportunity loss, reputation loss, other incidental costs or collateral damage.

4. Applicability

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 use other electronic platforms of the Bank like Mobile Banking etc.

b) This policy is not applicable to:

i) Non-Customer that use Bank's infrastructure e.g. ATMs, electronic wallet.

ii) Entities that are part of the ecosystem such as Interchange organisations, 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) Unauthorised 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 unique complaint. Date of receiving communication from the Bank, is excluded for purpose of computing number of working days for all action specified in this policy. The working schedule of the home branch would be considered for calculating working days for customer reporting. Time of reporting will be as per Indian Standard Time.

h) Notification means an act of the customer reporting unauthorized electronic banking transaction to the bank

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.

6. Points Covered Under the Policy

Customer shall be compensated in line with this policy in case of loss occurring due to unauthorized transaction as follows:

a) Zero Liability of customer

i) 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)

ii) 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 notifies the bank within **three working days** of receiving the communication from the bank regarding the unauthorised transaction

b) Limited Liability of customer

i) Liability in case of financial losses due to unauthorized electronic transactions where responsibility for such transaction 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 Annexure -1 whichever is lower

c) 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/Credit 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 until the customer reports unauthorised transaction to the bank. Any loss occurring after reporting of unauthorised 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.

d) Other Points

i) The Bank shall afford shadow credit to the customer account within 10 working days from the date of reporting in all cases as per above statements. Within 90 days of date of reporting, the Bank shall either establish customer negligence or provide final credit to customer. Customer will be given value dated credit (based on date of unauthorized transaction) when customer becomes eligible to be compensated. In case of debit card/ bank account, the customer shall not suffer loss of interest and in case of credit card; customer shall not bear any additional burden of interest for such credit.

ii) The Bank may, at its discretion, agree to credit the customer even in case of an established negligence by the customer.

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

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

7. 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

8. Roles and 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. 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. 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 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 enable various modes for reporting of unauthorized transaction by customers. These may include SMS, email, website, toll free number, IVR, Phone Banking or through its branches.

e) The 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.

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 Annexures 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.

i) The policy is available on the following link:

http://www.samridhibank.com/pdf/Customer_Protection_Policy.pdf

9. Rights & Obligations of the Customer

a) Customer is entitled to

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 multiple modes – as specified in point relating to Bank's roles & responsibilities

iv) Intimation at 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 Annexure-I

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, Mobile 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 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)

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.

10. 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 viz.

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 or at the nearest branch.

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

c) Customer shall authorise the bank to block the credit/ debit card/ Mobile banking/ 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 viz. cardholder dispute form.

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

Annexure -1

Unauthorised Transaction due to Bank's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	**Customer's Maximum Liability (Rs.)**
Customer to report as soon as possible to prevent future losses	Zero Liability
Unauthorised Transaction due to Customer's negligence	
Time taken to report the fraudulent transaction from the date of receiving communication from the Bank	**Customer's Maximum Liability (Rs.)**
Customer to report as soon as possible to prevent future losses	100% liability till it is reported to Bank

Maximum Liability of a Customer in case of unauthorized Electronic Transaction where Responsibility is neither with the Bank nor with the customer but lies elsewhere in the system & customer has reported unauthorized transaction from transaction date within working days specified in following table:		
Type of Account	**Within 3 working days (Rs.)**	**Within 4 to 7 working days (Rs.)**
BSBD Accounts	Zero Liability	5000.00
All other SB accounts		10000.00
Current/ Cash Credit/ Overdraft Accounts of MSMEs		10000.00
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		10000.00
All other Current/ Cash Credit/ Overdraft Accounts		25000.00
Credit cards with limit above Rs.5 lakh		25000.00

Any unauthorized electronic banking transaction reported after 7 working days will be treated as 100% customer liability.

11. REVIEW OF THE POLICY

The Policy will be reviewed before End of the Year or as and when felt necessary by the Board.

12. APPROVAL BY BOARD OF DIRECTORS

The Board of Directors approved "***Customer Protection Policy***" including Procedure in Board Meeting held on 31-03-2018 through. The Board Resolution No. is ***12 (2)(5)***.

CERTIFIED COPY

For, ***THE UDAIPUR MAHILA SAMRIDHI URBAN CO-OP. BANK LTD.***

VINOD CHAPLOT
MD & CEO

Place: UDAIPUR
Date: 31.03.2018