Pallavan Grama Bank

Customer Protection-Limiting Liability of Customers in Unauthorized Electronic Banking Transactions

Customer Protection-Limiting Liability of Customers in Unauthorized Electronic Banking Transactions

Introduction

Pallavan Grama Bank has put in place the necessary security measures in prevention and detection of fraudulent activities in order to provide secure and preeminent service to the customers.

In view of the increased thrust on financial Inclusion and the customer protection and considering the recent surge in customer grievances relating to unauthorized transactions resulting in debits to the customer's accounts/ cards, the criteria for determining the customer liability in these circumstances, and in reference to RBI circular DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017, the Bank has framed the Board approved policy for Customer Protection - Limiting Liability of Customers in Unauthorized Electronic Banking Transactions and made accessible to the public through Bank website and branches.

Objective

The objective of the policy is to ensure that the systems and procedures in banks are designed to make customers feel safe and define customer liability while carrying out electronic banking transactions.

- Robust and dynamic fraud detection and prevention mechanism.
- Appropriate measures to mitigate risks and protect themselves against liabilities arising thereon.
- A system to educate customers in protecting themselves from frauds arising from electronic banking & payments.

Strengthening of 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), Prepaid Payment Instruments (PPI), and

(ii) Face-to-face/ proximity payment transactions (transaction 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.)

Customer Protection Policy

The systems and procedures in bank must be designed to make customers feel safe about carrying our electronic banking transactions. To achieve this, bank must put in place:

(i) Appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers

(ii) The SMS alert shall mandatorily be sent to the customers wherever registered.

(iii) To facilitate complaints on unauthorized electronic transactions and/ or loss or theft of payment instrument such as card, etc., through multiple channels via website, SMS, e-mail, a dedicated toll-free helpline, reporting to home branch, etc.,

(iv) Bank shall enable customers to instantly respond by "Reply" to the 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 unauthorized electronic transactions shall be provide by bank on home page of the website.
(v) Robust and dynamic fraud detection and prevention mechanism
(vi) 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.
(vii) Appropriate measures to migrate the risks and protect themselves against the liabilities arising therefrom; and
(viii) A system of continually and repeatedly advising customers on how to protect themselves from electronic banking and payments related fraud.
(ix) Immediate response to the customers acknowledging the complaint.

Reporting of unauthorized transactions by customers to banks

(i) Customers need to mandatorily register for SMS alerts and wherever available for e-mail alerts, for electronic banking transactions.
(ii) Customer should notify the Bank about any change of mobile number, email ID & communication address.
(iii) Customers must notify the bank for any unauthorized electronic transaction at the earliest after the occurrence of such transaction, as the longer the time taken to notify the bank, the higher will be the risk of loss to the bank/customer.
(iv) Customer should not disclose the confidential details such as Account Number, Debit Card Number, PIN, CVV with anonymous persons over any mode of communications.
(v) Block/hotlist card or account in case of any suspected malicious activities and in the event of lost /theft of the card.
(vi) Customer must check the transaction alerts received through SMS/e-Mail and report to the bank immediately in case of any discrepancy.
(vii) In case of lodging a complaint, the customer must ensure to submit necessary proofs/documents within the given timeline to the bank else the complaint stands closed under customer liability.
(viii) Statement of Accounts should be checked periodically report to the bank immediately in case of any discrepancy noticed.
(ix) Crossed / account payee cheques should be issued as far as possible
(x) Blank cheques should not be signed and customers should not record their specimen signature either on pass book or cheque book
(xi) PIN & passwords should be changed on a regular basis

Limitations of Customer Liability

(a) Zero Liability of a Customer

A customer's entitlement to zero liability shall arise where the unauthorized 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 unauthorized transaction.

****Third party breaches:** Third party breaches would cover following unauthorized transactions without customer knowledge

1. **SIM duplication** – Cloning of original SIM to create duplicate SIM
2. **Application related frauds**- Stolen customer identity which is used to avail banks product & services
3. **Account takeover**- Theft of account information to obtain banks products and services including extracting funds from the customer's bank account
4. **Skimming**/**Cloning**- Collect data from the magnetic strip of the card and copying the information onto another plastic

(b) Limited Liability of a Customer

A customer shall be liable for the loss occurring due to unauthorized transaction in the following cases:

(i) In cases, where the loss is due to negligence by a customer, such as where the customer has shared the payment credentials, the customer will bear the entire loss until he reports the unauthorized transaction to the bank.

(ii) Any loss occurring after the reporting of the unauthorized transaction shall be borne by the bank.

(iii) 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 below, whichever is lower

Table 1
Maximum Liability of a Customer

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	10,000
• All other Current/ Cash Credit/ Overdraft Accounts	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 the policy in regard to customer's liability formulated in pursuance of these directions at the time of opening the accounts. Bank shall also display the approved policy in public domain for wider dissemination. The existing customers must also be individually informed about the bank's policy.

Overall liability of the customer in third party breaches, as detailed in paragraph headed "Zero Liability of a Customer" and "Limited Liability of a Customer" above, where the deficiency lies

neither with the bank nor with the customer but lies elsewhere in the system, is summarized in the below table.

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 approval 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.

Reversal Timeline for Zero Liability/Limited Liability of customer

On being notified by the customer, 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 (without waiting for settlement of insurance claim, if any). Banks may also at their discretion decide to waive off any customer liability in case of unauthorized electronic banking transactions even in cases of customer negligence. The credit shall be value dated to be as of the date of the unauthorized transaction.

Further, bank shall ensure that:

(i) A complaint is resolved and liability of the customer, if any, established within such time, as may be specified in the bank's board approved policy, but not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions mentioned under 'Limitations of customer liability';
(ii) Where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed under 'Limitations of customer liability' paid to the customer; and
(iii) In case of debit card/bank account, the customer does not suffer loss of interest.

Steps to be undertaken by Bank once customer reports fraud

(i) Bank to block the debit card on which the fraud is reported by customer.
(ii) If fraud is reported through Internet or Mobile banking channels, Bank to de-register/de-activate the service to prevent any further misuse.
(iii) Bank to post temporary credit for the fraudulent transaction under consideration as per Bank's policy.
(iv) Replace the card based on the consent of customer.
(v) Restore/Activate Mobile, Internet banking facility & UPI based on customer's consent.
(vi) Advise customer on submission of fraud intimation along with the documents as mandated by the bank on the fraudulent transaction under consideration.

Burden of Proof

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

Reporting and Monitoring Requirements

The banks shall put in place a suitable mechanism and structure for the reporting of the customer liability cases to the Board or one of its Committees. 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 in each bank shall periodically review the unauthorized electronic banking transactions reported by customer 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.