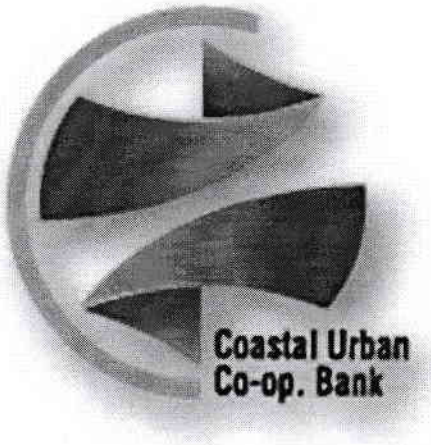

THE COASTAL URBAN CO-OPERATIVE BANK LTD. No. 3036, KOLLAM

CR No. 108 (6) Dated : 16.05.2025

Policy on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

1. Introduction

The Coastal Urban Co-operative Bank Ltd. No. 3036, Kollam is committed to provide customers with the best service possible so that the relationship with the customer is maintained and the Bank can provide various services via different electronic channels. With the increased usage of digital banking transactions and thrust on customer protection, there is a need for a framework to address customer grievances relating to unauthorised transactions, resulting in debit of their accounts maintained with the bank. This may cover transactions not initiated by them through different kinds of electronic modes viz., cards, E-COM, POS, Payment systems etc. This policy is framed in accordance with RBI Circular No. RBI/2017-18/109 DCBR.BPD(PCB/RCB). Cir.No. 06/12.05.001/2017-18 dated 14th December 2017 and covers various aspects of customer protection and criteria for determining the customer liability in such unauthorised electronic banking transactions reported by the customers and limiting the liability of the customers in such transactions. The Bank issues Rupay Debit Card to its customers.

2. Objective:

The objective of the policy is to ensure that the systems and procedures in bank are designed to make customers feel safe and protected and define customer liability while performing electronic banking transactions. This would involve having a robust and dynamic fraud detection and prevention mechanism, measures to mitigate risks and protect customers from liabilities arising out of fraudulent transactions and a system to educate customers in protecting themselves from frauds arising from electronic banking and payments.

3. Coverage:

This policy will cover the following transaction categories:

i) 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.) and

ii) 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) and UPI.

4. System and procedures for Safe Electronic banking:

Electronic banking transactions are performed securely with two-factor authentication like valid credentials like Card No., CVV, PIN, OTP. National Payments Corporation

of India provides Enterprise Fraud Risk Management tool for Rupay Network. Monitoring on real time basis is in available and various rules are implemented in Enterprise Fraud Risk Management to prevent frauds. Appropriate measures to mitigate the risks and protect the customers against liabilities arising therefrom is ensured by creating awareness through campaigns like displaying posters at branches, sending SMS, publishing on the Bank websites. The obligations of customers and the Bank in this regard shall be as under:

Obligations of the Bank:

a) Appropriate systems and procedures to ensure safety and security of electronic banking transactions.
b) Promptly attending to customer grievances.
c) Ensuring that customers register for SMS alerts and email alerts (wherever available)
d) Mandatorily send SMS for electronic banking transactions
e) Advise customers to immediately notify unauthorised electronic transactions.
f) Take immediate steps on being notified of unauthorised transaction and take steps to prevent further occurrences.

Obligations of the Customer:

a) Mandatorily register for SMS and Email (wherever available) alerts at time of availing any digital products including ATM debit card.
b) Mandatorily notify the Bank about any change of mobile number, email ID or address which is already registered with the Bank.
c) Customer should not disclose or share account details, card number, PIN, OTP, CVD with anyone.
d) Password for mobile banking and internet banking should be always kept confidential.
e) Customers must check transaction message and should immediately report any discrepancy to the Bank.
f) PIN and passwords should be changed at regular intervals.
g) Passbook / statement should be updated and verified from time to time.

5. Reporting of unauthorised Transactions by customers to Bank

The Bank shall act upon the unauthorised electronic banking transactions reported by the customers to the bank, based on the time of reporting, evidences and supporting documents submitted along with the complaints.

As per RBI guidelines, any transaction claimed as unauthorized debit must be reported by the customer to bank within 30 days to be eligible for compensation. The transactions which are not intimated to bank will be deemed as undisputed.

a) The Bank requires customers to notify the Bank about any unauthorised electronic banking transaction, immediately after the occurrence of such transaction, as longer the time taken to notify the bank, the higher will be the risk of loss to the bank/customer.

b) To enable reporting of unauthorised transactions by the customer, the Bank shall provide customers with 24x7 access through multiple channels (via Bank's official website, e-mail, reporting to home branch in person during working hours etc.). Immediate response (including auto response) will be sent to the customers acknowledging the complaint along with the registered complaint number.

c) It is Bank's endeavour to provide customers will be provided with various options to block his/her Debit card, in case of unauthorized transactions suspected. Currently such blocking facility is available to branches when customer reports in person and also for 24 hours for those customers who are having mobile banking facility.

d) On receipt of report of an unauthorized transaction from the customer, the Bank will take immediate steps to prevent further unauthorized transactions in the account/card by blocking the card or relevant channels.

e) Branches to clearly guide the customers on the risk involved in sharing the credentials which lead to fraudulent transactions by card cloning and data theft. However, the burden of proving the customer liability in case of unauthorized electronic transaction shall lie with the bank.

6. Liability of a Customer of Bank in unauthorized electronic Banking Transaction

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.

