City Union Bank Ltd

Customer Protection Policy for Unauthorized Electronic Banking Transactions

CUB/ISMS/Policy/005

(Version 1.6)

Document History

Document Management Information	
Document Title	Customer Protection Policy for Unauthorized Electronic Banking Transactions
Document Status	Final
Document number	CUB/ISMS/Policy/005

Document Review History

Version	Date	Remarks
1.0	08-Nov-2017	Initial version
1.1	22-Jun-2018	Annual Review – No changes
1.2	22-Nov-2019	Annual Review – No changes
1.3	13-Jul-2020	Annual Review – No changes
1.4	20-Sep-2021	Annual Review – No changes
1.5	15-Dec-2021	Annual Review – No changes
1.6	23-Dec-2022	Addition of New clauses
1.6	23-Mar-2025	Annual Review – No changes

Approval details

Version	Board Approval Date	Remarks
1.6	26-Mar-2025	Approved by the Board

Index

Content	Page No
Introduction	4
Purpose	4
Applicability, Definitions & Explanations	5
Robust Systems and Procedures	5
Reporting of unauthorized transactions by customers to banks	6
Limited Liability of a Customer	
(a) Zero Liability of a Customer	7
(b) Limited liability of a Customer	7
Summary of Customers' liability	8
Reversal Timeline for Zero Liability/ Limited Liability of customer	9
Reporting and Monitoring Requirements inside the Bank	9
Grievance Redressal escalation for customers	9
Escalation Matrix	10

Introduction

Use of Information Technology in our Bank has grown rapidly and is now an integral part of the operational strategy of the bank. The technology initiatives of our Bank are focusing on customer convenience and self service devices/ applications so that customers can transact at any time anywhere.

The usage of digital channels by customers is increasing consistently. On the other hand, the number, frequency and impact of cyber incidents / attacks have increased manifold in the recent past. Hence it is the bounden duty of the Bank to create a conducive environment to the customers to have safe and secured electronic transactions. The ignorant and less knowledgeable customers should not be exploited by cyber criminals. To create awareness, we have been educating our customers about the best practices to be followed through e-mails, SMS messages, and website information and through social and print media. In the event of customers losing money in the course of doing electronic transactions, their liability will be decided based on the nature of transactions and adequately compensated if required.

Purpose

We already had formulated customer compensation policy to compensate our customers for any financial loss he / she might incur due to deficiency in service on the part of the bank or any act of omission or commission directly attributable to the bank.

With the increased thrust on financial inclusion and customer protection 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 have been reviewed by Reserve Bank of India and RBI issued guidelines to Banks. Accordingly Our bank's Customer Protection Policy on limiting customer liability in unauthorised electronic transactions and compensation payable to customers has been formulated.

Taking into account the risks arising out of unauthorised debits to customer accounts owing to customer negligence / bank negligence / banking system frauds / third party breaches, we need to define the rights and obligations of customers in case of unauthorised transactions in specified scenarios. The revised policy covers the aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorised electronic banking transactions. The policy enumerates the mechanism of compensating the customers for the unauthorised electronic banking transactions and also prescribe the timelines for effecting such compensation keeping in view the instructions contained in the Reserve Bank of India Circular on Customer Protection. The policy shall be displayed in our website along with the details of grievance handling / escalation procedure on approval by the board.

Applicability, Definitions & Explanations (applicable for this policy)

This policy is applicable to those having relationship with bank viz.,

i) individuals / entities who hold Savings account / Current account and/or OD account
ii) individuals / entities who hold Debit / Credit and/or Prepaid Card
iii) individuals / entities who use Banks electronic platforms like Internet Banking / Mobile Banking / PPIs including wallet

Unauthorized debit – Unauthorized debit means debit in customers account without customers consent

Consent – Consent means to include authorisation of debit tansaction either through standing instructions, as per accepted banking practice and regulations, based on account opening process and related matters or based on additional authentication required by the bank such as user of security password, input of dynamic password (OTP), Challenge questions or use of card debilts (CVV/Expiry Date/PIN) or any other authentication option provide by the bank.

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

Third Party Breach – The following would be considered as Third party breach

i) Identity Theft
ii) Skimming / cloning
iii) External frauds / compromise of other system like ATM compromise, POS (or) e-Commerce transaction acquirer compromise

Robust 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 a card or mobile phone to be present at the point of transaction e.g. ATM, POS, etc.)

(iii) Any other electronic mode of payment effected from one entity to another entity 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 the customer (example 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 damages.

The systems and procedures in our Bank are designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, bank has 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 resulting from unauthorised 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.

