

THE PARWANOO URBAN COOPERATIVE BANK LTD
HO: PLOT NO.4-A, SECTOR-1, PARWANOO
DISTT: SOLAN (H.P) -173220

CUSTOMER PROTECTION POLICY

(Unauthorized Electronic Banking Transactions)

1. INTRODUCTION

The increasing use of electronic payment systems has enhanced customer convenience while also exposing customers and banks to risks arising from unauthorized electronic banking transactions. Protecting customers against such transactions is an important regulatory requirement and forms an integral part of the Bank's risk management framework.

*This Policy has been framed in accordance with the **Reserve Bank of India (RBI) Circular DCBR.BPD.(PCB/RCB).Cir.No.06/12.05.001/2017-18 dated 14 December 2017** on "Customer Protection – Limiting Liability of Customers of Co-operative Banks in Unauthorized Electronic Banking Transactions", as amended from time to time.*

- ❖ *The Policy establishes the framework for:*
- ❖ *Protecting customers from unauthorized electronic banking transactions;*
- ❖ *Determining customer liability;*
- ❖ *Providing timely reversal and compensation wherever applicable;*
- ❖ *Creating awareness regarding safe electronic banking practices; and*
- ❖ *Ensuring compliance with RBI guidelines.*

This Policy applies only to the electronic banking channels presently offered by the Bank, namely:

- ❖ *ATM transactions using the Bank's Debit/ATM Cards;*
- ❖ *Point of Sale (POS) transactions using the Bank's Debit/ATM Cards.*

2. OBJECTIVES

The objectives of this Policy are to:

- 1. Protect customers against unauthorized electronic banking transactions.*
- 2. Define the rights and responsibilities of customers and the Bank.*
- 3. Establish a mechanism for prompt reporting of unauthorized transactions.*
- 4. Specify zero liability, limited liability, and complete liability of customers.*
- 5. Ensure timely reversal of unauthorized transactions and compensation wherever applicable.*

6. *Promote customer awareness regarding safe usage of ATM/Debit Cards.*
7. *Ensure compliance with RBI guidelines.*

3. OWNERSHIP OF THE POLICY

The Information Technology Department shall be the owner and custodian of this Policy. The Department shall review the Policy annually; recommend amendments whenever required due to regulatory or operational changes; and place the revised Policy before the Board of Directors for approval.

4. APPLICABILITY

This Policy shall apply to all customers holding accounts with the Bank who use ATM/Debit Card facilities issued by the Bank; and all employees involved in issuing, operating, monitoring, or servicing electronic banking transactions.

5. SCOPE OF THE POLICY

This Policy covers unauthorized electronic transactions undertaken through:

- ❖ *ATM Cash Withdrawal;*
- ❖ *ATM Balance Enquiry;*
- ❖ *ATM Mini Statement;*
- ❖ *ATM Fund Transfer (where enabled); and*
- ❖ *POS transactions using the Bank's Debit/ATM Cards.*
- ❖ *Ecommerce Transactions through ATM*

The Policy covers:

- ❖ *Reporting of unauthorized transactions;*
- ❖ *Customer liability;*
- ❖ *Transaction reversal;*
- ❖ *Compensation;*
- ❖ *Grievance redressal;*
- ❖ *Fraud reporting;*
- ❖ *Customer awareness; and*
- ❖ *Responsibilities of the Bank and customers.*

The Policy does not cover manual transactions conducted through branch counters or electronic banking channels not offered by the Bank.

6. DEFINITIONS

- **Unauthorized Electronic Banking Transaction:**
Any electronic transaction carried out without the knowledge, authority, or consent of the customer.
- **ATM Transaction:**
Any financial or non-financial transaction performed using the Bank's Debit/ATM Card through an Automated Teller Machine.
- **POS Transaction:**
A transaction undertaken using the Bank's Debit/ATM Card at a Point of Sale terminal for payment of goods or services.
- **Customer:**
An individual or entity maintaining an account with the Bank and using ATM/Debit Card facilities.
- **Working Day:**
A day on which the customer's home branch is open for business, excluding the date on which the customer reports the unauthorized transaction.

7. POLICY FRAMEWORK

The Bank shall establish appropriate systems and procedures to ensure the safety and security of electronic banking transactions. The Bank shall:

- ❖ Implement fraud prevention and detection mechanisms;
- ❖ Monitor suspicious ATM and POS transactions;
- ❖ Promptly investigate reports of unauthorized transactions;
- ❖ Provide secure mechanisms for reporting fraud;
- ❖ Maintain appropriate insurance coverage against electronic banking fraud, wherever considered necessary;
- ❖ Periodically educate customers regarding safe usage of ATM/Debit Cards; and
- ❖ Continuously review internal controls to minimize operational and fraud risks.

The Bank shall ensure that customers receive transaction alerts through SMS for financial transactions wherever mobile numbers are registered with the Bank.