** (A glossary to important terminologies is provided in Annex -I)

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, clicked on a Link sent by strangers, and/or entered payment credentials, and/or installed screen sharing application, etc., 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 unauthorised 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 four to seven working days after receiving the communication from the bank) 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 the amount mentioned in Table 1, whichever is lower.

Table 1 - Maximum Liability of a customer applicable under Para 6 (b) ii	
Type of Account	Maximum liability Rs.
• BSBD Accounts	5,000
○ All other SB accounts ○ Current/ Cash Credit/ Overdraft Accounts of ○ Current Accounts/ Cash Credit/ Overdraft ○ Current Accounts/Cash Credit/Overdraft Accounts of individuals with annual average balance (during 365 days preceding the incidence of fraud) / limit upto Rs. 25.00 lakhs	10,000
○ All other Current / Cash Credit / Overdraft Accounts	25,000/-

(iii) Further, if the delay in reporting is beyond seventh working day, the customer liability shall be determined as under:

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. However, depending on case-to-case basis, Bank may compensate customer an amount maximum up to Rs. 10,000/- (Rupees Ten Thousand only) (if reported within 30 days) irrespective of the fact whether there is single or multiple number of transactions or transaction amount whichever is lower and the customer shall be entitled for such compensation only once in the customer's life time.

c) Overall liability of the customer in third party breaches, as detailed in para 6 (a) (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 g)
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 and within 30 days	Unlimited. (Bank may compensate a sum not exceeding Rs. 10,000/- (Rupees Ten thousand only)

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.

7. 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). Customer Service Cell at Head Office shall pass such accounting entries. Bank may also at its discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorised transaction.

8. Further, the bank shall ensure that:

i) A complaint is resolved and liability of the customer, if any, established within a period of 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraphs 5 and 6 above.

ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 5 and 6 above is paid to the customer; and

iii) in case of debit card/bank account, the customer does not suffer loss of interest

iv) a customer shall be eligible for compensation from the bank only once during the period of his/her banking relationship with the Bank.

For all disputed cases, customer shall be required to lodge a written complaint in his/her home branch or send email to bank from email address registered with the bank, along with supporting documents namely dispute form, copy of the police complaint duly acknowledged by the Police Department (copy of FIR or online Cybercrime complaint mandatory for claims of Rs. 50,000/- and above. For amount less than Rs. 50,000/-, complaint letter acknowledged by Police to be submitted) and other available evidence, within thirty calendar days, from the date of giving first intimation of the fraud by him/her to the Bank.

In case the customer is unable to provide the documents or there is a delay on part of the customer in submitting the documents within the aforesaid thirty days, the Bank shall term such disputes as unable to conclude and the liability of the unauthorized transactions in such cases will remain with the customer only,

Cash withdrawal from non-EMV compliant ATM Machine:

In case cash withdrawal is made from non-EMV compliant ATM Machine, and the transaction is reported as unauthorized by the card holder, bank will shift the liability on the Acquirer Bank by raising chargeback under EMV Liability Shift as per RBI guidelines.

9. Approving Powers:

As a measure of the Bank's commitment to speedy customer service, the customer will be compensated to the extent of amount as mentioned below where unauthorized electronic banking debits have taken place in the customer's account, after getting necessary approval from the Chief Executive Officer, by passing a debit to "Reimbursement for Electronic Banking Transactions — REBT A/c":

The power to write off the entries outstanding in the REBT A/c identified as not recoverable are vested with the Board of Directors.

10. Communication of the Policy:

The Bank shall provide this policy at the branch premises and also display it public domain through Bank's official website for wider dissemination.

11. Reporting and Monitoring Mechanism:

Customer liability cases shall be periodically submitted and reviewed to the Customer Service Committee on a quarterly basis. The reporting shall include the number of cases and the aggregate value involved and distribution across categories viz., card present transactions, card not present, mobile banking, ATM transactions, etc.

The Customer Service Committee shall periodically review the unauthorized electronic banking transactions reported by customers 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 concurrent auditors/statutory auditor also. Concurrent auditors will review such cases settled under this policy during their regular audit of the bank and their report shall include details of any deviation from the directives stipulated in the policy.

12. Review of Policy:

The policy shall be reviewed on an annual basis or any time in case of any change in regulatory instructions.

Annexure I

Terminology	Explanation
Unauthorised Electronic Banking Transaction	A financial or nonfinancial transaction taking place in the Bank account of a customer, through any type of electronic mode of payment, that was not done by the customer or done without the customer's knowledge or authorization.
Contributory Fraud	Involvement of Bank staff in wrongful or original deception, intended to result in financial or personal gain
Negligence	Means one or combination of more than one of the following: lack of proper care and attention, dereliction of duty, non-performance or non-fulfilment of duty, acts of laxity, irresponsibility, inattention, inattentiveness, thoughtless-ness etc.
Third Party Breach	Third party breach means where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system.
Payment Credentials	Payment credentials are confidential information like ATM PIN, CVV, OTP, UPI PIN etc., required for effecting payment through electronic mode, which are unique and exclusively in possession of the customer
Acquirer Bank	Bank whose terminal is used for processing transactions initiated by Bank card holder.

For The Coastal Urban Co-operative Bank Ltd. No:3036,Kollam

Managing Director

Managing Director

Director

For The Coastal Urban Co-operative Bank Ltd. No:3036,Kollam

Director

For The Coastal Urban Co-operative Bank Ltd. No:3036,Kollam

Chairman

Director

For The Coastal Urban Co-operative Bank Ltd.No.3036,Kollam

Director