Customer Protection Policy – AU Bank Credit Cards

1. Introduction:

As the focus on customer protection and financial inclusion is increasing, and considering the recent rise in customer complaints due to unauthorized electronic transactions, the norms to determine the customer liability under these circumstances becomes important.

Considering the risks associated, Reserve Bank of India had issued a circular on Customer Protection – Limiting Liability of Customers in Unauthorised Electronic Banking Transactions. (RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 6, 2017) which inter-alia requires Banks to formulate a Board approved policy regarding customer protection and compensation in case of unauthorized electronic banking transactions.

AU Bank is committed to provide safe customer service experience to all its customers and will abide by policies and regulations in place to ensure the superior customer experience.

2. Objective:

The aim of this policy is to communicate in a fair manner about bank's policy on Customer Protection, customer liability and customer compensation due to unauthorized electronic transactions. This establishes a system to compensate the cardholder for any financial loss due to deficiency in service on the part of the bank for any unauthorized electronic transaction.

This policy helps to provide better experience to our customers and protecting the customer against unauthorized transactions. This will help the customer to feel safe about carrying out electronic payment transactions.

3. Scope:

Electronic banking transactions covers the following:

a. Remote/ online transactions – physical Credit Card is not required at the point of transaction (ex.- card not present transactions)
b. Proximity payment transactions – physical Credit Card is required at the point of transaction (ex. – POS, ATM, QR code based transactions)
c. Any other electronic mode of payment which is accepted by bank for debiting/crediting customer account

This policy covers transactions only through the mentioned modes. The policy excludes electronic banking erroneous transactions by the AU Bank Credit Cardholder, transactions done under threat, claims due to opportunity loss, reputation loss or collateral damage.

4. Applicability:

The policy is applicable to

a. Individual/non-individual entities that hold credit card.

The policy is not applicable to:

a. Non-AU Bank Credit Cardholder who use Bank's infrastructure e.g. ATMs/ POS etc.
b. Entities that are part of the ecosystem such as Interchange organisations, Franchises, Agencies, Intermediaries, Service partners, Vendors, Merchants etc.

c. Cases in which customer is claiming non-receipt or short receipt of cash from ATM since such transactions are conducted by the customer himself/herself. Also, such complaints are resolved in line with RBI guideline on ATM failed transactions

5. Third Party Breach:

Third party breach is where deficiency does not lie with the Bank or with the customer but elsewhere in the system, including:

a. Identity Theft
b. Skimming/cloning
c. SIM Duplication
d. External frauds/compromise of other systems, e.g. ATMs/mail servers etc. being compromised

6. Points covered under the policy:

Customer will be compensated in case of loss occurring due to unauthorized electronic banking transaction as below:

Zero Liability of customer

i. Customer shall be entitled to full compensation of real loss in the event of contributory fraud or negligence on the part of the bank (irrespective of whether the transaction is reported by the customer)
ii. Customer has Zero Liability in cases of third party breach where the deficiency does not lie with the bank or with the customer but elsewhere in the system and the customer informs the bank about unauthorised transaction within **three working days** of receiving the communication from the bank

Limited Liability of customer

i. Liability in case of financial losses due to unauthorized electronic transactions where responsibility for such transaction does not lie with the bank or with the customer, but elsewhere in the system AND
ii. There is a delay by customer in informing to the Bank beyond 3 working days but less than or equal to 7 working days (after receiving the communication from the Bank), the liability of the customer per transaction will be limited to transaction amount

Complete Liability of customer

i. Customer shall bear the entire loss in cases where it is due to negligence by the customer, e.g. where the customer has shared payment credentials or Account details such as Internet Banking User Id & PIN, Credit Card PIN/OTP or due to improper protection on customer devices
ii. In cases where the responsibility for unauthorized electronic banking transaction lies neither with the Bank nor with the cardholder, but elsewhere in the system but there is a delay on the part of the cardholder in reporting to the Bank beyond 7 working days, the cardholder would be completely liable

7. Communication of the policy:

The Bank will provide the details of this policy at the time of account opening. The Bank will display the approved policy on its website and its branches. Also, bank will try to inform existing customers about this policy through publishing it on website and e-mail and SMS, if possible.

8. Summary of customer's liability:

<table>
<tr><td colspan="2">Unauthorised Transaction due to Bank's negligence</td></tr>
<tr><td>Time taken to report the fraudulent transaction from the date of receiving communication</td><td>Customer's Liability</td></tr>
<tr><td>Customer to report as soon as possible to prevent future losses</td><td>Zero liability</td></tr>
<tr><td colspan="2">Unauthorised Transaction due to customer's negligence</td></tr>
<tr><td>Customer to report as soon as possible to prevent future losses</td><td>100% liability till reported to the bank</td></tr>
<tr><td colspan="2">Maximum Liability of a Customer in case of unauthorized Electronic Transaction where Responsibility is neither with the Bank nor with the customer but lies elsewhere in the system</td></tr>
<tr><td>Within 3 working days</td><td>Zero liability</td></tr>
<tr><td>Within 4-7 working days</td><td><table><tr><th>Type of account</th><th>Maximum liability (₹)</th></tr><tr><td>Credit Cards with limit up to Rs. 5 lakh</td><td>10000</td></tr><tr><td>Credit Cards with limit above Rs. 5 lakhs</td><td>25000</td></tr></table></td></tr>
<tr><td>Beyond 7 working days</td><td>Customer liability shall be determined in accordance with the following factors:
Nature of transaction
Time of reporting
Justification given by the customer
The maximum compensation that shall be paid to the customers in such cases shall be up to INR 25, 000 or such value as decided by the business seniors on case to case basis.</td></tr>
</table>

