CTBC BANK
中國信託銀行

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

The electronic banking transactions offered by the Bank primarily to its Corporate customers for processing RTGS, NEFT, Internal Transfers are governed by the following terms and conditions:

(i) The Customer shall notify the Bank of persons authorized by it to give, modify or approve Instructions or Transactions by way of completing and delivering applicable application forms from time to time prescribed by the Bank. In case of any change in the authorization given to such Authorized Persons, the Customer shall promptly notify the Bank of the same in writing pursuant to applicable application forms from time to time prescribed by the Bank unless otherwise provided for in paragraph (ii) or (iii) below. If the Customer fails to timely notify the Bank of the aforesaid change, any loss or damage arising from such failure shall be only for the account of the Customer

(ii) The Customer may, by way of completing and delivering applicable application forms from time to time prescribed by the Bank, apply to the Bank to set and change the Authorized Persons, where the Bank will grant a log-in password to the person designated by the Customer in its application ("Authorized Administrator") so that the Authorized Administrator may set and change the Authorized Persons by himself/herself on the Bank's Internet banking website. The Bank shall be deemed notified of the change to the Authorized Persons when the Authorized Administrator completes such changes on the Bank's Internet banking website, and the Bank may act accordingly and will have no liabilities or responsibilities in connection therewith. The Customer shall properly keep and shall cause the Authorized Administrator to properly keep the aforesaid log-in password

(iii) The Customer may, by way of completing and delivering applicable application forms from time to time prescribed by the Bank, apply to the Bank to (a) set and change the authorizations given to the Authorized Persons and (b) set and change the Authorized Persons by itself on the Bank's Internet banking website, where the Bank will deliver a log-in password and Token to the Authorized Administrator so that the Authorized Administrator may act by himself/herself on the Bank's Internet banking website as aforesaid. The Bank shall be deemed notified of the change to the Authorized Persons when the Authorized Administrator completes such changes on the Bank's Internet banking website, and the Bank may act accordingly and will have no liabilities or responsibilities in connection therewith. The Customer shall properly keep and shall cause the Authorized Administrator to properly keep the aforesaid log-in password and Token.

In terms of RBI Notification No. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6th July 2017 (copy enclosed), banks are required to clearly define the rights and obligations of customers in case of unauthorised transactions in specified scenarios of electronic banking transactions. This policy is being framed to stipulate the mechanism of compensating the customers for the unauthorised electronic banking transactions and also prescribe the timelines for effecting such compensation.

Limited Liability of a Customer

(a) Zero Liability of a Customer - 1. 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 regarding the unauthorised transaction.*

(b) Limited Liability of a Customer- 2. 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
Maximum Liability of a Customer under paragraph (b) above:

Type of Account	Maximum liability (₹)
• Current, Cash Credit, Overdraft Accounts of MSMEs/ Savings, 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 Savings, Current, Cash Credit, Overdraft Accounts	25,000

Further, if the delay in reporting is beyond seven working days and in case of third party breaches as detailed in paragraph (a) ii and (b) ii, 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	50% of the transaction value or the amount mentioned in Table 1, whichever is lower

*Working days mentioned in the above table will be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

Reversal Timeline for Zero Liability/ Limited Liability of customer

On being notified by the customer, the Bank will 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. The 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.

RBI Notification No. RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6th July 2017

Notifications

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

July 6, 2017

All Scheduled Commercial Banks (including RRBs)
All Small Finance Banks and Payments Banks

Dear Sir/ Madam,

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

Please refer to our circular DBOD.Leg.BC.86/09.07.007/2001-02 dated April 8, 2002 regarding reversal of erroneous debits arising from fraudulent or other transactions.

2. 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. The revised directions in this regard are set out below.

Strengthening of systems and procedures

3. 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.)

4. The systems and procedures in banks must be designed to make customers feel safe about carrying out electronic banking transactions. To achieve this, banks 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 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 therefrom; and
v. a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

Reporting of unauthorised transactions by customers to banks

5. Banks must ask their 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 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, banks 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 unauthorised transactions that have taken place and/ or loss or theft of payment instrument such as card, etc. Banks shall 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 unauthorised electronic transactions shall be provided by banks on home page of their website. 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. The banks 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, banks must take immediate steps to prevent further unauthorised transactions in the account.

Limited Liability of a Customer

(a) Zero Liability of a Customer

6. 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 regarding the unauthorised transaction.

(b) Limited Liability of a Customer

7. 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
Maximum Liability of a Customer under paragraph 7 (ii)

Type of Account	Maximum liability (₹)
• BSBD Accounts • All other SB accounts • Pre-paid Payment Instruments and Gift Cards • Current/ Cash Credit/ Overdraft Accounts of MSMEs	5,000
• 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 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.

8. 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