Adarniya P.D.Patilsaheb Sahakari Bank Ltd Karad

CUSTOMER PROTECTION POLICY

(F. Y. 2022-23)

15/3 C Mangalwar Peth, Tilak Road, Karad,

Tal. Karad, Dist. Satara, Maharashtra, Pin- 415 110.

☎ Phone No. (02164) 226525,200125 Tele Fax - (02164) 226525

Email - contact@pdpbank.com

Adarniya P.D.Patilsaheb Sahakari Bank Ltd Karad

Customer Protection policy

1. **Introduction** –

The Reserve Bank of India issued guidelines by Circular No.06 dated December 14, 2017 and advised UCBs to formulate the Board approved policy regarding the limited liabilities of customers in respect of unauthorized Electronic Banking Transactions and compensation towards these digital transactions.

2. **Background**-

The bank has been fully computerized since it's establishment. The electronic transaction records are preserved in CBS. The bank had a digital platform under which the bank provided various digital channels to it's customers like ATM, POS, IMPS (Mobile Banking), UPI, etc. The bank had shifted it's data at Tire IV cloud Data Center. The bank had adopted all required measures to safeguard the security of banking Data. However, taking into account the probable risks arising out of unauthorized electronic transactions, to mitigate such type of risk the bank here defines the compensation limit towards such electronic transactions. This policy is applicable to individuals/entities who hold savings, current, cash credit, Overdraft etc. operative accounts with the bank.

3. **Objectives & Scope**-

The policy deals with fair and transparent manner with customer's digital transactions which covers

A. Customer protection – The customer protection includes mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions.

B. Customer liability- The customer liability arise in cases of unauthorized electronic banking transactions.

C. **Customer compensation-**The Customer compensation means to compensate the customer to some extend where financial transaction occurs due to unauthorized electronic banking transactions (within defined timelines).The customer protection Policy defines the Limited Liability of Customers in respect of Unauthorized Electronic Banking Transactions.

The policy assures the customers regarding the Bank's secured system of electronic banking . The policy also explains the bank's efforts for Creation of customer awareness on the risks and responsibilities involved in electronic banking transactions. The policy also covers rights and obligations of the customers as well as the Bank for measuring the liability arising out of unauthorized electronic transactions. The policy clearly states the Customer liability in cases of unauthorized electronic banking transactions resulting in debits to customers' accounts and Mechanism and timelines for compensating the customers for the losses due to unauthorized electronic banking transactions.

4. Coverage- The electronic banking transactions are broadly divided into two categories.

1. **Remote /online payment**- The transactions executed by customer without using physical payment instruments at the point of transaction e.g., transactions executed/authenticated through , Mobile banking transactions, UPI transactions, card not present (CNP) transactions, pre-paid payment instruments (PPI)etc.

2. Face to Face Transactions- The face to face transactions means the proximity payment 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.)
This policy covers transactions which are executed through above mentioned two modes only.
This policy **excludes** all such electronic banking transactions effected on account of error by a customer (e.g. NEFT, IMPS, RTGS carried out to an incorrect payee or for an incorrect amount), transactions done under force, claims due to opportunity loss, reputation loss, other incidental costs or collateral damage, loss due to the transactions executed by non-EMV comply ATMs etc.)

5. Safeguarding Banking Data-

The bank shall take all possible measures/steps for ensuring safety and security of electronic banking transactions carried out by the customers. The bank shall document & approve various IT security related policies and procedures listed below to safeguard the IT infrastructure.

1. The bank's environment shall be protected with multiple layers of security to allow only need based authenticated access to its systems. All data between the device and the bank's environment is encrypted through use of SSL.
2. The bank shall conduct periodic Vulnerability Assessments & Penetration Tests and keep its systems updated with the latest security updates/patches.
3. The bank has a robust alerting mechanism which sends alerts /SMS of any changes/events in the account. The bank takes adequate safeguards and keeps on reviewing its security processes at regular intervals.
4. The bank regularly monitors the transactions and the network to check the authenticity of the source of the transaction.

5. The Risk Assessment and analysis in respect of security of IT systems is carried out every six months and also whenever the situation demands. The bank modified the policy as per need.

6. The registration of mobile numbers is mandatory for each customer who wishes to carry out electronic banking transactions.

7. The Bank repeatedly advises its customers & staff members about the risks and responsibilities involved in electronic banking transactions. The bank regularly sends SMS messages to customers regarding awareness of digital banking transactions, areas of fraud etc. The bank frequently sends SMS alerts to customers regarding the importance of maintaining confidentiality of data such as card no, pin, cvv, user id and password.

