भारतीय रिज़र्व बैंक
RESERVE BANK OF INDIA
www.rbi.org.in

Draft Circular (for public comments)

RBI/2016-17/
DBR.No.Leg.BC./09.07.005/2016-17 August 11, 2016

All Scheduled Commercial Banks (including RRBs)
All Co-operative 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 and other transactions.

2. With the increased thrust on financial inclusion and customer protection as the two crucial pillars of financial stability and considering the recent surge in customer grievances relating to unauthorised transactions resulting in erroneous 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 present at the point of transactions e.g. internet banking, mobile banking, card not present (CNP) transactions) 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:

a) appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
b) robust and dynamic fraud detection and prevention mechanism;
c) mechanism to assess the risks (for example, gaps in the banks' existing systems) resulting from unauthorised transactions and measure the liabilities arising out of such events; and
d) appropriate measures to mitigate the risks and protect themselves against the liabilities arising therefrom.

Reporting of unauthorised transactions by customers to banks

5. Banks must ask their customers to mandatorily register for alerts for electronic banking transactions. The alerts shall be sent to the customers through different channels (email or SMS) offered by the banks. The customers must be advised to notify the bank concerned of any unauthorised electronic banking transaction at the earliest after the occurrence of such transaction. 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, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting fraudulent transactions that have taken place and/or loss or theft of payment instrument such as card, etc. 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 the customer's liability.

Liability of a Customer

(i) Zero Liability of a Customer

6. A customer's entitlement to zero liability shall arise where the security architecture and systems of the bank for electronic banking transactions are not able to protect the customer in the following events:

(a) Fraud/ negligence on the part of the bank (irrespective of whether the loss/fraudulent transaction is reported by the customer or not)
(b) Third party breach where the fault 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 an unauthorized transaction.

(ii) Limited Liability of a Customer

7. A customer shall be liable for the loss occurring due to fraudulent transactions in the following cases:
(a) In cases involving 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.
(b) 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) on the part of the customer in notifying the bank of such a transaction, the customer liability shall be limited to the transaction value or ₹ 5000/-, whichever is lower. Further, if the delay in reporting is beyond seven working days, the customer liability shall be determined as per bank's Board approved policy. Banks shall provide the details of the bank's policy in regard to customers' liability formulated in pursuance of these directions at the time of opening the accounts. Banks shall 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(b) and paragraph 7(b) above, where the fault lies neither with the bank nor the customer but lies elsewhere in the system, is summarised in the following table:

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 - 7 working days of receiving the communication	The transaction value or ₹ 5000/-, whichever is lower
Beyond 7 working days of receiving the communication	As per bank's Board approved policy

Reversal Timeline for Zero Liability/ Limited Liability

9. On being notified by the customer, the bank shall 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. Banks may also at their discretion decide to waive off any customer liability in case of unauthorised electronic banking transactions even in cases of customer negligence.

Further, banks shall ensure that:

(i) a complaint is resolved within 90 days from the date of reporting; and

(ii) in case of debit card/bank account the customer does not lose out on interest, and in case of credit card the customer does not bear any additional burden of interest.

Board approved Policy for Customer Protection Policy

10. Taking into account the risks arising out of unauthorised debits to customer accounts owing to customer negligence/ banking system frauds/ third party breaches, banks need to clearly define the rights and obligations of customers in case of unauthorised transactions in specified scenarios. Banks shall formulate/ revise their customer relations policy, with approval of their Board, to cover aspects of customer protection, including the mechanism of creating customer awareness on the risks and responsibilities involved in electronic banking transactions and customer liability in such cases of unauthorised electronic banking transactions. The policy must be transparent, non-discriminatory and should stipulate the mechanism of compensating the customers for the unauthorised electronic banking transactions and also prescribe the timelines for effecting such compensation, based on the circumstances of each case. The policy shall be displayed on the bank's website along with the

details of grievance handling/ escalation procedure. The instructions contained in this circular shall be incorporated in the policy.

Burden of Proof

11. The burden of proving customer liability in case of unauthorised electronic banking transactions shall lie on the bank. The bank's above policy shall also specify the maximum time period for establishing customer liability after which the bank shall compensate the customer.

Reporting and Monitoring Requirements

12. The banks shall put in place a suitable mechanism and structure for reporting of the customer liability cases to the Board or its Committee. 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 trasanctions, etc. The Standing Committee on Customer Service in each bank shall review, on a monthly basis, the unauthorised electronic banking transactions reported by customers or otherwise, as also the action taken thereupon, the functioning of the grievance redress mechanism and take appropriate measures to improve the systems and procedures.

Yours faithfully,

(Rajinder Kumar)
Chief General Manager