

Policy on Limited Liability of customers (Debit and Credit Cards, UPI, Internet Banking, Mobile Banking)

Introduction

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 and revised directions in this regard were issued by Reserve Bank of India (RBI) vide circular dated 6 July, 2017.

The revised guidelines broadly cover the following areas:

- Strengthening of systems and procedures
- Reporting of unauthorised transactions by customers to banks
- Zero liability of a customer
- Limited liability of a customer
- Reversal Timeline for Zero Liability/Limited Liability of customer
- Board Approved Policy for Customer Protection
- Burden of Proof
- Reporting and Monitoring Requirements

Transactions in scope

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).
- (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.)

Coverage of limited liability

Transactions executed using the following product channels

- Cards (both debit and credit)
- Liability account i.e. savings account
- Unified Payments Interface (UPI)
- Internet Banking
- Mobile Banking

Strengthening of systems and procedures

To ensure the customer's online transactions are safe, we have in place; –

- appropriate systems and procedures to ensure safety and security of electronic banking transactions carried out by customers;
- robust and dynamic fraud detection and prevention mechanism;
- 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;
- appropriate measures to mitigate the risks and protect ourselves against the liabilities arising there from; and
- 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 –

- Bank insists customers to register their mobile numbers/e-mails to get transaction alerts
- Banks provides its customers with 24x7 access through multiple channels (e.g. phone banking, SMS,e-mail, IVR, a dedicated toll-free helpline, reporting to home branch, etc.) for reporting unauthorised transactions.

To report unauthorized transactions, amongst other channels available, the Customer Dispute Form available in the website requires the customer to submit the document at

- Credit Card Disputes: cardsdisputes@hsbc.co.in
- Debit Card Disputes: complaints.india@hsbc.co.in
- HSBC Branches

Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

1. Zero Liability of a Customer

A customer's entitlement to zero liability will arise where the unauthorised transaction occurs in the following events –

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

2 *Limited liability of a customer

A customer shall be liable for the loss occurring due to unauthorised transactions in the following cases:

- 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.
- 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 the table below, whichever is lower.

*This is as per RBI guidelines and subject to change time to time.

Maximum Liability of a Customer under paragraph 2 (ii)

Table 1

Type of Accounts	Maximum Liability
BSBD Accounts	₹5,000
All other SB Accounts	₹10,000
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 ₹25 lakhs	
Credit cards with limit up to ₹5 lakhs	
All other Current/Cash Credit/Overdraft Accounts	
Credit cards with limit above ₹5 lakhs	₹25,000

Roadmap to protect customer's interest

For Liability accounts – As per Customer protection, Limited Liability of Customers in Unauthorised Electronic Banking Transactions issued by RBI, a shadow credit to be posted in the customer's account within 10 working days of the notification which includes submission customer dispute form. However, in case of transaction being found to be genuine i.e. undertaken by customer, the shadow credit will be reversed. Transaction which would be recognised as fraudulent, actual credit will be posted in customers account whenever customer has not been found to negligent. Complaints/feedback for non-card digital transactions are received through the customer touch points and the same is handled as per the Complaint Handling process. The amount of shadow credit to be passed to the customer until the investigation is completed will be determined basis the disputed amount by the respective branch.

For Credit /Debit Cards – The process of shadow credit (in line with the above requirements) is in place with card operations team.

On receipt of the complete customer dispute form along with the necessary documents, from 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).

Summary of Customer's Liability

Table 2

Time taken to report the fraudulent transaction from the date of receiving the communication	Customer's liability (in ₹)
Within 3 working days along with dispute documents	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	Merit based evaluation will be done on case to case basis

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.

Note – Holidays as per Negotiable Instrument act in that city will be excluded while calculating the number of Working days.

E.g. Case registered on Saturday which is a working day, will be considered as day 0 and following working day i.e. Monday will be calculated as day 1.

*Beyond 7 days' cases (Refer Table - 2)

From a Fraud Risk perspective, it is recommended that, internal team will investigate/opine on the case and advise on facts. Business will evaluate circumstances leading to delayed reporting, customer profile, relationship tenure, etc. to recommend the liability as exception.

Additionally, bank may consider cases for zero liability, 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 three working days of receiving the communication from the bank regarding the unauthorised transaction.

For ease of operations, since most such electronic transactions are pertaining to Credit/Debit cards, Disputes on Card not present transactions authenticated with 2 Factor authentication, will be treated as customer negligent transaction due to compromise of OTP and therefore the liability will be with customer irrespective of the period in which the same is notified to the Bank.

For suspect counterfeit card fraud cases, where customer hold the physical plastic card is his possession and card has been physically used for SWIPE transaction (non EMV Chip transaction), then the case will be referred to Fraud Investigation team irrespective of the reporting period not exceeding 90 days from the date of transaction. Customer will need to report transaction by submitting Customer Dispute Form to the Bank. Service Delivery will process basis the same.

Overall liability of the customer in third party breaches, as detailed in paragraph 1 (ii) and paragraph 2 (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 above.

Reversal timeline for Zero liability/limited liability of customer –

On receipt of the complete customer dispute form along with the necessary documents, from 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).

Bank 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 unauthorised transaction.

Bank will also ensure the following –

- 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 of the attached circular • where it is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in paragraphs above is paid to the customer; and
- 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

Burden of proof:

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

Reporting and monitoring requirements:

The Bank has put in place a suitable mechanism and structure for the reporting of the customer liability cases to the respective Customer Service Forum of each line of Business and further reporting to Senior Management (if required) The report will 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.

Important points to Note (for retail customers):

- Exceptions - Unique complaint reference number will not be send for SMS block cases due to system/ infrastructure constraint
- While customer is expected to write to email Id's provided above for reporting unauthorised transaction, there could be a lag of 48 hours before an alert from customers is attended to. However, any such delay in processing the alerts will not affect customer protection assigned under this circular.
- Customer Contact Center on receipt of the request forwards the same to operation team for further resolution.