



## **Customer Protection Policy - Limiting Liability of Customers in Unauthorised Electronic Banking Transaction**

### **1. Introduction**

Bandhan Bank is committed to provide world class banking experience to all its customers through superior systems and technology.

With the increased thrust on financial inclusion and customer protection and considering the recent surge in customer grievances relating to un-authorized electronic transactions causing debits to customer accounts/ cards, various aspects of customer protection and criteria for determining the customer liability have been reviewed by RBI and directions issued in this regard vide their circular bearing reference: DBR.No.Leg.BC.78/09.07.005/2017-18 dated 6th July 2017.

In line with the regulatory directives this policy has been formulated to cover the following aspects:

- a) Customers' liability in cases of unauthorized electronic banking transactions.
- b) Mechanism of compensating the customers for unauthorized transaction due to unauthorized electronic banking transactions and the timelines for effecting such compensation.
- c) Customer protection including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions.

### **2. Types of electronic banking transactions:**

Electronic banking transactions can be broadly 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.)

### **3. Bank's commitment to ensuring customer protection:**

The Bank is committed to ensuring safety and security of electronic banking transactions carried out by customers. The Bank will put in place the following:

- (i) appropriate systems and procedures to ensure safe and secure of electronic banking transactions
- (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 unauthorized transactions and measure the liabilities arising out of such events;
- (iv) appropriate measures to mitigate the risks;
- (v) a system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.

### **4. Reporting of unauthorised transactions by customers to Bank**

The Bank will ensure that customers are mandatorily registered for SMS alerts and wherever available for email alerts, for electronic banking transactions. Bank will mandatorily send SMS alerts to the customers, while the email alerts may be sent wherever registered. Further, the bank will not be able to offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank. These facilities will be withdrawn for customers after due notice is provided to them.

The Bank requires customers to notify the Bank about any unauthorised electronic banking transaction at the earliest 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. To enable this to be done in a smooth and efficient manner, the Bank will provide customers with 24x7 access through multiple channels (via website, SMS, e-mail, 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.

Further, the Bank will provide a direct link for lodging the complaints, with specific option to report unauthorised electronic transactions in the home page of the Bank's website. Immediate response (including auto response) will be sent to the customers acknowledging the complaint along with the registered complaint number. The communication systems used by the Bank to send alerts and receive their responses thereto will record the time and date of delivery of the message and receipt of customer's response, if any, to the Bank.

On receipt of report of an unauthorised transaction from the customer, the Bank will take immediate steps to prevent further unauthorised transactions in the account. On being notified by the customer, the Bank will undertake a preliminary investigation to establish the reason for the dispute. Where the transaction does

not involve a third party, the Bank will endeavor to complete the investigation within 10 working days of notification.

## 5. 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 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, the customer will bear the entire loss until he reports the unauthorised transaction to the bank. Transactions where a Password / PIN / OTP (One Time Password) has been used or where the transaction has been performed with information available only with the customer or can be done only with the knowledge of the customer will be treated as 'transaction performed due to customer negligence'. Any loss occurring after the reporting of the unauthorised transaction will 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 2.b.(ii)**

| <b>Type of Account</b>                 | <b>Maximum Liability (Rs)</b> |
|--|-------------------------------|
| <input type="checkbox"/> BSBD Accounts | 5,000.00                      |

|  |           |
|--|-----------|
| <input type="checkbox"/> All other SB accounts<br><input type="checkbox"/> Pre-paid Payment Instruments and Gift Cards<br><input type="checkbox"/> Current/ Cash Credit/ Overdraft Accounts of MSMEs<br><input type="checkbox"/> Current Accounts/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limit up to up to Rs.25 lakh<br><input type="checkbox"/> Credit cards with limit up to Rs.5 lakh | 10,000.00 |
| <ul style="list-style-type: none"> <li>• All other Current/Cash Credit/ Overdraft Accounts</li> <li>• Credit cards with limit above Rs.5 lakh</li> </ul>   | 25,000.00 |

(iii) **If the delay in reporting by the customer is beyond seven working days, the customer shall be liable for the entire value of the transaction(s) involved.**

The number of working days will be counted as per the working schedule of the home branch of the customer excluding the date of receiving the communication.

The summary of the customer's liability is provided in Table 2 for ease of reference.

**Table 2**

**Summary of Customer's liability**

| <b>Time taken to report the fraudulent Customer's liability Transaction from the date of receiving the communication</b> | <b>Rs.</b>  |
|--|---|
| Within 3 working days  | Zero liability  |
| Within 4 to 7 working days   | The transaction value or the amount mentioned in Table 1 of the Policy whichever is lower |
| Beyond 7 working days  | Full liability of the customer i.e. to the extent of value of the transaction(s)          |

**6. Communication of the policy:**

The Bank will provide the details of policy with regard to customers' liability at the time of opening the accounts. The Bank will display the approved policy in bank's website. The existing customers would also be informed about the Bank's policy through publication on the website and where possible, through SMS and email alerts.

## **7. Reversal Timeline for Zero Liability/ Limited Liability of customer**

On being notified by the customer, the Bank will credit 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 credit will be value dated to be as of the date of the unauthorized transaction. The credit will be provided as a shadow credit, which means that the customer will not be able to use the funds credited by way of temporary/shadow credit till the dispute is resolved in favour of the customer.

Further, the Bank will ensure that:

- i. a complaint is resolved and liability of the customer, if any, established within a period not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of paragraph no 5 above
- ii. where Bank is unable to resolve the complaint, or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraph no 4 above will be paid to the customer; and
- iii. in case of debit card/ bank account, the customer does not suffer loss of interest.

For all disputed cases, customers shall be required to provide all relevant information and supporting documents as required by the Bank for investigation or Insurance claim. The customer shall also have to fully cooperate and comply with the Bank's reasonable requirement towards investigations and legal actions initiated by it in regards to the disputed transactions.

In case the customer is unable to provide the necessary documents or there is a delay on part of the customer in submitting the documents within the stipulated timeframe, post due follow up by the Bank, 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.

## **8. Proof of customer liability:**

The 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 is available. Any unauthorized electronic banking transaction which has been processed post second factor authentication known only to the customer would be considered as sufficient proof of customer's involvement / consent in effecting the transaction.

## **9. 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 labour 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.

## **10. Reporting and Monitoring Mechanism**

Customer liability cases shall be periodically reviewed in the Customer Service Committee of the Board on a quarterly basis. The reporting shall, *inter alia*, include 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.

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 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/statutory auditor also.

## **11. Linkage to other Customer Service Policies of the Bank:**

This Policy shall be read in conjunction with the Customer Compensation policy and Customer Grievance Redressal policy.

## **12. Review of policy:**

The policy has been approved by the Board of the Bank and is reviewed at regular intervals by the Customer Service Committee of the Board.

These reviews shall consider the following:

- ✓ Internal factors such as changes in organisational structure or products and services offered
- ✓ External factors such as changes in legislation, regulatory guidelines or technological innovation.
- ✓ The results of audit, if any conducted during the year by internal / external auditors

\*\*\*\*\*