CUSTOMER RELATION / CUSTOMER PROTECTION/ CUSTOMER LIABILITY POLICY 2020

OPERATIONS DEPARTMENT

Central Office

Karur

CUSTOMER RELATION /CUSTOMER PROTECTION/ CUSTOMER LIABILITY POLICY

Preamble:

The phenomenal innovations in technology based products/services have lead to sizable increase in electronic banking transactions. It will be the Bank's endeavor to update the technology as per the market trend and offer services to its customers with best possible utilization of its technology infrastructure and at the same time enable a safe and secure environment to enable them to carry out their transactions with ease and confidence. However, there is an ever present hazard of e-frauds inspite of continuous safety measures being taken by Bank at various levels. Hence, there is a need to clearly define the rights and obligations of the Bank and the customers in case of loss resulting from unauthorized transactions in specified scenarios. Hence this policy.

This policy is a mandate for the bank to stipulate the mechanism of compensating the customers for the unauthorized electronic banking transactions in different scenarios and also to prescribe the timeline for effecting such compensations.

***

CHAPTER-1

Categories of electronic Banking transactions:

The electronic banking transactions can be divided as two categories namely:

1) Card present (CP) transactions: The 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.

2) Card not present (CNP) transactions: The transactions which does not require the physical payment instrument at the point of transaction,e.g., online purchases, etc.

Specified scenarios of unauthorized electronic banking transactions:

1) Delayed alerting of customers for the channel transactions (ATM/BNA/POS/Internet Banking/Mobile banking/Debit cards/Prepaid Cards/Credit Cards etc.).

2) Sharing of payment credentials (PIN/Password/CVV) by customer to known/unknown persons, online sites, etc.

3) Security breach in the systems of the bank & or its terminals and the bank's third party vendors/service providers who manages the transactions.

Reporting of unauthorized transactions by customers to banks:

1) Bank must ask the customers to mandatorily register for SMS alerts and wherever available, register for e-mail alerts for electronic banking transactions.

2) The SMS alerts shall mandatorily be sent to the customers, while email alerts may be sent, wherever registered.

3) The customers shall be advised to notify the 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 customer/ bank.

4) Bank shall include suitable information in the Account opening forms, Welcome Kit/Instant kit letters etc. given to the customer, to bring to their knowledge the terms and conditions of Bank's policy with respect to customer's liability for unauthorized electronic banking transactions.

5) Bank shall provide customers with 24x7access 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.

6) 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.

7) 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.

8) 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.

9) On receipt of report of an unauthorized transaction from the customer, Bank shall take immediate steps to prevent further unauthorized transactions in the account.

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

11) The Bank shall not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the Bank.

***

CHAPTER-2

Liability of a customer:

As mandated by RBI, the liability of a customer for the unauthorized electronic banking transactions is limited as follows:

I. (a) Zero liability of a customer:

The customer is entitled to ZERO liability where the unauthorized transaction occurs in the following cases:

1) Contributory fraud / negligence / deficiency on the part of the Bank. (Irrespective of whether or not the transaction is reported by the customer).

2) 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:

Limited liability of a customer shall arise for the loss occurring due to unauthorized transactions in the following cases where:

1) The loss is due to negligence by a customer, such as where he/she has shared the payment credentials to unknown person, the customer will bear the entire loss until he/she reports the unauthorized transaction to the Bank. Any loss occurring after the reporting of the unauthorized transaction shall be borne by the Bank.

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 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.

3) Bank shall provide the details of the policy in regard to customer's liability at the time of opening the accounts. Bank shall also display the approved policy in website and the existing customers must also be individually informed about the bank's policy.

4) Overall liability of the customer in third party breaches as detailed in paragraph (a) 1&2 and paragraph (b) 1&2 above, where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized in the Table 2:

Table 1

Maximum Liability of a Customer as per the mandate

Type of Account	Maximum liability (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	25000/-

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.

***

CHAPTER-3

Bank's discretion for customer compensation for unauthorized transactions reported beyond the mandated timelines:

I. 1. In case 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 beyond **seven working days but within 30 days** after receiving the communication from the bank regarding the unauthorized transaction, Bank shall compensate the customer with 10% of the total disputed transaction value (aggregate value of all unauthorized transactions) or the amount mentioned in Table 1, whichever is lower. The customer has the right to claim the unauthorized amount as per the scenarios detailed under the paragraph of "liability of customers".

2. In all other cases, Bank shall not compensate the customer for the loss arising out of unauthorized electronic banking transactions.

3. If any claims are made on unauthorized transactions reported beyond thirty working days by the customers and if the unauthorized transactions happened without negligence of the customer, then the bank may at its sole discretion, compensate the customer for 10% of the total disputed transaction value on case to case basis, taking into account the circumstances. This discretion shall be exercised by the President & COO of the Bank.

4. Bank shall take appropriate insurance coverage to offset the loss arising out of payment of compensation to customers for the unauthorized electronic banking transactions.

II. **Force majeure**: The bank shall not be liable to compensate customers for delayed credit if some unforeseen event (including but not limited to civil commotion, sabotage, lockout, strike or other labor disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents it from performing its obligations within the specified service delivery parameters.

III. Timeline to pass on the credit for Zero liability/Limited liability of customer:

Bank shall credit (shadow reversal/by marking 'Hold funds') 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 (without waiting for settlement of insurance claim, if any). The Shadow credit may be given after obtaining an Indemnity from the customer. The credit shall be value dated to be as of the date of the unauthorized transaction.

Further Bank shall compensate the customer:

i) A compliant is resolved and liability of the customer, if any, established within such time but not exceeding 90 days from the date of receipt of the complaint, the customer is compensated as per provisions of paragraph **I**. a.(1) & (2) paragraph **I**. b (1) & (2) above.

ii) In case of debit card/bank account, if the complaint is unable to be resolved within 90 days, the compensation has to be paid to the customer with the interest as applicable for the type of account.

iii) In case of credit card, if the complaint is unable to resolve within 90 days, the compensation has to be paid to the customer without any additional burden on interest.

CHAPTER-4

Reporting and Monitoring:

1) The customer liability cases have to be reported to Customer Service and Stake Holders relationship Committee of the Board on a half yearly basis. The report should include the number of cases with distribution of card present card not present cases, mobile banking, internet banking etc. and aggregate value involved.

2) The Standing Committee on Customer Service shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise, as also the action taken thereon, the functioning of the grievances redress mechanism and take appropriate measures to improve systems and procedures.

3) All such transactions shall be reviewed by the bank's internal auditors.

4) The amount compensated to the customers is to be reported as operational loss to the Bank by providing details to Risk Management Department.

5) Root cause analysis of the transaction and compromise point is to be undertaken and wherever necessary the same should be taken up with respective Banks/ Service providers.

6) 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.

Review of Policy:

(i) The policy will be reviewed once in 3 years and will be placed before the Board for approval.

***