DIGITAL BANKING DEPARTMENT

Customer Protection Policy

(Unauthorized Electronic Banking Transaction)

Version – 4.1

September, 2023

Table of Contents

1) Introduction:

With the increased thrust on financial inclusion, customer protection and surge in customer grievances relating to unauthorized electronic banking transactions, Reserve Bank of India notification on Customer Protection — Limiting Liability of Customers in Unauthorized Electronic Banking Transactions. (Ref.: RBI/2017-18/15 DBR.No.Leg.BC.78/09.07.005/2017-18 dated July 06, 2017), requires Banks to formulate a Board approved policy on customer protection and compensation in cases of unauthorized electronic banking transactions.

The policy defines the criteria for determining the customer liability based on customer's negligence, Bank's negligence or deficiency lies elsewhere in the system, the time period of reporting of unauthorized transaction to the bank, inter-alia includes aspects of customer protection, covering the mechanism for customer awareness on the risks and responsibilities involved in electronic banking transactions.

2) Objective of the policy:

Bank of India is committed to provide better and safe customer service experience to the customers. The aim of this policy is to ensure transparency and non-discrimination with the customers on the mechanism for customer compensation for unauthorized banking transactions, customer liability for the unauthorized banking transactions and creating customer awareness on the risks and responsibilities involved in electronic banking transactions.

3) Scope and Coverage:

The Policy covers electronic banking transactions broadly divided in two categories as under:

a) 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), etc., and

b) Face-to-face / proximity payment transactions (transactions which require physical payment instruments, e.g. card or mobile phone to be sent at the point of transaction e.g. ATM, POS, etc.)

The policy excludes electronic banking transactions effected on account of error committed by a customer (e.g. NEFT/ RTGS/ IMPS, etc. carried out to an incorrect payee or amount), transactions done under duress, claims due to opportunity loss, reputation loss, other incidental costs or collateral damage.

This policy is applicable only to those persons/ entities, who are the customers (Individual/ Non individual) of the Bank as account holder, card holder (credit/ prepaid), etc.

4. Liability of a Customer:

The extent of liability of Customer in Unauthorized Electronic Banking Transactions is as under :

4.1 Zero liability of customer: Customer shall be entitled to reimbursement upto full loss i.e. direct financial loss (no liability on customer) in the following events -

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

ii. Third party breach where the deficiency lies neither with the customer nor with the Bank but lies elsewhere in the system and the customer notifies transaction as unauthorized to the bank **within three working days of receiving the communication** from the bank regarding the said transaction.

4.2 Limited Liability of customer: In cases where responsibility for unauthorized banking transaction lies neither with the customer nor with the bank, but lies elsewhere in the system **and** when there is **delay of four to seven working days** on the part of customer in notifying/reporting to the Bank of transaction as unauthorized, even after receiving of the communication/ intimation from the Bank, the liability of the customer **per transaction** shall be limited to the transaction value or amounts mentioned below in Table 1, whichever is lower-

Table1

Maximum Liability of Customer per transaction in case of unauthorized electronic banking transaction where responsibility is neither with the customer nor with the bank but lies elsewhere in the system and when there is delay of four to seven working days on the part of customer in notifying/reporting to the Bank of transaction as unauthorized, even after receiving of the communication/ intimation from the Bank (Beyond the stipulated three days).	
Type of Account	**Maximum Liability**
• Basic Saving Bank Deposit Accounts	5,000
• All other Saving Bank accounts • Pre-paid Payment Instruments/ Gift Cards of the Bank • Current/ Cash Credit/ Overdraft Accounts of MSMEs • Current/ Cash Credit/ Overdraft Accounts of Individuals with annual average balance (during 365 days preceding the incidence of fraud)/ limits up to Rs.25 lakh	10,000
• All other Current/ Cash Credit/ Overdraft Accounts • Credit Cards with limit above Rs.5 lakh	25,000

4.3 Complete liability of Customer / No Compensation to Customer:

i. In cases where the loss is due to negligence on the part of the customer, where customer has shared the payment credentials, **in whatever form** or due to improper protection on customer devices like mobile / laptop/ desktop leading to malware / Trojan or Phishing / Vishing attacks or due to non-blocking of mobile SIM on deactivation by the fraudster or where the customer was aware of fraud.