These measures are continuously reviewed and improved.

Reporting of unauthorised transactions by customers to banks

For doing electronic transactions, customers are requested to mandatorily register for SMS alerts and wherever available register for e-mail alerts. The SMS alerts and email alerts shall mandatorily be sent to the customers, wherever registered. The customers are advised to notify the bank of any unauthorised 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, Bank has provided customers with 24x7 accesses through the following channels

1. Customer care @ 044-71225000
2. Internet Banking
3. Mobile Banking
4. Customer Grievances portal in Bank's corporate website
5. Branches.

for reporting unauthorised transactions that have taken place and / or loss or theft of payment instrument such as card, etc.

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 unauthorised transaction from the customer, bank will immediately hotlist the card / stop the transactions in the account to prevent further unauthorised transactions.

Limited Liability of a Customer

(a) Zero Liability of a Customer

A customer's entitlement to zero liability shall arise where the unauthorised 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 (through SMS alert/email alert/push notification or any other mode) regarding the unauthorised transaction.

(b) Limited Liability of a Customer

A customer shall be liable for the loss occurring due to unauthorised 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 unauthorised transaction to the bank. Any loss occurring after the reporting of the unauthorised 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

Type of account	**Maximum liability of customer (Rs)**
• 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 up to Rs.5 lakh	10,000
• All other Current / Cash Credit / Overdraft Accounts • Credit cards with limit above Rs.5 lakh	25,000

Further, if the delay in reporting is beyond **seven working days**, the per transaction liability of the customer shall be the transaction value as mentioned in Table 2.

Table 2

Type of Customer	**Liability of customer (Rs)**
• BSBD Accounts	Transaction value
• 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 up to Rs.5 lakh	Transaction value
• All other Current/ Cash Credit/ Overdraft Accounts • Credit cards with limit above Rs.5 lakh	Transaction value

Overall liability of the customer in third party breaches, as detailed above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarised as follows

Summary of Customers' liability

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	The transaction value as mentioned in Table 2.

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.

Proof of customer liability: Bank has a process of second factor authentication for electronic transactions, as regulated by the Reserve Bank of India. Bank has onus to prove that all logs / proofs / reports for confirming two factor authentication are available. Any unauthorized electronic banking transaction which has been proceed post second factor authentication known only to the customer would be considered as sufficient proof of customer's involvement / consent in effecting the transaction.

Reversal Timeline for Zero Liability/ Limited Liability of customer

On being notified by the customer, the bank shall shadow credit (reversal by marking 'Hold') 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 for all the cases where customers liability is Zero (or) customer liability is Limited. The credit shall be value dated to be as of the date of the unauthorised transaction.

Further, bank shall ensure that:

(i) a complaint is resolved and liability of the customer is established within 90 days from the date of receipt of the complaint, and the customer is compensated as specified above.

(ii) In case Bank is unable to resolve the complaint or determine the customer liability within 90 days of reporting date, then the Bank shall credit the customer with compensation as prescribed in this policy. Customer will be given value dated credit.
   a) in case of debit card/ bank account, the customer shall not suffer loss of interest
   b) in case of credit card, the customer shall not bear any additional burden of interest

(iii) Customer would not be entitled to compensation of loss if any, in case customer does not agree to get the card blocked, net/mobile banking blocked, enable block on his/her account or does not co-operate with the Bank by providing necessary documents including but not limited to copy of police complaint and cardholder dispute form complete in all respect

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

Reporting and Monitoring Requirements inside the Bank.

The 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 will be placed to Standing Committee of Customer Service. The Standing Committee on Customer Service shall periodically review the unauthorised electronic banking transactions reported by customers, the action taken thereon, the functioning of the grievance redress mechanism and take appropriate measures to improve the systems and procedures. All such transactions shall be reviewed by the bank's internal auditors.

Grievance Redressal escalation for customers

The credits for unauthorised electronic banking transactions will be effected within 10 days from the date of informing the bank. If any dispute is there to identify whether it is the fault of bank or customer or third party, it will be resolved within 90 days.

Escalation Matrix

The escalation matrix for dispute resolution / complaint redressal is

I level – Customer Care Centre – 149, TSR Big street, Kumbakonam – 044-71225000. customercare@cityunionbank.in

II level – Deputy General Manager – Computer Systems Department , 706 Anna salai, Chennai – 044- 28297905.

III level – General Manager - Computer Systems Department , 706 Anna salai, Chennai – 044- 28297905.

IV Level – Principal Officer for Complaints and Redressal – Senior General Manager (Inspection and Audit) - Tel : 0435-2402322