In spite of all the efforts, described above, if any unauthorized electronic transaction takes place in the customer's account, the customer should inform the Bank immediately by calling cell no.9730919555 which is displayed at all branches as well as at all ATM centers. The customer also registers a complaint at a website where mail ID was provided. The Bank will take immediate steps to prevent further unauthorized transactions after receipt of mail/call.

6. Liability of Customer-

A. Zero liability of Customer-In the event of following cases were an unauthorized electronic banking transactions resulting in debits to customers' accounts

1. Customers shall be entitled to full compensation of outgo from the customer's account in the event of contributory fraud/ negligence/ deficiency on the part of the bank. (Irrespective of whether transaction is reported or not, by the customer)

2. 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 unauthorized transactions.

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, 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. The details of limit under Customer protection Policy Limiting Liability in respect of Unauthorized Electronic Banking Transactions are as under-.

Maximum liability of a customer -

Sr.No.	Type of account	Maximum liability (Rs.)
1	Basic Savings Bank Deposit Account	Rs.5,000/-
2	All other Savings Bank accounts	Rs.10,000/-
3	Current / Cash Credit / Overdraft accounts of individuals with average balance (during 365 days preceding the incidence of fraud) / limit up to Rs. 25 lakhs.	Rs.10,000/-
4	All other Current / Cash Credit / Overdraft Accounts	Rs.25,000/-

C-Complete liability of customer-

1. The 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. 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 transactions to the bank. Any loss occurring after reporting of unauthorized transactions shall be borne by the bank.

2. In cases where the responsibility for unauthorized electronic banking transactions 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.

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

D) Additional points-

i) The 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

Sr.No.	Particulars	Customers Liability (In Rs)
1.	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
2.	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
3.	1. In case of Customer's default. 2. In case of Third-party breach and customer notifies beyond 7 working days	Complete liability

7. Reversal Time line for Zero Liability/Limited Liability of Customers- The bank shall credit (shadow credit) 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. Within 90 days of the date of reporting, the Bank shall either establish customer negligence or provide final credit to the customer.

The credit shall be valued dated to be as of the date of the unauthorized transaction such that in case of a debit card/bank account. The Bank may, at its discretion, agree to credit the customer even in case of an established negligence by the customer. The customer would not be entitled to compensation of loss if any, in case customer does not agree to get the card blocked and/or does not cooperate with the Bank by providing necessary documents including but not limited to police complaint and cardholder dispute form.

8. 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) Skimming / cloning;

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

d) If financial loss occur due to the transactions executed by customer on non-EMV comply ATMs.

9. Roles & Responsibilities of Bank-

a) The Bank will provide the details of the policy with regard to customer liability at the time of opening the accounts. The Bank shall display the approved policy on the Bank's website. The policy will also be available 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 through publication on the website.

b) The Bank will regularly conduct awareness on carrying out safe electronic banking transactions to its staff. Information of Safe Banking practices will be made available on any or all of the following - website, emails, ATMs,. Such information will include rights and obligations 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 register for SMS alerts. The Bank will send SMS alerts to all valid registered mobile numbers 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 transactions by customers. These may include SMS, email, website, Mobile Banking, or through its branches.

e) The Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgement. 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) During investigation, in case it is detected that the customer has falsely claimed or disputed a valid transaction, the bank reserves its right to take due preventive action of the same including and not limited to closing the account or blocking card limits

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

10. Rights & Obligations of Customers-

a) Customer's Rights:

i. The customer shall have a right to receive a SMS alert on a valid registered mobile number for all financial electronic debit transactions.

ii. The customer shall have a right to receive Email alerts where valid email Id is registered for alerts with the Bank.

iii. The customer shall have a right to Register complaint through the modes specified in this document.

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

v. To 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 above.

b) Customer obligations:

I. The Customer shall mandatorily register a valid mobile number with the Bank.

ii.Customer shall regularly update his /her registered contact details as soon as such details are changed. The Bank will only reach out to customers at the last known email/ mobile number. Any failure of the 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.The Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide a copy of the same to the Bank. Customer protection Policy Limiting Liability of Customers in Unauthorized Electronic Banking Transactions.

iv. The Customer should cooperate with the Bank’s investigating team and provide all assistance.

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

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

viii.The Customer must set transaction limits to ensure minimized exposure available in mobile banking.

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

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

11. Reporting & monitoring mechanism –

The Customer liability cases shall be periodically reviewed in the Executive Committee of the board as and when received. The Board shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of 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.

12.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. Customer protection Policy Limiting Liability of Customers in Unauthorized Electronic Banking Transactions. The policy shall be reviewed annually preferably at the beginning of the financial year and will be modified as per need & RBI guidelines.

For Adarniya P.D.Patilsaheb Sahakari Bank Ltd, Karad.

Chief Executive Officer