

Customer Protection Policy (Unauthorised Electronic Banking Transactions)

Capital Small Finance Bank Ltd. is committed to provide superior and safe customer service experience to all its customers. Taking into account the risks that arise out of unauthorized debits to customer accounts owing to customer negligence/ bank negligence/ banking system frauds/ third party breaches, it is very important to ensure that the systems and procedures followed in the bank must be designed in way that the customer feel safe about carrying out electronic banking transactions.

Keeping in mind the increasing thrust on financial inclusion & customer protection, the Reserve Bank of India had issued a circular on Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. (RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017) which requires Banks to formulate a Board approved policy in regard to customer protection and compensation in case of unauthorized electronic banking transactions

1. Objective:

This policy seeks to communicate in a fair and transparent manner the Bank's policy on:

- Customer protection (including mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions);
- Customer liability in cases of unauthorized electronic banking transactions;
- Customer compensation due to unauthorized electronic banking transactions (within defined time-lines).

2. Categorization of Electronic banking transactions:

The electronic banking transactions can be broadly divided into two categories:

2.1 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

2.2 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.

3. Applicability:

This policy is only applicable to the entities which hold a relationship with the bank i.e. Individual and non-individual customers who hold current or savings account, ATM/Debit Card, or uses other electronic platforms of the Bank like internet banking. The policy shall not be applicable to the Non-Customers that uses the Bank's infrastructure e.g. ATMs etc.

4. Liability of the Customer:

Customer shall be compensated in line with this policy in case of loss occurring due to unauthorized transaction as follows:

4.1 Zero Liability of a Customer:

- 4.1.1** Customer shall be entitled to full compensation of real loss in the event of contributory fraud/ negligence/ deficiency on the part of the bank (irrespective of whether or not the transaction is reported by the customer).
- 4.1.2** 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 unauthorised transaction.

4.2 Limited Liability of customer:

- 4.2.1** 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.
- 4.2.2** 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** there is a delay on the part of customer in notifying/reporting to the Bank beyond 3 working days and less than or equal to 7 working days (after receiving the intimation from the Bank), the liability of the customer per transaction shall be limited to transaction value or amounts mentioned in **Annexure -1** whichever is lower.

4.3 Complete Liability of customer:

- 4.3.1** 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 the payment credentials or Account/Transaction details, viz. Internet Banking user Id & PIN, Debit Card PIN/OTP or due to improper protection on customer devices like laptop/desktop leading to malware/Trojan or Phishing attack.

Under such situations, the customer will bear the entire loss until the customer reports unauthorised transaction to the bank. Any loss occurring after reporting of unauthorised transaction shall be borne by the bank.

- 4.3.2** In cases where the responsibility for 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 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.

5. Reversal Time line for Zero Liability/ Limited Liability of customer

- 5.1** The bank shall credit (shadow reversal) 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.

- 5.2 Within 90 days of the date of reporting, the Bank shall either establish customer negligence or provide final credit to the customer. A value dated credit (based on date of unauthorized transaction) or credit along-with the Savings Bank interest shall be given to the customer, in case, the customer becomes eligible to be compensated. In case of debit card/ bank account, the customer shall not suffer loss of interest.
- 5.3 The Bank may, at its discretion, agree to credit the customer even in case of an established negligence by the customer.
- 5.4 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, as requested, including the police complaint etc.
- 5.5 Compensation would be limited to the real loss after deduction of reversals or recoveries received by the customer.

6. Responsibilities of the Bank:

- 6.1 The Bank shall ensure that the Customer protection policy is available on the Bank's website as well as at Bank's branches for the reference of the customers. The Bank shall also ensure that existing customers are individually informed about the bank's policy.
- 6.2 The Bank will regularly conduct awareness on carrying out safe electronic banking transactions to its customers and its staff. Such information will include rights and obligation of the customers as well as non-disclosure of sensitive information e.g. password, PIN, OTP, date of birth, etc.
- 6.3 The Bank shall communicate to its customers to mandatorily register for SMS alerts. The Bank will send SMS alerts to all valid registered mobile number for all debit electronic banking transactions. The Bank may also send alert by email where email Id has been registered with the Bank.
- 6.4 For reporting of unauthorized transactions, the customers may refer to the "Customer Grievance Redressal Policy" of the bank.
- 6.5 The Bank shall respond to customer's notification of unauthorized electronic banking transaction with acknowledgment specifying the date and time of receipt of customer's notification.
- 6.6 On receipt of customer's notification, the Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the account.
- 6.7 The Bank shall ensure that all such complaints are resolved and liability of customer if any, established within a maximum of 90 days from the date of receipt of complaint, failing which, bank would pay compensation.

7. Obligations of the Customer:

- 7.1** Customer shall mandatorily register valid mobile number with the Bank where he/she will get an alert for all financial electronic debit transactions.
- 7.2** Customer shall regularly update his/her registered contact details as soon as such details are changed. Any failure of 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.
- 7.3** Customer should co-operate with the Bank's investigating authorities and provide all the necessary documentation i.e. proof of transaction success/ failure etc. and should also file a police complaint and provide copy of the same to the Bank.
- 7.4** Customer must not share sensitive information (such as Debit Card details & PIN, CVV, Net-Banking Id & password, OTP etc.) with anyone, including bank staff.
- 7.5** Customer must protect his/her device (Laptop/Desktop etc.) as per the best practices, including updation of latest anti-virus software on the device.
- 7.6** Customer shall go through various instructions and awareness communication sent by the bank on secured banking i.e. through SMS etc.
- 7.7** Customer must verify transaction details from time to time in his/her bank statement and raise query with the bank as soon as possible in case of any mismatch.

Annexure -1

Maximum Liability of a Customer in case of unauthorized Electronic Transaction where Responsibility is neither with the Bank nor with the customer but lies elsewhere in the system & customer has reported unauthorized transaction from transaction date within the working days as specified:

Type of Account	Within 3 working days (Rs.)	Within 4 to 7 working days (Rs.)
BSBD Accounts	Zero Liability	5000
All other SB accounts		10000
Pre-paid Payment Instruments and Gift Cards		10000
Current/ Cash Credit/ Overdraft Accounts of MSMEs		10000
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		10000
All other Current/ Cash Credit/ Overdraft Accounts		25000