8. CUSTOMER LIABILITY

Zero customer liability	Limited customer liability	Complete Liability of Customer
Contributory fraud/ Negligence/ deficiency on the part of the bank (Irrespective of whether or not the transaction is reported by the customer)	Loss due to negligence of a customer by sharing payment credentials will be borne by the customer till the time he reports the unauthorized transaction to the Bank. Loss occurring after reporting of unauthorized transaction to	The customer shall bear complete liability for losses arising from unauthorized electronic transactions where the loss occurs due to the customer's negligence, including but not limited to:

	<i>the Bank, shall be borne by the Bank</i> <i>If the investigation establishes that the transaction is 2 factor authenticated liability of such transactions lies with customer, burden of proof lies with the bank.</i>	<i>Sharing ATM PIN, card details, OTP, or other confidential credentials;</i> <i>Keeping PIN or authentication details accessible to others;</i> <i>Responding to fraudulent calls, messages, or emails requesting banking information;</i> <i>Failure to protect the Debit/ATM Card or authentication credentials.</i>
<i>**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.</i>	<i>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 when there is a delay of 4 to 7 working days on the part of the customer in notifying the bank of such a transaction, the per transaction liability of the customer shall be limited to the transaction value or amount mentioned in table 2 whichever is lower</i> <i>If the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy</i>	<i>The customer shall bear the loss until the unauthorized transaction is reported to the Bank. Any loss occurring after the customer has reported the unauthorized transaction shall be borne by the Bank.</i>

The liability of customers for unauthorized electronic banking transactions shall be determined in accordance with RBI guidelines issued from time to time.

9. REVERSAL AND COMPENSATION TIMELINE

A. *In cases where the customer has zero liability, the Bank shall:*

- ❖ *Credit the amount involved in the unauthorized transaction to the customer's account within **10 working days from the date of notification by the customer.***
- ❖ *Ensure that such credit is value-dated to the date of the unauthorized transaction.*

- ❖ *Resolve customer complaints and provide final decision within the timelines prescribed by RBI from time to time.*

B. Harmonisation or Turn Around Time (TAT) and customer compensation for failed transactions using authorized Payment systems.

Sl. No.	Description of Incident	Framework for auto-reversal and compensation	
		Timeline for auto-reversal	Compensation payable
1.	<i>Customer's account debited but cash not dispensed</i>	<i>Pro-active reversal (R) of failed transaction within a maximum of T +5 days</i>	<i>Rs. 100/- per day of delayed beyond T+5 days, to the credit of the account holder.</i>
2.	<i>Point of Sale (PoS)(Card present) including Cash at PoS</i> <i>Account debited but confirmation not received at merchant's system.</i>	<i>Auto-reversal within T +5 days</i>	<i>Rs. 100/- per day of delayed beyond T+5 days</i>
3.	<i>Delay in crediting beneficiary's account or reversal of amount</i>	<i>Beneficiary bank to reverse the uncredited transaction with T+1 day</i>	<i>Rs. 100/- per day if delay is beyond T+1 day</i>

10. BURDEN OF PROOF

The burden of proving customer liability in unauthorized electronic banking transactions shall rest with the Bank.

11. CUSTOMER AWARENESS

The Bank shall undertake suitable awareness initiatives regarding Safe usage of Debit/ATM Cards; Protection of PIN and confidential information; Reporting of unauthorized transactions immediately and avoiding disclosure of banking credentials to unknown persons. Customers may report unauthorized transactions through branch offices or designated customer service channels provided by the Bank. The Bank shall maintain a mechanism for timely investigation and resolution of complaints. Depositors shall be advised not to share PIN and handover ATM to any known/unknown persons.

12. REVIEW OF POLICY

This Policy shall be reviewed annually or earlier whenever required due to regulatory or operational changes. Any amendment shall be placed before the Board of Directors for approval.

13. INSURANCE COVERAGE:

The Bank shall assess the risks arising from unauthorized electronic banking transactions and may obtain appropriate insurance coverage against electronic banking frauds, cyber risks, and operational losses, wherever considered necessary.

The Bank shall ensure that:

- ❖ *The insurance coverage is reviewed periodically based on the volume, nature, and risk exposure of electronic banking transactions.*
- ❖ *Claims, wherever applicable, are lodged with the insurance provider within the prescribed timelines.*
- ❖ *The existence of insurance coverage shall not affect the Bank's responsibility towards customers for providing timely credit/reversal of amounts as per RBI guidelines.*
- ❖ *Insurance arrangements shall be treated as an internal risk mitigation mechanism of the Bank and shall not limit customer rights under this Policy.*

14. ROLES AND RESPONSIBILITIES OF THE BANK

The Bank shall establish adequate systems, controls, and procedures to ensure protection of customers against unauthorized electronic banking transactions.