The customer shall be liable to bear the entire loss until the customer reports unauthorized transaction to the bank. Any loss occurring after reporting of unauthorized transaction shall be borne by the bank.

ii. In cases where the responsibility of unauthorized electronic banking transaction lies neither with customer nor with the bank, but lies elsewhere in the system and when there is delay on the part of customer in reporting transaction as unauthorized to the bank **after seven working days from receipt of communication** from the Bank.

4.4 Overall liability of the customer - where the deficiency lies neither with the bank nor with the customer but lies elsewhere in the system, is summarized in the Table-2 as under:

Table-2 (Summary of customer's Liability)

Time taken to report the fraudulent transaction from the date of receiving the communication	**Customer's Liability in**
Within 3 working days	Zero liability
Within 4 to 7 working days	The transaction value or the amount mentioned in Table1, whichever is lower
Beyond 7 working days	**Complete liability of customer / No Compensation of customer.**

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 date of receiving communication.

4.5 Reversal Timelines for Zero Liability / Limited Liability of customer:

i. Bank shall afford value dated **shadow credit** (where the amount reversal shall be kept under lien and will not be permitted to be withdrawn by the customer) of the amount involved in unauthorized transaction to the customer account within ten (10) working days from the date of reporting/ notifying of electronic banking transaction as unauthorized by the customer.

ii. Bank shall resolve the complaint within ninety (90) days from the date of receipt of communication regarding unauthorized electronic banking transaction either by releasing the eligible compensation amount (as per exhibit of para 4.1 and para 4.2

above) for customer use or by establishing customer negligence and recover the shadow credit amount.

5. Bank's Roles and Responsibilities:

i. Bank shall ensure that customer protection policy is available on the Bank's website and at branches for the general awareness of public on electronic banking transactions and make available ready reference to the customers.

ii. Awareness on safe usage of electronic banking transactions by the customers shall be provided by the Bank through sharing of Information/ advisories on Safe Banking Practices through emails, posters, pamphlets, notice board at branches, ATM outlets and also on Bank's website, Twitter, etc.

iii. Bank shall communicate to the customers for mandatorily registration of their mobile number to enable the Bank to intimate through SMS alerts for all debit electronic banking transactions and through email also where valid email Id has been registered with the Bank.

iv. Bank will enable and facilitate various modes of communication to customers for reporting of unauthorized transaction through SMS, email, website, toll free number, IVR, Phone Banking or through the Bank branches.

v. Bank shall acknowledge the customer complaint on reported unauthorized electronic banking transaction with unique customer complaint number; date and time of receipt of customer's notification. Bank will take immediate steps to prevent further unauthorized electronic banking transactions in the said account or card.

vi. Bank shall ensure to resolve customer's complaint within a timeline of ninety days from the date of receipt of customer complaint on electronic banking transaction as unauthorized. Bank shall either release the eligible compensation amount (as per exhibit of para 4.1 and para 4.2 above) to customer for use or recover the shadow credit amount by establishing customer negligence.

vii. Bank shall compensate the customer as per exhibit of para 4.1 and para 4.2 as stated herein above, if bank fails to resolve the customer complaints within ninety days from the receipt of customer complaint.

Bank reserves the right to take suitable recovery and / or penal action against the customer, where it has been established that customer has falsely claimed or disputed a valid transaction.

viii. Bank reserves the right to suspend the facility to transact electronic banking transaction on receipt of complaint of banking transaction as unauthorized to avoid any further loss to the customer.

ix. Bank reserves the right to suspend the facility to transact electronic banking transaction on receipt of complaint of banking transaction as unauthorized to avoid any further loss to the customer.

x. Bank may with prior notice restrict customer facility to execute electronic banking transactions including **ATM** transactions, in case of non-registration of mobile number for delivery of SMS alerts.

xi. The Digital Banking Department shall report the customer liability cases to the Customer Service Committee of Board every quarter. The reporting shall include volume/number of cases and the aggregate value involved and distribution across various categories of cases.

xii. Technology related Fraud Monitoring Group of bank shall periodically review the unauthorized electronic banking transactions reported by customers or otherwise. Committee shall also review the action taken, the functioning of the grievance redress mechanism and suggest appropriate measures to improve the systems and procedures.

