Customer Protection - Limiting Liability of Customers in Unauthorised Electronic Banking Transactions (Oct 2025)

Contents

1. Preamble/ Introduction

Customer centricity is one of the five core values of the bank. Bank truly believes that Customer Experience is the key to keeping customers happy and thereby ensuring a long-lasting relationship with the Bank. Axis Bank's Customer Protection Policy has been formulated in line with regulator guidelines on Customer Protection – Limiting Liability of Customers in unauthorised Electronic Banking Transactions. Policy outlines the framework for addressing & handling customer grievances related to unauthorized transactions to their accounts /cards and the criteria for determining the customer liability in these circumstances.

The Bank shall ensure that the policy is made available in public domain (Bank's website & Branches).

2. 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.

3. References to Regulations

RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017
Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

4. Applicability

The policy document is applicable to all the customers of the bank.

5. Communication of the Policy

The Customer Protection Policy will be published on the comprehensive notice board of the branches and on the Bank's website.

6. Details of the Policy

Coverage of the Policy

Electronic banking transactions are divided into two categories:

1) 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 (credit or a debit card), Pre-paid Payment Instruments (PPI) & UPI

2) Face-to-face/ proximity payment transactions (transactions which require physical payment instrument such as a card (includes credit, debit or any prepaid payment instrument including Forex card) or mobile phone to be present at the point of transaction, e.g. ATM, POS, UPI etc.)

Aspects of Customer protection policy:

Policy outlines the obligations on behalf of bank and customer to ensure the onus of liability arising out of fraudulent transactions.

Bank must ensure following:

- Appropriate systems and procedures to ensure safety and security of electronic banking transactions.
- Dealing quickly and empathetically with customer grievances
- Mandatorily ask customers to register for SMS & wherever available, register for E-mail alerts for electronic banking transactions
- Mandatorily send SMS and wherever available send E-mail alerts for electronic banking transactions.
- May not offer facility of electronic transactions, other than ATM cash withdrawals, to customers who do not provide mobile numbers to the bank.
- Advise customers to notify unauthorised electronic banking transactions to Banks instantly upon occurrence.
- Provide customers with 24*7 access via Phone Banking, website (support section), IVR dedicated toll-free helpline, SMS, email, and Branch network for reporting unauthorised electronic banking transactions that have taken place and / or loss or theft of the payment instruments such as cards etc.
- Ensure immediate acknowledgement of fraud reported by customer along with acknowledgement number.
- Take immediate steps on receipt of an unauthorised transaction from customer to prevent further damage.
- Provide temporary credit to customer within 10 working days from the date of reporting.
- If the Bank identifies through external intelligence or during the course of its investigations, that the customer is a repeated offender in reporting fraudulent transactions, then it shall not only declare customer's liability, but also terminate the relationship with due notice.

Customer must ensure the following:

- Mandatorily register for SMS at the time of account opening
- Register for email alerts, wherever available.
- Mandatorily notify the Bank about any change of mobile number, email ID & communication address
- Block/hotlist card or account if they suspect any malicious activities or in an event of lost /theft.
- Customers at any point should not disclose or share account details, credit card number, PIN, CVV with anyone over mail, calls, or any other mode of communication.

- Confidentiality of password for internet banking & mobile banking should be ensured at all times.
- Customers to ensure passwords are kept secure and not to be recorded on paper or accessible electronic devices.
- Customer should check the transaction message triggered by bank and report any discrepancy immediately.
- Customer must submit necessary documentation to the bank as per defined timelines else the case stands closed under customer liability.
- Statement of account should be checked regularly and discrepancy if any should be reported to the Bank immediately.
- Passbook issued if any should be updated from time to time.
- Crossed / account payee cheques should be issued as far as possible.
- Blank cheques should not be signed, and customers should not record their specimen signature either on passbook or cheque book.
- PIN & passwords should be changed on a regular basis.

Table 1: Defining Customer Liability

Zero customer liability	Limited customer liability
Contributory fraud/ Negligence/ deficiency on the part of the bank (Irrespective of whether or not the transaction is reported by the customer)	Loss due to negligence of a customer by sharing payment credentials will be borne by the customer till the time he reports the unauthorised transaction to the Bank. Loss occurring after reporting of unauthorised transaction to the Bank, shall be borne by the Bank If the investigation establishes that the transaction is 2 factor authenticated liability of such transactions lies with customer, burden of proof lies with the bank.
**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.	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 4 to 7 working days 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 amount mentioned in table 2 whichever is lower If the delay in reporting is beyond seven working days, the customer liability shall be determined as per the bank's Board approved policy.

****Third party breaches:**

Third party breaches would cover following unauthorised 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 customers bank account.