14.1 Information Technology Department

The Information Technology Department shall:

- ❖ *Ensure secure operation of ATM and POS transaction systems.*
- ❖ *Maintain appropriate security controls for electronic transaction processing.*
- ❖ *Monitor system vulnerabilities and implement corrective measures.*
- ❖ *Coordinate with service providers for timely resolution of technical issues.*
- ❖ *Maintain records relating to electronic transaction incidents.*

14.2 Operations Department / Branches

The Operations Department and branches shall:

- ❖ *Provide assistance to customers for reporting unauthorized transactions.*
- ❖ *Verify and process customer complaints promptly.*
- ❖ *Ensure adherence to prescribed timelines for investigation and reversal.*

- ❖ *Maintain proper documentation of complaints and actions taken.*

14.3 Fraud Risk Management Function

The concerned department/function shall:

- ❖ *Monitor suspicious transaction patterns.*
- ❖ *Investigate reported unauthorized transactions.*
- ❖ *Identify fraud trends and emerging risks.*
- ❖ *Recommend preventive measures to reduce fraud exposure*

14.4 Customer Service Function

The customer service function shall:

- ❖ *Provide accessible channels for reporting unauthorized transactions.*
- ❖ *Ensure customers receive acknowledgement of complaints.*
- ❖ *Track complaints until final resolution.*

15. RIGHTS AND OBLIGATIONS OF CUSTOMERS

<i>Rights of Customers</i>	<i>Obligations of Customers</i>
<i>Customers shall have the right to:</i> <i>• Receive protection against unauthorized electronic banking transactions in accordance with RBI guidelines.</i> <i>• Report unauthorized transactions through available Bank channels.</i> <i>• Receive timely acknowledgement and resolution of complaints.</i> <i>• Obtain reversal/credit wherever the customer is eligible under this Policy.</i> <i>• Receive information regarding the status of reported unauthorized transactions.</i> <i>• Approach the Bank's grievance redressal mechanism in case of dissatisfaction.</i> <i>• Immediate credit of reversal of ATM Transactions on demand.</i>	<i>Customers shall:</i> <i>• Keep Debit/ATM Cards, PINs, and authentication credentials confidential.</i> <i>• Do not share card and/or its details, PIN, OTP, or other confidential information with any person.</i> <i>• Immediately report loss, theft, or misuse of Debit/ATM Cards.</i> <i>• Review transaction alerts and account statements regularly.</i> <i>• Inform the Bank immediately upon noticing any unauthorized transaction.</i> <i>• Follow security instructions issued by the Bank from time to time.</i> <i>• Cooperate with the Bank during investigation of unauthorized transactions.</i>

16. REPORTING:

The Bank shall provide suitable channels for customers to report unauthorized electronic banking transactions. Customers may report unauthorized transactions through:

- ❖ *Home branch;*
- ❖ *Customer service channels provided by the Bank; or*
- ❖ *Any other reporting mechanism notified by the Bank from time to time.*

Upon receipt of a complaint, the Bank shall:

- ❖ *Record the date and time of reporting;*
- ❖ *Provide acknowledgement/reference number to the customer;*
- ❖ *Block the affected card/channel wherever required;*
- ❖ *Initiate investigation immediately;*
- ❖ *Determine customer liability as per RBI guidelines and this Policy; and*
- ❖ *Process reversal/credit wherever applicable within prescribed timelines.*

The Bank shall encourage customers to report unauthorized transactions immediately after becoming aware of such transactions.

17. MONITORING AND REVIEW MECHANISM

The Bank shall establish a monitoring framework to ensure effective implementation of this Policy.

The monitoring framework shall include:

- ❖ *Periodic review of unauthorized transaction incidents.*
- ❖ *Analysis of fraud trends and transaction risks.*
- ❖ *Monitoring of ATM and POS transaction patterns.*
- ❖ *Review of complaint handling and resolution timelines.*
- ❖ *Periodic assessment of effectiveness of fraud prevention controls.*
- ❖ *Reporting of significant fraud incidents to the appropriate authority.*
- ❖ *Review of customer awareness initiatives.*

The Information Technology Department, in coordination with concerned departments, shall periodically submit reports on unauthorized electronic banking transactions, complaints, reversals, and preventive measures to the appropriate authority.

The Policy shall be reviewed annually or earlier whenever required due to changes in RBI guidelines, technology, operational processes, or risk environment.

18. RECORD MAINTENANCE

The Bank shall maintain appropriate records relating to:

- ❖ *Customer complaints;*
- ❖ *Unauthorized transaction reports;*
- ❖ *Investigation findings;*
- ❖ *Liability determination;*
- ❖ *Reversal and compensation provided;*
- ❖ *Fraud monitoring reports; and*
- ❖ *Regulatory reporting requirements.*

The Bank presently does not provide Internet Banking, Mobile Banking, UPI, QR Code payments, IMPS, WhatsApp Banking, or any other digital banking channels. Hence, such services are outside the scope of this Policy.

<i>Approval Authority:</i>	<i>Board of Directors</i>
<i>Review Frequency:</i>	<i>Annual</i>
<i>Effective Date:</i>	
<i>Next Review Due:</i>	