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

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.)

बैंकिंगविनियमनविभाग,केंद्रीयकार्यालय, 12वींऔर 13वींमंज़िल, केंद्रीयकार्यालयभवन, शहीदभगतसिंहमार्ग, मुंबई 400001
टेलीफोन /Tel No: 22661602, 22601000 फैक्स/Fax No: 022-2270 5670, 2260 5671, 5691 2270, 2260 5692
Department of Banking Regulation,Central Office, 12th & 13th Floor, Central Office Bhavan, ShahidBhagat Singh Marg, Mumbai - 400001
Tel No: 22661602, 22601000 Fax No: 022-2270 5670, 2260 5671, 5691 2270, 2260 5692

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	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	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

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

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 (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 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.

10. Further, banks 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 of paragraphs 6 to 9 above;

(ii) where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs 6 to 9 is paid to the customer; and

(iii) in case of debit card/ bank account, the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest.

Board Approved Policy for Customer Protection

11. Taking into account the risks arising out of unauthorised debits to customer accounts owing to customer negligence/ bank 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 Boards, 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 keeping in view the instructions contained in paragraph 10 above. 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

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

Reporting and Monitoring Requirements

13. 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 unauthorised 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.

14. The instructions contained in this circular supersede some of the instructions contained in our Master Circular DBR.No.FSD.BC.18/24.01.009/2015-16 dated July 1, 2015 on Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card Operations of Banks and Credit card issuing NBFCs as detailed in the Annex.

Yours faithfully,

(Prakash Baliarsingh)
Chief General Manager

Annex

Instructions in our Master Circular on Credit Card, Debit Card and Rupee Denominated Co-branded Pre-paid Card Operations of Banks and Credit card issuing NBFCs (DBR.No.FSD.BC.18/24.01.009/2015-16 dated July 1, 2015) which stand revised in respect of Scheduled Commercial Banks

Sr. No.	Existing Instructions		Revised instructions in this circular (Para No.)
	Para No.	**Instructions**	
1	I.14.1	Banks/ NBFCs should set up internal control systems to combat frauds and actively participate in fraud prevention committees/ task forces which formulate laws to prevent frauds and take proactive fraud control and enforcement measures.	4
2	II.7.(viii)(c)	7. Terms and conditions for issue of cards to customers: (viii) (c) The terms shall put the cardholder under an obligation to notify the bank immediately after becoming aware: - of the loss or theft or copying of the card or the means which enable it to be used; - of the recording on the cardholder's account of any unauthorised transaction; and - of any error or other irregularity in the maintaining of that account by the bank.	5
3	II.7.(viii)(d)	(viii) (d): The terms shall specify a contact point to which such notification can be made. Such notification can be made at any time of the day or night.	5
4	II.7.(x)	The terms shall specify that the bank shall be responsible for direct losses incurred by a cardholder due to a system malfunction directly within the bank's control. However, the bank shall not be held liable for any loss caused by a technical breakdown of the payment system if the breakdown of the system was recognizable for the cardholder by a message on the display of the device or otherwise known. The responsibility of the bank for the non-execution or defective execution of the transaction is limited to the	6 & 7

		principal sum and the loss of interest subject to the provisions of the law governing the terms.	
5	II.9.(i)	The bank shall ensure full security of the debit card. The security of the debit card shall be the responsibility of the bank and the losses incurred by any party on account of breach of security or failure of the security mechanism shall be borne by the bank.	4, 6 & 7
6	II.9.(iv)	iv) The cardholder shall bear the loss sustained up to the time of notification to the bank of any loss, theft or copying of the card but only up to a certain limit (of fixed amount or a percentage of the transaction agreed upon in advance between the cardholder and the bank), except where the cardholder acted fraudulently, knowingly or with extreme negligence.	6 & 7
7	II.9.(v)	Each bank shall provide means whereby his customers may at any time of the day or night notify the loss, theft or copying of their payment devices.	5
8	II.9.(vi)	On receipt of notification of the loss, theft or copying of the card, the bank shall take all action open to it to stop any further use of the card.	5