4. Skimming/Cloning – Collect data from the magnetic strip of the card and copying the information onto another plastic.

Table 2: Summary of Customer's Liability

<table>
<tr><th>Time taken to report the fraudulent transaction from the date of receiving the communication</th><th colspan="2">Customer's liability (₹)</th></tr>
<tr><td>• Within 3 working days</td><td colspan="2">Zero Liability</td></tr>
<tr><td rowspan="4">• Within 4 to 7 working days</td><td>Type of Account</td><td>Maximum Liability (₹)</td></tr>
<tr><td>• BSBD Accounts</td><td>5,000</td></tr>
<tr><td>• 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</td><td>10,000</td></tr>
<tr><td>• All other Current/ Cash Credit/ Overdraft Accounts
• Credit cards with limit above Rs.5 lakh</td><td>25,000</td></tr>
<tr><td>• Beyond 7 working days</td><td colspan="2">Full Liability
However, customer to be compensated up to a limit of Rs.5000/- or the transaction value, whichever is lower, only once in the lifetime of the account as per Bank's Board approved compensation policy</td></tr>
</table>

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.

Resolution Time frame post reporting of fraudulent transaction

10 working days to provide temporary credit to customer from the date of reporting.

The credit shall be value dated to be as of the date of the unauthorised transaction.

- Customer to submit necessary documentation within 30 days (20 days for Debit & Credit Cards) of reporting fraudulent transaction.
- Final resolution within 90 days
- A complaint is resolved and liability of the customer, if any, established within such time, as specified in the bank's Board approved policy, not exceeding 90 days from the date of receipt of the complaint, and the customer is compensated as per provisions of table 1 and 2 above
- In scenarios where Bank is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in table 1 and 2 above is paid to the customer; and
- In case of debit card/ bank account, the Bank ensures that the customer does not suffer loss of interest, and in case of credit card, the customer does not bear any additional burden of interest. INR PPIs are not interest generating products hence there is no loss of interest to the customer.

For INR Prepaid card (Smart Pay Card, Meal Card, Gift Card): -

- The customer can raise the complaint within 3 days from the transaction date with relevant documentation.
- The shadow credit will be provided within 10 working days from the date of dispute raised/lodged by the customer with Bank where the dispute is not resolved within that 10-working day period.
- In scenarios where Bank is unable to resolve the complaint or determine the customer liability, if any, within 90 days, the compensation as prescribed in table 1 and 2 above is paid to the customer.

For Transit card: -

- In case the disputed transaction (retail purchases) is not resolved within 10 working days from the date of dispute raised/lodged by the customer with Bank, then the disputed transaction amount will be credited back to the Transit card by 10th working day for customer to use.
- Offline contactless transactions i.e. offline debits from the Card towards ticket purchases at transport (transit) ecosystem/ parking/ etc. is not considered under the ambit of this Policy.

For Freecharge wallet: -

- In case the disputed transaction is not resolved within 10 working days from the date of dispute raised/lodged by the customer with Freecharge, then the disputed transaction amount will be credited back to the Freecharge wallet on 10th working day for customer to use.

Channels to report fraudulent transactions by customers:

- Phone Banking Channel (special "0" option in IVR which will be direct customer to dedicated fraud officer)
- Through support section at website (https://application.axis.bank.in/webforms/axis-support/index.aspx)
- At Axis bank branches
- Customers can report fraud via digital channels like Internet & mobile banking under the services & support section/Get support.
- Fastag Customers can report through dedicated phone banking number or through ETC fastag website.
- **For INR Prepaid Cards (Smart Pay Card, Meal card, Gift Card): -**
  - Phone Banking Number - 022 6798 7700
- **For Transit Cards: -**

- Phone Banking Number - 18004194477
- Email - transit.cards@axis.bank.in

- **Freecharge Wallet Customers can report their disputes as below –**
  - 24/7 Helpline: 0124 663 4800
  - E-mail: care@freecharge.com
  - Freecharge Mobile App: Under Account section – Help and Support
  - For more information – please visit - https://www.freecharge.in/

Steps to be undertaken by Bank once customer reports fraud

- Bank to block the card (debit, credit, INR PPI, forex card) on which the fraud is reported by customer. In case of Freecharge wallet the same is blocked by Freecharge team.
- If fraud is reported through Internet or Mobile banking channels, Bank to de-register/de-activate the service to prevent any further mis-use.
- Bank to post temporary credit for the fraudulent transaction under consideration except for certain cases where permanent credit would be given subject to fulfilment of certain criteria. In Freecharge wallet, permanent credit is given if Freecharge is unable to resolve the dispute in 10 working days.
- Replace card plastic based on consent of customer. In case of Freecharge wallet, upon customer consent the same wallet is unblocked.
- Restore/Activate Mobile, Internet banking facility & UPI based on customer consent.
- 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 unauthorised electronic banking transactions shall lie on the bank.

7. Reporting / Monitoring requirements

The bank has put in place a suitable mechanism and structure for the reporting of the customer liability cases to the Customer Service Committee of the Board every quarter. 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.

8. Review of the Policy

The Policy will be effective from the date of the approval of the Board would be aligned to the amendments in accordance with regulations, circulars, notifications, etc. as may be issued by regulatory authorities from time to time. In case of any inconsistency of the provisions of this Policy with any amendments, circulars, clarifications issued by relevant authorities, then such amendments, circulars, clarifications shall prevail upon the provisions of this policy.

This policy shall be reviewed by the Board on annual basis subject to any regulatory / statutory amendment requiring an earlier review.

Last reviewed: October 2025