Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions

Background

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).

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

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 instrument including Forex card) or mobile phone to be present at the point of transaction e.g. ATM, POS, 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 transaction

***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
- Advise customers to notify unauthorised electronic banking transactions to Banks instantly upon occurrence
- Facilitate reporting of unauthorised electronic banking transactions through Phone Banking, website(support section) IVR (dedicated helpline) and Branch network
- Ensure immediate acknowledgement of fraud reported by customer
- Take immediate steps on receipt of an unauthorised transaction from customer to prevent further damage
- 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 & Email alerts at the time of account opening
- 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 pass book or cheque book
- PIN & passwords should be changed on a regular basis

Defining Customer Liability

Zero customer liability	Limited customer liability
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>Customer's liability (₹)</th></tr>
<tr><td>♦ Within 3 working days</td><td>Zero Liability</td></tr>
<tr><td>♦ Within 4 to 7 working days</td><td>All other SB accounts
<table>
<tr><th>Type of Account</th><th>Maximum Liability (₹)</th></tr>
<tr><td>BSBD Accounts</td><td>5,000</td></tr>
<tr><td>All other SB accounts
Prepaid Instruments & Gift Cards/Forex Cards
Current/Cash Credit/OD accts. of MSMEs
Current Account/Cash Credit/OD accts 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>Current/Cash Credit/OD accts,Credit Cards with limit above Rs. 5 lacs</td><td>25000</td></tr>
</table></td></tr>
<tr><td>♦ Beyond 7 working days</td><td>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.
- Customer to submit necessary documentation within 30 days(20 days for Debit & Credit Cards) of reporting fraudulent transaction
- Final resolution within 90 days

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.axisbank.com/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

Steps to be undertaken by Bank once customer reports fraud

- Bank to block the card (debit , credit or forex card) on which the fraud is reported by customer
- 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
- Replace card plastic based on consent of customer
- 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.

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 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.

Last reviewed: Apr 2019