9. Roles & Responsibilities of the Bank:

a. The bank shall make sure that appropriate systems and procedures are in place for security of electronic banking transactions
b. The Bank shall make sure that the Customer protection policy is available on the Bank's website and Bank's branches for the reference
c. The Bank shall create awareness on safe electronic transactions amongst its customers. Information on Safe Banking practices will be made available via - website, emails, ATMs, net banking, mobile banking.
d. The Bank will enable various channels for reporting of unauthorized electronic banking transactions. These include SMS, email, website, Customer Care, toll free number, IVR or through its branches.

e. The Bank shall ensure immediate acknowledgement of fraud reported by customer by specifying complaint number, the Bank will take necessary steps to prevent further unauthorized electronic banking transactions in the account or card.
f. The Bank shall ensure that all such complaints are resolved and liability of customer is established within 90 days from the date of receipt of complaint, failing which, bank would pay compensation.
g. During investigation, if it is found that customer is a repeated offender in reporting fraudulent transactions, the bank reserves right to take preventive action on the same including closing the account, terminating the relationship and declaring customer's liability
h. The Bank may restrict customer from conducting electronic banking transactions other than ATM transactions in case of non-availability of customer's mobile number.

10. Customer's Rights and Responsibilities:

a. Customer is entitled to:
    i. SMS alerts on registered mobile number for all financial electronic credit transactions
    ii. Email alerts if valid email id is registered for alerts with the Bank
    iii. Register complaint through multiple modes
    iv. Intimation at registered email/ mobile number with complaint number

b. Customer has following obligations with respect to banking activities:
    i. Customer shall mandatorily register for SMS at the time of account opening
    ii. Customer shall update his/her registered contact details if changed. Bank will only contact customer at the last known email/ mobile number. Any failure of customer to update the Bank with changes due to loss of mobile handset/change of mobile number or any other reason by customer leading to transaction alerts/OTP not reaching customer will be considered as customer negligence. Any unauthorized transaction arising out of this negligence shall be treated as customer liability.
    iii. Customer should provide all necessary documentation – customer dispute form, proof of transaction success/ failure and should also file a police complaint and provide copy of the same as per defined timelines by the bank else case stands closed under customer's liability
    iv. Customer should co-operate with the Bank's investigation and provide assistance if needed
    v. Customer must not disclose sensitive information (such as Credit Card details & PIN, CVV, NetBanking Id & password, OTP, transaction PIN) with anyone, including bank staff.
    vi. Customer shall abide by the tips and safeguards mentioned on the Bank's website
    vii. Customer must go through various instructions sent by the bank on secured banking
    viii. Customer must set transaction limits to ensure minimized exposure from time to time
    ix. Customer shall report unauthorized electronic banking transaction(s) to the Bank at the earliest after occurrence of the transaction.
    x. PIN and passwords should be updated on a frequent basis

11. Dispute Resolution process - Notifying the Bank of the unauthorized transaction:

a. Customer is required to report unauthorized electronic banking transaction to the Bank at the earliest, with basic details such as Card No., date & time of transaction and amount of transaction through the channels provided by the bank.
b. Customer shall authorize bank to take immediate steps to prevent further unauthorized transaction by blocking/ deregistering customer from notified electronic channel.
c. Customer shall clearly specify the channels to be blocked failing which the Bank holds right to block all modes through which electronic banking transactions can be carried out.
d. Customer shall share relevant documents needed for investigation or insurance claim
e. Customers should comply with Bank's reasonable requirements towards investigation and provide details of transaction, customer presence, etc.

12. Channels to report unauthorised transactions:

a. Customer Care Channel (option in IVR which will be direct customer to dedicated fraud officer)
b. Through dedicated section on the website
c. At AU Bank Branches
d. Customers can report fraud via digital channels like Internet & mobile banking

13. Resolution time frame:

a. Customer is entitled to temporary credit within 10 working days from reporting date.
b. Customer shall submit necessary documents within 20 days of reporting fraudulent transaction.
c. Customer shall receive final credit within 90 days of reporting date subject to customer fulfilling obligations.
d. The credit shall be value dated to be as of the date of the unauthorised transaction.

14. Proof of customer liability:

A second factor authentication process for electronic transactions is followed by bank, as regulated by the Reserve Bank of India. Bank has to prove all logs/reports for confirming two factor authentication. Any unauthorized transaction which has been processed after second factor authentication which can be accessed only by the customer would be considered as sufficient proof of customer's involvement or consent in transaction.

15. Force Majeure:

The bank shall not be liable to compensate customers for delayed credit if some unforeseen event (including but not limited to civil commotion, sabotage, strike or other labour disturbances, accident, fires, natural disasters or other "Acts of God", war, damage to the bank's facilities, absence of the usual means of communication etc.) beyond the control of bank which prevents it from performing its obligations within the specified time.