6. Obligations of Customer:

Customer is bound by the following obligations with respect to banking activities related to Electronic Banking Transactions-

i. Customer must mandatorily register valid mobile number and email ID with the bank and access the alert, messages, emails on real time basis.

ii. Customer must intimate the bank immediately on change of mobile number, email ID for updation in the Account/ Customer ID along with valid documentary evidence. Any unauthorized transaction arising out of this delay will be construed as customer liability.

iii. Customer should also notify the Bank of changes of registered contact address and other details at the earliest.

iv.Customer shall consent and authorize the bank to block the credit card/ debit card/ net banking/ account in their own interest to minimize likelihood of additional loss.

v.Customer must lodge First Information Report (FIR) with police station/ cyber-crime police for the unauthorized electronic banking transaction.

vi. Customer should provide following documents to the parent branch to claim compensation for unauthorized electronic banking transaction

a) Claim Form along with Customer letter/ application on details of unauthorized banking transaction.
b) Copy of FIR lodged for unauthorized electronic banking transaction.
c) Proof of success/ failure of transaction.
d) Copy of all pages of Passport & Visa, if applicable.
e) Undertaking for restoration of loss amount upto Rs. 25,000/- and Affidavit in case where loss amount is more than 25,000/-.

vii. Customer should co-operate with the Bank's investigating authorities and provide all required assistance to resolve the complaint within the stipulated timelines of ninety days.

viii. Customer must not share sensitive information (such as Debit/Credit Card details & PIN, CVV, Net Banking ID & Password, OTP, Transaction PIN, Challenge Questions) to any person/ entities, including bank staff.

ix. Customer must protect their device as per advisories specified on the Bank's website, including updation of latest antivirus software on the device (Device includes smart phone, feature phone, laptop, desktop and Tab).

x. Customer shall abide by the "Do's and Don'ts" do tips and safeguards mentioned on the Bank's website on Secured Electronic Banking Transactions.

xi. Customer should periodically change passwords of Debit Card/ Credit Gard/ Internet banking, etc. on a regular basis.

xii. Customer should scrutinize the transaction details/ entries of passbook/ bank statement and/or credit card statement and intimate the bank immediately, in case of any discrepancy.

7. Intimation to the customer

Communication to the Customer as referred to in the policy includes SMS/ e-mail alerts sent to the customers on their registered mobile number/ e-mail ID and also includes any other means of intimation like details of transactions updated through passbook printing, statement of account, mini statement, etc. received by/ generated by the customer.

In proving so, it will be sufficient if the communication has been made as above irrespective of whether customer has read through the SMS/ e-mail alert or the updated entries in passbook/ account statement/ mini statement, etc.

8. Reporting of an Unauthorized Electronic Banking Transaction by customer

Reporting of an Unauthorized Electronic Banking Transaction by the customer to Bank is defined as date and time on which customer has reported the unique complaint to the bank i.e. from the time and date of receipt of first of first communication as above, whether by SMS or by e-mail or by updating the passbook or by obtaining/ generating account statement or by any other means. Date and time of reporting will be construed as per Indian Standard Time.

9. Proof of burden of customer liability :

Bank shall provide logs / OTP delivery status/ SMS Alerts status and digital evidence on usage of cards/ Login and Transaction Password/ PIN/ OTP / IP Address/ Mobile Applications details, etc. as proof of customer's consent/ involvement/ negligence in executing electronic banking transactions. Content of complaint, FIR, time of transaction and time of reporting of transaction as unauthorized will also have significance on proof of burden of customer liability.

The third party frauds shall be considered, where deficiency lies neither with the Bank nor customer but elsewhere in the system, viz. Application frauds, Account takeover, Skimming/ Cloning and External Frauds/ Systems like ATMs / Mail servers etc. have been compromised.

10. Force Majeure –

Notwithstanding anything contrary which contains in the policy, the bank shall not be liable to compensate customers for delayed resolution of customer complaint beyond the specified period of ninety days, if some unforeseen event (including but not limited to civil commotion, sabotage, lockout, strike or other labour disturbances, accident, fires, natural disasters/ calamities or other "Acts of God", war, damage to the bank's facilities or of its correspondent bank(s), absence of the usual means of communication or all types of transportation, etc. beyond the control of the bank prevents from performing its obligations within the specified service delivery parameters.

11. Amendment/Modification of the policy – Sunset clause

The Policy shall be valid till next review. Review of the policy shall be done at least once in three years by the Board or in case of need at lesser frequency, as per requirement of the Regulatory authority from time to time. This Policy review to be undertaken by HO-Digital Banking Department in consultation with other functional departments.