TOWN BANK
RESERVE BANK LICENCED

THE PAYYANUR CO-OPERATIVE TOWN BANK LTD. NO.C.827

Policy for

Customer Protection - Limiting Liability

(Limiting Liability of Customers in Unauthorized Electronic Banking Transactions)

Approved in the Board meeting held on 01/01/2024 – DBR No. 14

PAYYANUR CO-OP TOWN BANK LTD. NO.C.827 PAYYANUR

For The Payyanur Co-op. Town Bank Ltd.No.C.827/UBD.KR 889 P (RBI)

Chief Executive Officer

Limiting Liability of Customers in Unauthorised Electronic Banking Transaction.

With the increased thrust on IT enabled financial inclusion and related customer Protection issues, and considering the recent surge in customer grievances relating to unauthorised transactions resulting in debits to their accounts/cards, the criteria for determining the customer liability in these circumstances ,is warranted and so we have framed the directions in this regard which are set out below :

Though our bank is extending ATM card /POS/E-Com, facilities only at present, we are planning to introduce IMPS, Net banking etc. in the near future. As such we have framed this policy taking into consideration of both remote/online and Face to Face transactions.

This should clearly define the rights and obligations of customers in case of unauthorized transactions in specified scenarios i.e. debits to customer accounts owning to customer negligence / bank negligence / banking system frauds/ third party breaches etc. The policy also aims to include mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions, and customer liability in case of unauthorized electronic banking transactions, procedure for reporting unauthorized electronic banking transactions and acknowledgement of complaints. We also provide for a robust grievance redressal structure as per RBI instructions, escalation matrix, clear timelines for resolution of customer complaints, and compensation keeping in view the instructions of RBI and the policy will be prominently displayed at all our branches.

I). Strengthening of systems and procedures.

Broadly, the electronic banking transactions can be divided into two categories:

(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),

and

(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 systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, our bank must put in place:

(i) appropriate systems and procedures to ensure safety and security of electronic Banking transactions carried out by customers;

(ii) robust and dynamic fraud detection and prevention mechanism;

(iii) mechanism to assess the risks (for example, gaps in the bank's existing systems) resulting from unauthorized transactions and measure the liabilities arising out of such events;

(iv) appropriate measures to mitigate the risks and protect themselves against the liabilities arising there from;

and

(v) a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

Reporting of unauthorized transactions by customers to bank,

Our Bank must ask our customers to mandatorily register for SMS alerts and, wherever available, register for e-mail alerts, for electronic banking transactions. The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered. The customers must be advised to notify their bank of any unauthorized electronic banking transaction at the earliest after the occurrence of such transaction, and informed that the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/customer. To facilitate this, we will be providing e-banking services which must provide customers with 24x7 access through multiple channels (at a minimum, via website, phone banking, SMS, e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorized transactions that have taken place and/or loss or theft of payment instrument such as card, etc. Bank will also enable customers to instantly respond by "Reply" to the SMS and e-mail alerts and the customers should not be required to search for a web page or an e-mail address to notify the objection, if any. Further, a direct link for lodging the complaints, with specific option to report unauthorized electronic transactions shall be provided by our bank on home page of our website soon. The loss/fraud reporting system shall also ensure that immediate response (including auto response) is sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by banks to send alerts and receive their responses thereto must record the time and date of delivery of the message and receipt of customer's response, if any, to them.

This shall be important in determining the extent of a customer's liability.

Our bank may not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. On receipt of report of an unauthorized transaction from the customer, banks must take immediate steps to prevent further unauthorized transactions in the account.

II). Limited Liability of a Customer

(a) Zero Liability of a Customer

A customer's entitlement to zero liability shall arise where the unauthorized transaction occurs in the following events:

(i) Contributory fraud/ negligence/deficiency on the part of the bank (irrespective of Whether or not the transaction is reported by the customer).

(ii) 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.

(b) Limited Liability of a Customer

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

(i) In cases where the loss is due to negligence by a customer, such as where he has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

(ii) 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 within four to seven working days of receiving a communication of the transaction, the per transaction liability of the customer shall be limited to the transaction value or the amount mentioned in Table 1, whichever is lower.

Table 1

Maximum Liability of a Customer—as per -II (b), above

Type of Account	Maximum liability (₹)
• BSBD Accounts	5,000
• All other SB accounts • Pre-paid Payment Instruments and Gift Cards • 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 • Credit cards with limit upto Rs. 5 lakh	10,000
• All other Current/Cash Credit/Overdraft Accounts	25,000

If the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy. Banks shall provide the details of their policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Banks shall also display their approved policy in public domain for wider dissemination. The existing customers must also be individually informed about the bank's policy.

Overall liability of the customer in third party breaches, as detailed in paragraph 6 (ii) and paragraph 7 (ii) above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised in the Table 2:

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 amount mentioned in Table 1, whichever is lower
Beyond 7 working days	As per bank's Board approved policy

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.

(C)Reversal Timeline for Zero Liability/Limited Liability of customer

On being notified by the customer, the bank shall credit (shadow reversal) the amount involved in the unauthorised 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 unauthorised transaction. Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence.

Further, banks shall ensure that:

(i) a complaint is resolved and liability of the customer, if any, established and the customer is compensated , within such time as may be specified in the bank's Board approved policy, but not exceeding 90 days from the date of receipt of the complaint;

(ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in Table-1&2 is paid immediately to the customer; and

(iii) in case of debit card/bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

D) Burden of Proof

The burden of proving customer liability in case of unauthorised electronic banking transactions shall lie on the bank.

E) Reporting and Monitoring Requirements

The banks shall put in place a suitable mechanism and structure for the reporting of cases of unauthorized electronic banking transactions to the Board or one of its Committees. The reporting shall, inter alia, include volume/number of cases and the aggregate value involved and distribution across various categories of cases viz., card present transactions, card not present transactions, internet banking, mobile banking, ATM transactions etc. The Board shall periodically review the unauthorised electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the 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.

Any doubts/clarifications /confusions aroused on the above document, the decisions taken by the Board of directors, are final and binding on the customers.

@@@@@@@@@@@@@@@@@@@@

PAYYANUR CO-OP. TOWN BANK LTD. NO.C.827 PAYYANUR

For The Payyanur Co-op. Town Bank
Ltd.No.C.827/UBD.KR 889 P (RBI)
Chief Executive Officer